ANUÁRIO
DA PROTEÇÃO DE DADOS
2024

COORDENAÇÃO
FRANCISCO PEREIRA COUTINHO
GRAÇA CANTO MONIZ

CEDIS
CENTRO DE I&D SOBRE DIREITO E SOCIEDADE

ANUÁRIO
DA PROTEÇÃO DE DADOS
2024

ANUÁRIO
DA PROTEÇÃO DE DADOS
2024

COORDENAÇÃO
FRANCISCO PEREIRA COUTINHO
GRAÇA CANTO MONIZ

CEDIS
CENTRO DE I&D SOBRE DIREITO E SOCIEDADE

ANUÁRIO DA PROTEÇÃO DE DADOS 2024
Ano 6 – 2024

Coordenação:
Francisco Pereira Coutinho e Graça Canto Moniz

Secretariado Executivo:
Elodie Beco

Paginação:
Gráfica 99

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

Suporte: Impresso
Impressão: 150 exemplares

Outubro, 2024
ISSN 2184-5468

Catalogação na Publicação
Pereira Coutinho, Francisco e Canto Moniz, Graça (coord.). Anuário da Proteção de Dados 2024. Lisboa: CEDIS, 2024.

Índice

"CONSENT OR PAY" – NOVO CAPÍTULO NA SAGA DOS DADOS PESSOAIS COMO CONTRAPRESTAÇÃO NOS CONTRATOS DE FORNECIMENTO DE CONTEÚDOS E SERVIÇOS DIGITAIS
Martim Farinha 11

BRAIN-COMPUTER INTERFACES AND THE DECODING OF THOUGHTS AS PERSONAL MENTAL DATA
Diogo Miguel de Brito Fonseca 67

METADADOS, DIREITOS FUNDAMENTAIS E O NOVO REGIME PORTUGUÊS
Beatriz Assunção Ribeiro e Iakovina Kindylidi 109

PUBLICIDADE E TRANSPARÊNCIA NO ÂMBITO DO REGULAMENTO DOS SERVIÇOS DIGITAIS (REGULAMENTO (UE) 2022/2065 DE 19 DE OUTUBRO)
Maria Madruga de Medeiros 137

SYNTHETIC DATA: A HOLY GRAIL TO HEALTHCARE RESEARCH?
Marta Beleza Costa e Miguel Goulão 165

A OBRIGAÇÃO DE NOTIFICAR UMA VIOLAÇÃO DE DADOS PESSOAIS À AUTORIDADE DE CONTROLO
Luís Pinto Monteiro 193

OS FUNDAMENTOS DE LICITUDE APLICADOS NAS RELAÇÕES LABORAIS À LUZ DO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS
Patrícia Batista Santos 225

Nota Introdutória

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

Os sete artigos publicados na edição de 2024 do Anuário resultam de uma chamada lançada em setembro de 2023 no sítio da internet do Observatório da Proteção de Dados Pessoais. Os textos foram sujeitos a um processo de *blind peer review* e posteriormente revistos pelos coordenadores do Anuário. Aos autores foi permitido escrever de acordo com a nova ou a antiga grafia.

O Anuário inicia-se com um texto da autoria do Martim Farinha sobre os dados pessoais como contraprestação nos contratos de fornecimento de conteúdos e serviços digitais, seguindo-se um artigo do Diogo Fonseca que trata dos pensamentos enquanto dados pessoais. Os metadados no regime português é o tema do texto da Beatriz Ribeiro e da Iakovina Kindylidi. De seguida, a Maria Madruga de Medeiro debruça-se sobre a problemática da transparência no Regulamento dos Serviços Digitais. A Marta Beleza Costa e o Miguel Goulão apresentam uma análise dos dados sintética na investigação médica. Por fim, o Luís Pinto Monteiro analisa a obrigação de notificar uma violação de dados pessoais à autoridade de controlo e a Patrícia Batista Santos aborda os fundamentos de licitude aplicados nas relações laborais.

Esta obra não teria sido possível sem o patrocínio da SRS Advogados e da FUTURA, a quem agradecemos, nas pessoas do Luís Neto Galvão (SRS Advogados) e do Rodrigo Adão da Fonseca (FUTURA), o apoio que têm prestado desde a primeira hora a este projeto. Igualmente devidos são agradecimentos aos revisores deste número, ao Domingos Farinho, ao Eduardo Magrani, à Graça Canto Moniz, à Iakovina Kindylidi, à Inês Oliveira, ao Luís Neto Galvão e à Mariana Melo Egídio. Por fim, agradecemos à Elodie Beco e à Sofia Solayman o auxílio prestado na edição do Anuário, bem como a todos os autores que participam nesta edição.

Lisboa, 1 de outubro de 2024

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

"*Consent or Pay*" – novo capítulo na saga dos dados pessoais como contraprestação nos contratos de fornecimento de conteúdos e serviços digitais

Martim Farinha[1]

Resumo: Depois da Meta ter sido efetivamente proibida de utilizar a cumprimento do contrato e os interesses legítimos como base de licitude do tratamento de dados para diversas finalidades, incluindo publicidade personalizada, e da decisão do TJUE no caso C-252/21 a confirmar esta interpretação, esta anunciou que iria passar a basear o tratamento no consentimento dos titulares de dados. No entanto, a Meta acabou por implementar um modelo de "Pay or Consent", em que os titulares de dados têm duas opções: fornecer o seu consentimento a estes tratamentos de dados ou aceitar o pagamento de uma mensalidade. No seguimento deste anúncio, organizações não governamentais (ONG) como a NOYB apresentaram várias queixas quanto à validade do consentimento e à violação de direitos fundamentais a autoridades de controlo nacionais, que por sua vez remeteram ao Comité Europeu de Proteção de Dados (EDPB), enquanto um consórcio liderado pela BEUC apresentaram queixas com base em violações do Direito do Consumo. O presente texto pretende enquadrar as questões levantadas pela adoção destes modelos contratuais, relembrando parte do debate que ocorreu quanto à compatibilidade da solução adotada na Diretiva 2019/770 (DCD) dos contratos de fornecimento de conteúdos e serviços digitais com o Regulamento 2016/679 (RGPD), quanto aos dados

[1] Professor Convidado e Doutorando na NOVA School of Law, Knowledge Lawyer na Vieira de Almeida & Associados. Master in Law and Technology, NOVA School of Law. Investigador no NOVA Consumer Lab, Observatório para a Proteção de Dados Pessoais,WhatNext.Law e CEDIS I&D. ORCID: 0000-0002-3183-0774, SSRN https://ssrn.com/author=4096365

As opiniões e posições deste texto são apenas do autor.

pessoais como contraprestação, de forma a compreender os antecedentes, e as principais falhas e críticas da decisão do EDPB na Opinion 08/2024[2].

Palavras-chave: Proteção de Dados; Regulamento Geral de Proteção de Dados Pessoais; Dados como Contraprestação; Direito do Consumo; Cookie Walls; Paywalls; Consentimento; Meta; Facebook; Privacidade, Consentir or Pagar.

Abstract: After Meta was effectively banned from using performance of contract and legitimate interests as the basis for lawful data processing for various purposes, including personalised advertising, and the CJEU ruling in case C-252/21 confirming this interpretation, it announced that it would be basing processing on the consent of data subjects. However, Meta ended up implementing a "Pay or Consent" model, in which data subjects have two options: provide their consent to this data processing or accept payment of a monthly fee (€12.99 for access to one of the social networks, with an additional €8 for the other). Following this announcement, non-governamental organizastions such as NGOs such as NOYB lodged several complaints about the validity of consent and the violation of fundamental rights with national supervisory authorities, which in turn referred them to the European Data Protection Board (EDPB), while a consortium lead by BEUC also submitted complaints on the basis of violations of EU Consumer Law. This text aims to frame the issues raised by the adoption of these contractual models, recalling part of the debate that took place regarding the compatibility of the solution adopted in Directive 2019/770 (DCD) for contracts for the supply of digital content and services with Regulation 2016/679 (GDPR), regarding personal data as consideration, in order to understand possible directions of the EDPB's decision.

[2] O principal objetivo deste texto foi prever o sentido de decisão deste órgão. Atendendo a que decisão foi publicada posteriormente, este é apenas sumariamente criticada.

Keywords: Data Protection; General Data Protection Regulation; Data as Counter-Performance; Consumer Law; Cookie Walls; Paywalls; Consent; Meta; Facebook; Privacy, Consent or Pay.

1. Introdução – Uma notificação estranha no Facebook e no Instagram

Para o típico utilizador das redes sociais Facebook e Instagram, da Meta Inc., o mês de outubro de 2023 pode ter sido um mês "normal" como tantos outros. Para uma minoria, ligeiramente mais informada, até pode ocorrido uma conversa de café: "olha, vi nas notícias, acho que o Instagram vai passar a ser pago"[3]. Estas conversas eventualmente esmoreciam devido à falta de certeza sobre os detalhes, desconfiança na veracidade do "rumor" ou simples indiferença.

No entanto, já em novembro, estas conversas foram retomadas, agora com muito mais participação. Isto porque, no início deste mês, todos os utilizadores destas redes socias[4], receberam uma notificação bastante "estranha", em cada um dos serviços. "Estranha", não porque parecesse um caso de *phishing*, pela apresentação ou linguagem, mas pela "persistência" da mesma e do conteúdo da mensagem.

A notificação, que ativamente interrompia a visualização do *feed* de ambas as aplicações, referia que "No âmbito de alterações legislativas na tua região, agora podes optar por continuar a usar os produtos da

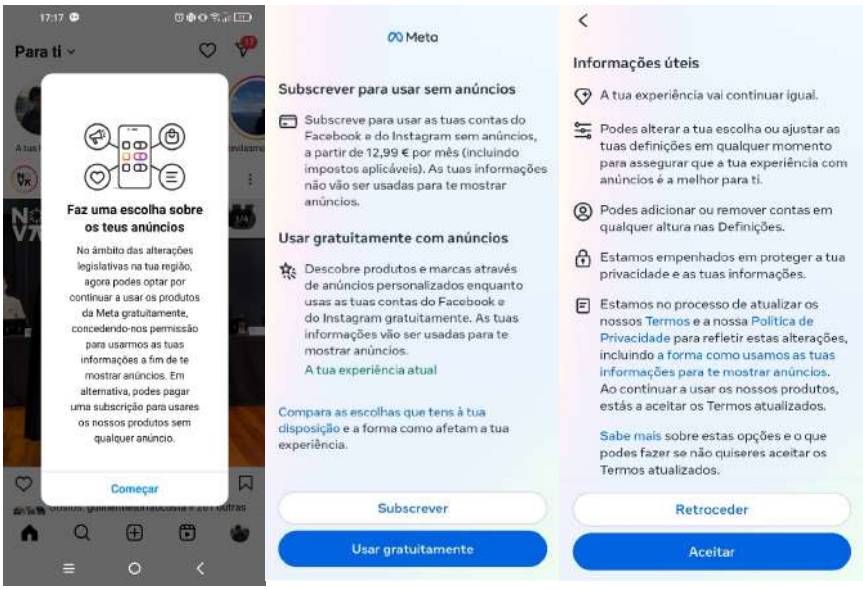
---

[3] Expresso, "Se quiser Facebook e Instagram sem anúncios, prepare-se para pagar pelo menos 10 euros", Expresso, 03/10/2023, disponível em https://expresso.pt/economia economia_tecnologia/2023-10-03-Se-quiser-Facebook-e-Instagram-sem-anuncios-prepare-se-para-pagar--pelo-menos-10-euros-36060c2c

Sam Schechner, "Meta Plans to Charge $14 a Month for Ad-Free Instagram or Facebook" Wall Street Journal, 03/10/2023, disponível em https://www.wsj.com/tech/meta-floats-charging--14-a-month-for-ad-free-instagram-or-facebook-5dbaf4d5 (consultados em 29/02/2024)

[4] Exame Informática, "Facebook e Instagram vão ter modalidade paga, sem anúncios" Visão, Exame Informática, 31/10/2023, disponível em https://visao.pt/exameinformatica/noticias-ei/mercados/2023-10-31-facebook-e-instagram-vao-ter-modalidade-paga-sem-anuncios/ (consultado em 29/02/2024)

Meta gratuitamente, concedendo-nos permissão para usarmos as tuas informações a fim de te mostrar anúncios. Em alternativa, podes pagar uma subscrição para usares os nossos produtos sem qualquer anúncio"[5].



Esta notificação não podia ser fechada para continuar a utilizar a aplicação, era mesmo preciso clicar em "Começar", passando para uma interface da Meta, "Centro das Contas", onde a escolha teria de ser feita. Em Portugal e no resto da UE, EEE e na Suiça, todos os utilizadores foram assim obrigados a escolher entre pagar ("Pay") 12,99€ por mês ou o dar o consentimento ("Okay") ao tratamento de dados pessoais.

A ideia de passar a pagar uma mensalidade com um valor substancial pelo Facebook e ou o Instagram, que sempre foram "gratuitos", causou choque e controvérsia[6].

5

[6] Blake Montgomery, "Is Meta's ad-free service just another way to make people pay for privacy?", The Guardian, December 2023, Is Meta's ad-free service just another way to make people pay for privacy? | Technology | The Guardian

No entanto, embora estas mensagens tenham causado algum burburinho e confusão, a realidade é que poucos utilizadores devem ter lido completamente todas as mensagens, e a maioria dos que leu rapidamente as deve ter esquecido, após terem dado o consentimento ao tratamento de dados. Uma vez fechada a notificação que obstruía o ecrã e passada a "novidade" e o choque dos 13€ arredondados, o assunto "morreu".

Porém, para uma ínfima minoria de pessoas que insiste em estudar estas matérias (profissionais, ativistas, académicos, advogados, encarregados de proteção de dados, entre outros) este tema continuou. E continuou com bastante pujança porque não se tratou de um incidente isolado, que até pode ter aberto alguns telejornais e servido como pergunta em jogos de *trivia* obscuros. Estas notificações e aquilo que efetivamente implicam são apenas o mais recente capítulo de uma autêntica saga que já tem vários anos: o tratamento de dados pessoais como contraprestação em contratos (tipicamente de consumo) de fornecimento de conteúdos e serviços digitais.

Esta questão implica um debate sobre a natureza do direito fundamental à proteção dos dados: se este pode ser "comodificado", até que ponto é que os dados pessoais podem ser tratados como um ativo económico, se os titulares de dados podem "pagar" com os seus dados, e se o consentimento para o tratamento de dados nestes casos pode ser considerado válido, compatível com as normas e princípios do Regulamento Geral de Proteção de Dados (RGPD)[7].

[7] 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/?uri=CELEX%3A32016R0679&qid=1709311878874

A admissibilidade dos dados como contraprestação já tinha sido muito discutida entre 2015-2022[8-9], devido aos procedimentos legislativos (e aos subsequentemente procedimentos de transposição) de duas diretivas de direito consumo, a Diretiva 2019/770, dos contratos de fornecimento de conteúdos e serviços digitais (DCD) e da Diretiva 2019/2161, de modernização do direito de consumo (Diretiva Omnibus). Neste debate, a doutrina foi gradualmente pendendo para a sua permissibilidade, pela admissibilidade das soluções adoptadas. O assunto foi, de certa forma, esmorecendo/pacificando-se com as transposições.

No entanto, como vemos, este assunto afinal não se encontrava assim tão fechado.

Após ter sofrido uma série de derrotas frente à autoridade de controlo (DPA – *Data Protection Authorities*) irlandesa[10-11],

---

[8] O autor já apresentou e defendeu várias das posições defendidas neste texto em obras anteriores, entre as quais destaca Martim Farinha, "Os limites da Proteção dos Consumidores no regime do Tratamento de Dados Pessoais como Contraprestação na Diretiva (UE) 2019/770", Jorge Morais Carvalho, Inês Crispim, Maria Miguel Oliveira da Silva, Martim Farinha, *Diretivas 2019/770 e 2019/771 e Decreto-Lei n.º 84/2021 – Compra e Venda, Fornecimento de Conteúdos e Serviços Digitais, Conformidade, Sustentabilidade e Dados Pessoais,* Almedina 2022, pp. 143-187.

[9] Sobre o tema de dados como contraprestação e a DCD, a doutrina portuguesa já explorou bastante este tema, essencialmente concordando pela admissibilidade deste mecanismo. Jorge Morais Carvalho, Manual de Direito do Consumo, Almedina 8.ª edição 2022, pp. 94-100. Também do NOVA Consumer Lab, analisando a proteção dos consumidores, Matilde Ortins de Bettencourt, "A proteção do consumidor em contratos digitais: análise dos contratos celebrados com dados como contraprestação", Anuário do NOVA Consumer Lab Ano 3- 2021, pp.387 e ss. Com uma posição bastante diferente, sobre a admissibilidade da base de licitude de execução do contrato para o tratamento de dados pessoais além dos estritamente necessários do art. 6.º n.º1 al. b) do RGPD, Rui Gordete Almeida, "Os dados pessoais como contraprestação nos contratos de consumo – a necessidade para a execução do contrato como fundamento de licitude do tratamento", RED – Revista Electrónica do Direito, Vol. 21 N.º 2, 2023. Concordando com várias das posições assumidas pelo autor deste texto, Matilde Bettencourt e Jorge Morais Carvalho, Maria Cunha Pinto, "Dados Pessoais Como Objeto Mediato de Negócios Jurídicos Onerosos", Revista da Ordem dos Advogados ROA III/IV 2022 pp. 607-646.

[10] EDPB, "Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR)", Janeiro 2023, disponível em https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-42022-dispute-submitted_en

[11] Data Protection Commission, "Data Protection Commission announces conclusion of two inquiries into Meta Ireland", Janeiro 2023, disponível em https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland

norueguesa[12-13], ao Comité Europeu de Proteção de Dados (doravante, "EDPB", de *European Data Protection Board*) e ao Bundeskartellamt (autoridade da concorrência federal na Alemanha) no Tribunal de Justiça da União Europeia (TJUE)[14], a Meta viu-se proibida de utilizar a execução do contrato e os interesses legítimos como base de licitude para o tratamento de dados. "Forçada" a utilizar o consentimento (e talvez inspirada num *obiter dictum* do TJUE no caso C-251/22), a Meta introduziu o mecanismo referido acima e reabriu este grande debate, com a equiparação nua e crua do consentimento aos 12,99€.

Rapidamente, ainda em novembro de 2023, várias organizações não governamentais (ONG), da qual destacamos a NOYB, apresentaram queixas junto de diversas autoridades de controlo, enquanto outras organizações, como a BEUC[15-16], com o apoio de um grande consórcio de associações de defesa dos direitos de consumidores, apresentaram queixas similares junto da Rede de Cooperação das Autoridades de Defesa dos Consumidores – tudo isto, de forma a combater esta prática, cunhada de "*Pay or Okay*"[17] ou "*Consent or Pay"*.

No final de janeiro de 2024, a autoridade de controlo norueguesa, *Datatilsynet*, colocou um pedido, em conjunto com a autoridade de

---

[12] Datatilsynet, "Temporary ban on behavioural advertising on Facebook and Instagram", julho 2023, disponível em https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/temporary-ban-of-behavioural-advertising-on-facebook-and-instagram/

[13] Datatilsynet, "The Norwegian Data Protection Authority's decision against Meta is extended to the EU/EEA and made permanent", novembro 2023, disponível em https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/the-norwegian-data-protection-authoritys-decision-against-meta-is-extended-to-the-eueea-and-made-permanent/

[14] C-252/21 Meta Platforms Inc. v. Bundeskartellamt, ECLI:EU:C:2023:537 https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=249028

[15] BEUC, "Choose to lose with Meta", disponível em https://www.beuc.eu/choose-to-Lose-with-Meta

[16] BEUC, "An assessment of Meta's new paid-subscription model from a consumer law perspective", novembro 2023, disponível em https://www.beuc.eu/reports/assessment-metas-new-paid-subscription-model-consumer-law-perspective

[17] NOYB, "noyb files GDPR complaint against Meta over 'Pay or Okay'", NOYB, 28/11/2023, disponível em https://noyb.eu/en/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay

controlo dos Países Baixos e a autoridade de controlo de Hamburgo, ao EDPB para emitir um parecer sobre estas práticas[18].

Com este item na agenda do EDPB – tendo sido discutido no passado dia 13 de fevereiro[19] – existiam muitas expectativas em volta desta matéria. Como a autoridade norueguesa referiu, existe uma encruzilhada "*this is a huge fork in the road. Is data protection a fundamental right for everyone, or is it a luxury reserved for the wealthy*?".

O EDPB ficou então de votar e emitir um parecer final sobre o pedido da autoridade norueguesa nas reuniões seguintes. Ainda nesta reunião de fevereiro, foi ainda reconhecida a necessidade de linhas de orientação com um âmbito mais alargado, que vá além do contexto destas grandes plataformas online[20-21], tendo este item ficado para setembro-outubro.

Adicionalmente, a Comissão Europeia, com base no art. 74(2) do Regulamento dos Serviços Digitais[22], requereu no início de março à Meta o fornecimento de informações sobre várias matérias, incluindo quanto ao modelo de *pay or consent* ("*Subscription for no Ads options*") adotado no Facebook e Instagram[23]. No Reino Unido, a ICO (*Information*

---

[18] Datatilsynet, "Request for an EDPB opinion on "consent or pay", 2024, disponível em https://www.datatilsynet.no/en/news/aktuelle-nyheter-2024/request-for-an-edpb-opinion-on-consent-or-pay/

[19] EDPB, "Agenda 90th EDPB meeting 13 February 2024", 2024, disponível em https://www.edpb.europa.eu/system/files/2024-02/20240213pleni.2.agenda_public.pdf

[20] EDPB, "EDPB clarifies notion of main establishment and calls on EU legislators to make sure CSAM Regulation respects rights to privacy and data protection", 14 de fevereiro 2024, disponível em https://www.edpb.europa.eu/news/news/2024/edpb-clarifies-notion-main-establishment-and-calls-eu-legislators-make-sure-csam_en

[21] EDPB, "Final 90th Plenary meeting 13 February 2024, in person", 14 de fevereiro 2024, disponível em https://www.edpb.europa.eu/system/files/2024-03/20240213finalminutes90thplenarymeeting_public.pdf

[22] 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).

[23] Comissão Europeia, "Commission sends request for information to Meta under the Digital Services Act", 1 de março de 2024, disponível em https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act-1

Commissioner's Office) lançou uma consulta pública sobre este tema[24].

Finalmente, após muita antecipação e bastante especulação, o EDPB na sua reunião de abril acordou a sua posição e publica a "Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms"[25] a 17 de abril. As conclusões do documento suscitaram reações muitas distintas.

Este artigo pretende enquadrar os leitores nas principais questões a ser debatidas, e sugerir possíveis posições futuras. Sendo este um tema de grande "sobreposição" e encontro entre o direito da proteção de dados, o direito dos contratos, e o direito do consumo, exige uma abordagem completa multidisciplinar.

Para tal, vamos começar por: a) em primeiro lugar, iremos brevemente introduzir a questão do tratamento dos dados pessoais terem um valor económico que impede a classificação de certas relações jurídicas (como o fornecimento de conteúdos e serviços digitais), como contratos gratuitos; b) de seguida, vamos enquadrar como o Legislador Europeu procurou abordar esta questão através da Diretiva 2019/770[26], dos conteúdos e serviços digitais (DCD) e da Diretiva 2019/2161[27], da Modernização do Direito do Consumo (Diretiva *Omnibus*), procurando enquadrar este fenómeno de forma a permitir a aplicação do Direito do Consumo Europeu em conformidade com o RGPD; c) vamos aferir como é que é a feita a articulação entre estes instrumentos e o RGPD,

---

[24] ICO, "Call for views on "consent or pay" business models", março 2024, disponível em https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/call-for-views-on-consent-or-pay-business-models/

[25] EDPB, "Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, 17 abril 2024, disponível em: https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf

[26] Diretiva (UE) 2019/770 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, sobre certos aspetos relativos aos contratos de fornecimento de conteúdos e serviços digitais, disponível em Diretiva – 2019/770 – PT – EUR-Lex (europa.eu)

[27] Diretiva (UE) 2019/2161 do Parlamento Europeu e do Conselho de 27 de novembro de 2019 que altera a Diretiva 93/13/CEE do Conselho e as Diretivas 98/6/CE, 2005/29/CE e 2011/83/UE do Parlamento Europeu e do Conselho a fim de assegurar uma melhor aplicação e a modernização das regras da União em matéria de defesa dos consumidores, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32019L2161&qid=1709311806227

em especial quanto à questão do consentimento. Quanto a este, a decisão recente do Tribunal de Justiça da União Europeia (TJUE) em julho de 2023 no caso C-251/52 Meta Inc., tem especial importância devido a um *obiter dictum* que aparenta ter aberto as portas ao mecanismo do "*Consent or Pay*"; d) depois deste enquadramento, apresentamos as queixas que foram realizadas pelas ONG e iremos refletir sobre as previsões feitas sobre a decisão do EDPB, contrastanto com o resultado final da Opinion 08/2024.

2. Não são contratos gratuitos: a importância económica dos dados pessoais

Falar da importância económica dos dados pessoais em 2024 é o equivalente a "bater na mesma tecla"[28].

Este é um assunto gasto e fechado depois de uma década de controvérsias, escândalos, documentários na Netflix, reportagens, audiências de reguladores e comissões de inquérito em ambos os lados do Atlântico, envolvendo os principais atores da revolução digital os GAMTA (Google, Amazon, META, Twitter e Apple) e as suas contrapartes chinesas (Tiktok e Alibaba).

A perceção pública nunca esteve tão consciente e informada sobre o "capitalismo de vigilância"[29], os modelos de negócio das plataformas online e a importância económica dos dados pessoais dos utilizadores. O lançamento do ChatGPT e a corrida subsequente para a criação de melhores LLMs (*large language models*) e ferramentas de inteligência artificial generativa (GenAI), exacerbou ainda mais o interesse e

[28] Já defendido anteriormente em parte em Martim Farinha, "Os limites da Proteção dos Consumidores no regime do Tratamento de Dados Pessoais como Contraprestação (…)" Almedina 2022, pp. 143-146.

[29] Shoshana Zuboff, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power", 2019, Profile Books Ltd., ISBN:9781781256855.

preocupação da sociedade no seu todo em relação à forma como os seus dados pessoais podem estar a ser utilizados[30].

Desta forma, os utilizadores sabem que o facto de muitos serviços digitais (redes sociais, plataformas online, videojogos, etc.) não requererem um pagamento de uma quantia monetária não significa que estes serviços sejam "verdadeiramente gratuitos". O tratamento dos dados pessoais estava a ser utilizado para diversas finalidades comerciais, seja para treinar algoritmos ou a criação de perfis detalhados para publicidade personalizada.

Ainda assim, como acontece frequentemente com inovações disruptivas[31], quando estes modelos de contratação surgiram e posteriormente se tornaram omnipresentes, durante a primeira metade da década de 2010, o Direito não estava preparado para dar resposta a este novo problema[32]. Durante este período, devido à ausência de uma base legal clara, subsistiram bastantes dúvidas sobre o caracter gratuito ou oneroso destes negócios jurídicos. Como esta incerteza favorecia a primeira posição, os consumidores-titulares de dados foram prejudicados, dado que isto impedia a aplicabilidade de grande parte do Direito do Consumo. Em muitas jurisdições, que não reconhecem os contratos sem "*consideration*", a conclusão pelo carácter gratuito era assim "fatal".

Felizmente, como já sabemos, o paradigma mudou, em especial na União Europeia.

A proteção dos consumidores e dos seus dados pessoais foi elevada a uma das principais prioridades do Legislador Europeu, como se

---

[30] Ver Comissão Europeia, "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.

[31] Só na última década, tecnologias disruptivas como Blockchain e Inteligência Artficial Generativa, têm levantado grandes desafios e forçado o legisladores em todo o mundo a repensar modelos regulatórios.

[32] C. Langhanke e M. Schmidt-Kessel, "Consumer Data as Consideration", Journal of European Consumer and Market Law, 2015, pp. 218 e segs.

pode observar pela estratégia do Mercado Único Digital de 2015[33], no "*New Deal for Consumers*" de 2018[34] e na Década Digital de 2020[35].

Destas agendas legislativas resultaram a DCD e a Diretiva *Omninus*, que reconhecem expressamente o papel dos dados pessoais dos consumidores na contratação e asseguram a aplicabilidade das normas do Direito de Consumo Europeu a estes modelos de negócios, no qual não há lugar a um pagamento em quantias monetárias[36].

Entretanto, ainda antes destes diplomas se tornarem aplicáveis, surgiu mais um caso que sedimentou a irreversibilidade desta questão.

Se durante muitos anos a página inicial do Facebook tinha o seu slogan "*It's free and always will be"*, este teve de ser retirado, tendo inclusive sido aplicada uma coima de cinco milhões de euros à Facebook em Itália[37] em 2021, por o *slogan* constituir uma prática comercial desleal[38],

---

[33] Comissão Europeia, "*Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões Estratégia para o Mercado Único Digital na Europa*" COM(2015) 192 final.

[34] Comissão Europeia, "*Novo Acordo para os Consumidores*", 2018, disponível com todas as propostas, diretivas revistas, linhas de orientação e outros documentos em: https://ec.europa.eu/info/law/law-topic/consumer-protection-law/review-eu-consumer-law-new-deal-consumers_pt

[35] Comissão Europeia, "*Uma Europa preparada para a Era Digital*", 2020 disponível em: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_pt

[36] A Diretiva *Omnibus* vem também permitir a aplicabilidade da Diretiva 2011/83/EU, ver Comissão Europeia, "Commission *Notice Guidance on the interpretation and application of Directive 2011/83/EU of the European Parliament and of the Council on consumer rights*" 2021, pp. 17 a 19.

[37] Ver a Decisão n.º 2631/21 Consiglio di Stadio, que pode ser consultada em: Giuseppe Cassano "Si può fare commercio di dati personali? [Consiglio di Stato, sentenza 29 marzo 2021 n. 2631]", 2021, em https://dirittodiinternet.it/si-puo-fare-commercio-di-dati-personali-consiglio-di-sato-sentenza-29-marzo-2021-n-2631/ Para uma análise do acórdão, ver Donato Maria Matera, "Personal Data as Counter-performance and Consumer Protection. An Unfair Commercial Practices Italian Decision", NOVA Consumer Lab, 2021, em https://novaconsumerlab.novalaw.unl.pt/personal-data-as-counter-performance-and-consumer-protection-an-unfair-commercial-practices-italian-decision/

[38] A querela que subsistia sobre a gratuidade desses serviços já não se coloca nível europeu, sendo essas práticas comercias consideradas desleais. Ver Comissão Europeia, "Commission Notice, Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market" 2021, pp. 22 a 23, 82 a 84. Disponível: https://ec.europa.eu/info/sites/default/files/c_2021_9320_1_ucpd-guidance_en.pdf

à luz da lei nacional que transpunha a Diretiva das Práticas Comerciais Desleais, Diretiva 2005/29/CE[39].

No entanto, como referimos, a aprovação final e transposição pelos Estados-Membros da DCD e da Diretiva *Omnibus* não puseram fim ao debate jurídico sobre a (im)possibilidade de dados pessoais constituírem contraprestações contratuais. Embora a doutrina europeia tenha assumido uma posição mais recetiva na adoção desta noção[40] e o debate tenha minguado, como vemos com as alegações feitas quanto ao "Pay and Consent" ainda subsistem alguns dúvidas (especialmente junto de certos stakeholders), quanto a uma possível colisão e incompatibilidade entre o Direito da Proteção de Dados e o Direito da Privacidade e o Direito das Obrigações e o Direito dos Contratos.

Estas dúvidas centram-se na própria validade da contratualização/comoditização do tratamento dos dados pessoais enquanto possível violação de direitos fundamentais (o que implicaria que estes contratos seriam contrários à ordem pública), e em especial, quanto compatibilidade entre a solução adotada na DCD e Diretiva *Omnibus* com o RGPD, em especial quanto à validade do consentimento.

---

[39] Diretiva 2005/29/CE do Parlamento Europeu e do Conselho, de 11 de Maio de 2005, relativa às práticas comerciais desleais das empresas face aos consumidores no mercado interno e que altera a Directiva 84/450/CEE do Conselho, as Directivas 97/7/CE, 98/27/CE e 2002/65/CE e o Regulamento (CE) n.° 2006/2004 («directiva relativa às práticas comerciais desleais»), disponível em Diretiva – 2005/29 – PT – EUR-Lex (europa.eu)

[40] Axel Metzger, "Data as Counter-Performance: What Rights and Duties do Parties Have?", 8 *JIPITEC* 2, 2017; Giuseppe Versaci, "Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection", *ERCL*, Vol. 14(4) 2018; Philipp Hacker, "Regulating the Economic Impact of Data as Counter-Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive", disponível no SSRN 2019; Madalena Narciso, "'Gratuitous' Digital Content Contracts in EU Consumer Law.", EuCML 6.5 (2017); Jorge Morais Carvalho e Martim Farinha, "Goods with Digital Elements, Digital Content and Digital Services in Directives 2019/770 and 2019/771", Revista de Direito e Tecnologia, Vol. 2 (2020), No. 2, 257-270.

3. O mecanismo de aplicabilidade da Diretiva 2019/770 e da Diretiva 2019/2161

3.1 Os procedimentos legislativos destas diretivas

A DCD e a sua "irmã", a Diretiva 2019/771 da compra e venda de bens de consumo[41], foram propostas no final de 2015 num contexto muito particular[42].

No âmbito da recém-lançada Estratégia do Mercado Único Digital[43], a Comissão delineou entre as suas prioridades legislativas a necessidade de harmonizar as normas do comércio eletrónico no espaço europeu, de forma a melhorar a proteção dos consumidores e facilitar o seu acesso a conteúdos e serviços digitais.

Neste sentido, decidiu aproveitar as melhores partes[44] do CESL (sigla inglesa da proposta um Regulamento relativo a um direito europeu comum da compra e venda)[45], uma tentativa anterior de promover

---

[41] Diretiva (UE) 2019/771 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativa a certos aspetos dos contratos de compra e venda de bens que altera o Regulamento (UE) 2017/2394 e a Diretiva 2009/22/CE e que revoga a Diretiva 1999/44/CE

[42] Sobre este procedimento legislativo, ver Martim Farinha, "Os limites da Proteção dos Consumidores no regime do Tratamento de Dados Pessoais como Contraprestação (…)", Almedina 2022, pp. 147-154. Jorge Morais Carvalho, Martim Farinha, Tecnología, "Plataformas Digitales y Derecho del Consumo: Evolución Legislativa Reciente en la Unión Europea". In *Aportaciones Jurídicas a la Economía de Plataformas,* Editorial Aranzadi.2023. 1 ed., pp. 35-53.

[43] Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões Estratégia para o Mercado Único Digital na Europa COM(2015) 192 final.

[44] É notável que o considerando 18 da proposta do CESL, publicada em outubro de 2011, já mencionava a questão de "os conteúdos digitais são muitas vezes fornecidos Os conteúdos digitais são muitas vezes fornecidos não a troco de um preço, mas combinados com outros bens ou serviços pagos, incluindo contrapartidas não pecuniárias, como o acesso a dados pessoais, ou gratuitos, no contexto de estratégias de marketing (…) Atendendo a esta estrutura específica do mercado (…) a possibilidade de aplicar o direito europeu comum da compra e venda não deve estar dependente do pagamento de um preço pelos conteúdos digitais em causa.

[45] Proposta de Regulamento do Parlamento Europeu e do Conselho relativo a um direito europeu comum da compra e venda COM/2011/0635 final. Este instrumento incluía já várias normas sobre contratos cujo objeto fosse o fornecimento de conteúdos digitais. Schulze (ed.), "*Common European Sales Law – Commentary*", Nomos 2012. M. Loo, "The regulation of digital content B2C contracts in CESL", *EuCML* 2014.

um "código civil europeu"[46], para "montar" estas duas diretivas de Direito de Consumo.

Ao optar por este caminho, a Comissão assumiu uma postura bastante mais pragmática, que lhe permitia contornar vários obstáculos. Ao focar o âmbito no Direito do Consumo conseguia circundar a resistência levantada pelo carácter muito distintivo das culturas jurídicas nacionais em matéria de Direito dos Contratos, e o formato escolhido, diretivas, ainda que de máxima harmonização, permitia desbloquear as negociações ao conferir alguma margem de discricionariedade na transposição aos Estados-Membros.

O RGPD ainda não tinha sido aprovado[47] mas as questões relacionadas com a proteção dos dados pessoais já estavam bem destacadas pela Comissão. Entre estas, destacamos a problemática dos contratos que não contemplam o pagamento de uma quantia monetária, mas a permissão pelo consumidor para o tratamento de dados pessoais, bastante patente no próprio texto da proposta da DCD[48] e na Análise de Impacto da mesma[49].

A proposta da DCD incluía assim no seu art. 3.º parágrafos 1 e 4 (cuja interpretação seria complementada pelos considerandos 13, 14 e 15) um mecanismo que permita a aplicação das normas da Diretiva (com algumas adaptações) aos contratos em que "a contrapartida consiste em dados pessoais".

Esta norma que estendia o âmbito objetivo da DCD para os casos em que os dados fossem ativamente fornecidos pelos consumidores, estabelecia como principais exceções os casos em que os dados

---

[46] O CESL tratava-se de um instrumento meramente optativo para regular os contratos entre privados focado essencialmente no Direito das Obrigações.

[47] Só aconteceria mais tarde, maio de 2016.

[48] Proposta de Diretiva do Parlamento Europeu e do Conselho sobre certos aspetos relativos aos contratos de fornecimento de conteúdos digitais COM(2015) 634 final.

[49] Commission Staff Working Document, *Impact Assessment Accompanying the document Proposals for Directives of the European Parliament and of the Council (1) on certain aspects concerning contracts for the supply of digital content and (2) on certain aspects concerning contracts for the online and other distance sales of goods* {COM(2015) 634 final}, pp. 10, 31, 33, 39.

pessoais fossem apenas os estritamente necessários à execução do contrato e ou ao cumprimento de obrigações legais que recaíssem sobre o profissional. Foi deixado de fora também os dados que fossem automaticamente recolhidos pelo profissional, como os endereços IP e metadados recolhidos através de *cookies*[50].

3.2 As críticas à comodificação de Direitos Fundamentais na DCD e da Diretiva Omnibus

Esta formulação dos artigos na proposta da Comissão, que equiparava de forma "crua" a permissão do tratamento dos dados pessoais ao pagamento do preço[51], foi bastante controversa. Com a aprovação do RGPD uns meses depois, o procedimento legislativo da DCD tornou-se bastante conturbado, tendo a redação destes preceitos em específico suscitado bastante críticas de vários *stakeholders*, seja de ONGs,[52] de *Think tanks*[53], da Academia[54] e de outras próprias instituições europeias[55]. Estes afirmavam que a equiparação do tratamento de dados pessoais ao pagamento de um preço monetário poderia resultar na

---

[50] Axel Metzger, Data as Counter-Performance: What Rights and Duties do Parties Have?, 8 (2017) *JIPITEC* 2; L. Drechsler, "Data as Counter-Performance: A New Way Forward or a Step Back for the Fundamental Right of Data Protection?", 2018, pp. 2 a 4.

[51] As críticas também se focaram na limitação do escopo apenas aos dados que fossem ativamente fornecidos pelos consumidores, deixando de lado os dados que fossem recolhidos "passivamente".

[52] Proposal for a Directive on Contracts for the Supply of Digital Content BEUC preliminary position, BEUC 2016.

[53] European Law Institute (ELI), *Statement of the European Law Institute on The European Commission's Proposed Directive on The Supply of Digital Content to Consumers*, Com (2015) 634 Final.

[54] Rafał Mańko e Shara Monteleone, 'Contracts for the Supply of Digital Content and Personal Data Protection' (2017) http://bit.ly/2URMM9W; Madalena Narciso, "Dados Pessoais como Contraprestação em Contratos de Consumo – Breve Reflexão", *Anuário NOVA Consumer Lab Ano 1 – 2019*, p. 143; J. Metzger et al., 'Data-Related Aspects of the Digital Content Directive', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* Vol.9 2018, pp. 93 e segs.

[55] EDPS, "Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, EDPS 2017, disponível em https://www.edps.europa.eu/sites/default/files/publication/17-03-14_opinion_digital_content_en.pdf

comodificação, na mercantilização expressa de um direito fundamental[56].

Entre os principais críticos destacamos a Autoridade Europeia de Proteção de Dados (EDPS), que foi especialmente veemente nesta questão, opondo-se à formulação na proposta da DCD no seu parecer 4/2017, e posteriormente também sobre a proposta da Diretiva *Omnibus*, lançada em 2018, no "Novo Acordo para os Consumidores", com o seu parecer 8/2018[57].

O EDPS referiu que, ainda que fosse meritória a extensão de aplicabilidade de ambas as Diretivas para permitir enquadrar estes falsos serviços grátis, que tal não deveria ser alcançado ao equiparar os dados pessoais ao pagamento de um preço. Na sua defesa dos dados pessoais enquanto um direito fundamental, à luz do Direito da UE e da Convenção Europeia dos Direitos do Homem (CEDH), o EDPS apontou que, ainda que haja um mercado para o tráfico de órgão humanos, o Direito Europeu não pode legitimar tais práticas, regulando-as.

Além destas considerações o EDPS apontou falhas também à ausência de uma clara definição de contraprestação e contrapartida, as dificuldades que surgem com o exercício do direito de resolução e o direito de restituição do preço (como é que se calcula o valor económicos dos dados pessoais a ser restituído ao consumidor), a falta de compreensão pelos consumidores sobre as políticas de privacidade, que por sua vez eram pouco transparentes.

O EDPS efetuou ainda uma análise das bases legais de tratamento de dados e dos direitos dos titulares no contexto nestes contratos. Concordou com o WP29 (atual EDPB) que, em alguns casos, a utilização de operações de tratamento com base em interesses legítimos do responsável ou de terceiros, como a colocação de publicidade

[56] Ver Martim Farinha, "Os limites da Proteção dos Consumidores no regime do Tratamento de Dados Pessoais como Contraprestação (…)", Almedina 2022, pp. 149-155.

[57] EDPS, "Opinion 8/2018 on the legislative package 'A New Deal for Consumers'", 2018, disponível em https://www.edps.europa.eu/sites/default/files/publication/18-10-05_opinion_consumer_law_en.pdf

personalizada, poderia ser admissível. Ainda assim, expressou várias dúvidas sobre esta possibilidade, assim como a utilização do consentimento, especialmente no que se refere à exigência deste ser livre.

Esta posição do EDPS, assumindo uma posição praticamente proibitiva de qualquer exploração económica dos dados pessoais, decorrente do seu carácter como direito fundamental, não foi completamente bem recebida pela doutrina[58].

3.3 A letra final do art. 3.º na DCD – "contrapartida" é palavra proibida e o tratamento de dados pessoais é uma contraprestação *sui generis*

No seguimento destas intervenções, o art. 3.º-1 e os considerandos 24, 25, 32 e 37 a 40 da DCD são o resultado final de muita negociação e vários compromissos[59] assumidos para apaziguar as preocupações do EDPS e dos seus apoiantes[60].

Para assegurar que a aplicabilidade da DCD se mantém sempre compatível com a proteção do direito fundamental do direito à proteção de dados, é reiterado, repetidamente, a primazia do RGPD e das suas normas[61].

Todas as menções expressas a "dados como contraprestação", "contrapartida" e qualquer elemento indicador de um sinalagma ou

---

[58] Guiseppe Versaci, "Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection", *ERCL*, Vol. 14(4) 2018, pp. 382 a 391.

[59] Ver Martim Farinha, "Os limites da Proteção dos Consumidores no regime do Tratamento de Dados Pessoais como Contraprestação (…)", Almedina 2022, pp. 154-158.

[R.] Manko e S. Monteleone, "Contracts for the Supply of digital content and personal data protection", EPRS Briefing PE 603.929, 2017; Parlamento Europeu, "Report on the proposal for a directive of the European Parliament and the Council on certain aspects concerning contracts for the supply of digital content (First Reading) – General Approach", 2017.

[60] Dado que a Diretiva Omnibus, aprovada em dezembro do mesmo ano segue a mesma formulação à letra, centraremos a nossa abordagem na DCD.

[61] Qualquer tentativa de mencionar o princípio *lex posterior derogat legi priori*, em relação à DCD sobre o RGPD é completamente inútil nestes termos.

troca recíproca entre profissional e consumidor foram, essencialmente, "purgadas" do texto[62-63].

Há uma separação clara entre a noção de preço e pagamento[64] face à aplicabilidade da DCD aos contratos em que o "consumidor faculta ou se compromete a facultar dados pessoais".

Nos considerandos, em especial o 24, encontramos expressamente o que está apenas "nas entrelinhas" dos artigos, isto é, a proibição de chamar a uma contrapartida, contrapartida.

O texto reconhece que há conteúdos e serviços digitais que são fornecidos em "situações em que o consumidor não paga um preço, mas faculta dados", que estes modelos de negócio já são uma "parte considerável do mercado", que "Embora (…) a proteção dos dados pessoais" seja um direito fundamental e os dados pessoais não possam ser considerados um "produto de base", a DCD deverá aplica-se para assegurar que os consumidores são protegidos nestes contratos.

O "embora" é particularmente revelador. Os dados pessoais não podem ser considerados com um ativo económico, mas nos casos em que "são", por serem uma condição de acesso a conteúdos e serviços, então, as normas da DCD, de contratos de consumo, devem aplicar-se. "Contraprestação" é assim tratada como "A-PALAVRA-QUE-NÃO--PODE-SER-PRONUNCIADA", como refere José Antonio Castillo Parrilla[65]. Funcionalmente é uma contrapartida, que não pode ser reconhecida expressamente como tal.

---

[62] Madalena Narciso, Dados Pessoais como Contraprestação em Contratos de Consumo – Breve Reflexão, *Anuário NOVA Consumer Lab Ano 1 – 2019*, pp. 143. Sein e Spindler, 'The new Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1' (2019) 3 *ERCL* 257–279, p. 263.

[63] Zohar Efroni, "Location Data as Contractual Counter-Performance: A Consumer Perspective on Recent EU Legislation", pp. 257–283, pp. 275 e seguintes, in M. Finck et al. (eds.), *Smart Urban Mobility*, 2020, MPI Studies on Intellectual Property and Competition Law 29, https://doi.org/10.1007/978-3-662-61920-9_13.

[64] (no art. 2.º-7 e considerando 23).

[65] Numa referência acutilante ao nome utilizado pelos mágicos que temiam o terrível Voldmort dos livros do Harry Potter, em José Antonio Castillo Parrilla "'A-PALAVRA-QUE-NÃO--PODE-SER-PRONUNCIADA' – Pagar Com Dados Pessoais Em Portugal E Em Espanha", junho 2023, NOVA Consumer Blog, https://novaconsumerlab.novalaw.unl.pt/a-palavra-que-nao-pode-ser-pronunciada-pagar-com-dados-pessoais-em-portugal-e-em-espanha/

A DCD indica que os Estados-Membros usufruem de bastante discricionariedade para estenderem o Art. 3.º-1 a outros casos na transposição para os seus ordenamentos jurídicos, desde a inclusão da recolha de metadados[66], os casos em que o consumidor seja exposto a anúncios como condição de acesso a conteúdos e serviços digitais antes de celebrar qualquer contrato e, de forma mais notória, quais os efeitos para o contrato quando o consumidor-titular de dados retire o seu consentimento.

Acresce que, se analisarmos o art. 3.º-1, percebemos que o seu âmbito de aplicação é já por si, bastante extenso.

Em primeiro lugar, aplica-se apenas a contratos, deixando a sua concretização normativa, definição e as matérias de formação, validade, nulidade e efeitos para o direito nacional. Em contraste, ignora quaisquer tipologias contratais (nacionais, regionais, etc.), focando-se no objeto. Aplica-se a todos os contratos em que haja o fornecimento de conteúdos e serviços digitais e sejam tratados dados pessoais do consumidor-titular de dados, ou este se comprometa a facultá-los[67].

Esta exclusão dos contratos é especialmente relevante para o caso paradigmático da navegação online em que o consumidor-titular de dados esteja meramente exposto a anúncios publicitários, e do tratamento de metadados, geralmente obtidos por cookies. Estes casos são geralmente deixado para o possível campo de aplicação da Diretiva da Privacidade Eletrónica ("*e-Privacy Directive*"[68]), exceto nos casos em que o direito nacional do Estado Membro considerar que se encontra celebrado um contrato entre as partes. O Legislador Europeu não

---

[66] Zohar Efroni, "Location Data as Contractual Counter-Performance: A Consumer Perspective on Recent EU Legislation", pp. 257–283, p. 276, in M. FINCK et al. (eds.), Smart Urban Mobility, 2020, MPI Studies on Intellectual Property and Competition Law 29, https://doi.org/10.1007/978-3-662-61920-9_13

[67] Dirk Staudenmayer, "Article 3", pp. 69 e segs. In Reiner Schulze e Dirk Staudenmayer, *EU Digital Law Article-by-Article Commentary*, Nomos 2020.

[68] 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.

pretendeu expandir a DCD a estas situações (que no fundo seria impor a sua aplicabilidade na quase totalidade das atividades online)[69].

Existem apenas duas exceções em que não se aplica: as operações de tratamento de dados que tenham como finalidade exclusiva o fornecimento dos conteúdos e serviços em conformidade com a diretiva e ou no cumprimento de requisitos legais em que o profissional-responsável do tratamento está sujeito. O alcance deste preceito é assim conceptualmente definido por uma delimitação negativa, resultando num âmbito de aplicação bastante amplo[70].

O enunciado desta norma permite ainda outro resultado: se o responsável pelo tratamento violar o RGPD, seja porque o tratamento não foi transparente, por não ter sido devidamente comunicado ao titular dos dados e ou este não tiver uma base de licitude válida, a DCD é ainda assim aplicável.

Desta forma, caso o responsável pelo tratamento indicasse incorretamente que o tratamento de dados era necessário para a execução do contrato (art. 6.º n.º 1 alínea b RGPD), a DCD seria ainda aplicável[71]. O titular de dados, enquanto consumidor, beneficia assim da proteção simultânea do RGPD e da DCD, e o profissional-responsável pelo tratamento não beneficia de violar o primeiro para impedir a aplicação do segundo.

Quanto às duas exceções exclusivas do art. 3.º n.º 1 DCD, defendemos que estas devem ser interpretadas com referência a duas bases de licitude do tratamento do art. 6.º RGPD[72], devido aos princípios subjacentes à sua redação.

---

[69] Sein e Spindler, 'The new Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1' (2019) 3 *ERCL* 257–279, p. 263.

[70] O número 4 do mesmo artigo contém um elenco taxativos de serviços digitais que estão excluídos do âmbito material da DCD.

[71] Axel Metzger, "A Market Model for Personal Data: State of Play under the New Directive on Digital Content and Digital Services", In "*Data as Counter-Performance – Contract Law 2.0?*", pp. 33 e 34.

[72] Discordando da nossa posição, Dirk Staudenmayer, "Article 3", p. 72 e segs. In Reiner Schulze e Dirk Staudenmayer, *EU Digital Law Article-by-Article Commentary*, Nomos 2020.

Quando os tratamentos de dados sejam exclusivamente para assegurar que os serviços e conteúdos digitais sejam fornecidos em conformidade com a DCD, somos remetidos para o cumprimento das obrigações contratuais no art. 6.º n.º 1 alínea b) RGPD. Embora haja algumas divergências que possam indicar que o preceito da DCD vai muito além da mera execução das obrigações contratuais, substancialmente não existem grandes diferenças – como o considerando 25 da DCD aponta (e os trabalhos preparatórios confirmam)[73], o princípio determinante é a necessidade, complementado pela minimização dos dados e de limitação de finalidades, isto é, o tratamento ser indispensável, essencial para assegurar o fornecimento[74] ao consumidor.

Esta exceção só se aplica aos tratamentos de dados necessários ao cumprimento pontual das obrigações, quando outros meios menos intrusivos não sejam possíveis.

A outra exceção aplica-se no leque limitado de circunstâncias em que o profissional está sujeito a claras obrigações legais[75], fruto do direito nacional ou europeu, que obrigam a realizar estes tratamentos de dados. Aqui a equiparação ao art. 6.º n.º 1 alínea c) RGPD é inevitável.

Após esta análise, é aparente que "sobram" poucas bases de licitude em que a DCD (e a Diretiva Omnibus) sejam aplicáveis para os

---

[73] Houve tentativas de assegurar que esta exceção poderia ter um intuito muito mais extensivo, incluindo tratamentos de dados com a finalidade de "melhorar o serviço", que extravasavam o critério da necessidade para o cumprimento, aproximando-se mais dos interesses legítimos, porém foram rejeitados. Esta discussão pode ser observada na "Amendment 83" do Parlamento Europeu, *Relatório sobre a proposta de diretiva do Parlamento Europeu e do Conselho sobre certos aspetos relativos aos contratos de fornecimento de conteúdos digitais* (COM(2015)0634 – C8-0394/2015 – 2015/0287(COD))", Comissão do Mercado Interno e da Proteção dos Consumidores, Comissão dos Assuntos Jurídicos, Relatores: Evelyne Gebhardt, Axel Voss A/2017/0375, p. 54. Sobre este procedimento, recomendamos a consulta de Sein e Spindler, 'The new Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1' (2019) 3 *ERCL* 257–279, p. 264, nota de rodapé 28.

[74] Zohar Efroni, "Gaps and Opportunities: The Rudimentary Protection to 'Data-Paying Consumers' under New EU Consumer Protection Law" *Weizenbaum Series 4 Working Paper*, 2020, p. 9 e 10.

[75] Como exemplos, há obrigações de "know-your-customer" aplicáveis a plataformas online e prestadores de serviços de pagamento.

tratamentos de dados pessoais realizados no contexto de contratos de fornecimento de conteúdos e serviços digitais: os interesses legítimos do responsável e o consentimento do titular (este último analisaremos em seguida).

Para os consumidores, a aplicabilidade das normas destas diretivas permite que tenham "acesso" a diversas normas em matéria de deveres de informação, cláusulas[76] e práticas abusivas[77], conformidade com o contrato, os direitos decorrentes da violação deste (com algumas adaptações quanto ao preço) o direito de resolução (especialmente relevante quanto aos dados não pessoais), que de outra forma não teriam.

As normas de direito do consumo, veem assim complementar a proteção conferida pelo RGPD. Como referido, a DCD faz diversas remissões para o RGPD, assegura a primazia deste, os direitos dos titulares podem ser livremente exercidos sem afetar as disposições da DCD, os princípios do RGPD podem ser considerados como parte dos requisitos subjetivos ou objetivos da conformidade do contrato, e as considerações sobre o consentimento são remetidas, também, para o RGPD.

Quanto aos efeitos no contrato da retirada do consentimento pelo titular, são deixados para os Estados Membros densificaram ou não, segundo o considerando 40.

Neste ponto é imperativo afirmar que DCD não alterou ou afetou os princípios de proteção de dados, mesmo quando poderia existir um interesse de *policy* na proteção dos consumidores-titulares de dados.

Uma possibilidade que foi muito debatida durante o procedimento legislativo da DCD, que o próprio EDPS colocou, foi que o exercício do direito de resolução do contrato pelo consumidor (em caso de falta

---

[76] Apenas as normas referentes ao controlo da transparência das cláusulas contratuais seriam aplicáveis. Ver M. Loos and J. Luzak, "Wanted: a Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers", *Journal of Consumer Policy*, 2016, p. 67. Madalena Narciso, "'Gratuitous' Digital Content Contracts", 2017, pp. 203. C-226/12 Constructora Principado ECLI:EU:2014:10, para. 25.

[77] Art. 5.º-1-c) e 6.º-1-e) Diretiva 2011/83/UE, e Madalena Narciso, "'Gratuitous' Digital Content Contracts", 2017, pp. 201 e 202.

de conformidade ou a realização de uma alteração com impacto negativo no serviço digital) deveria criar na esfera jurídica do profissional uma obrigação de restituição do valor económico gerado pelos dados do consumidor. Esta construção, que implicaria a verdadeira cristalização no expoente máximo da mercantilização dos dados pessoais, foi desde cedo afastada[78].

4. A compatibilidade da lógica contratual com o consentimento no RGPD

4.1 A contestação da visão proibitiva dos dados como contraprestação

No âmbito da discussão em torno do art. 3.º n.º 1 do DCD, houve vários opositores da visão "ortodoxa" do EDPS, que apontaram diversos contra-argumentos e falhas na fundamentação[79]-[80].

Primeiramente, a exploração económica[81] de dados pessoais não é proibida pelo Direito Europeu, pelos Tratados, pela Carta dos Direitos Fundamentais da União Europeia (CDFUE)[82] ou pela jurisprudência do Tribunal de Justiça da União Europeia (TJUE).

---

[78] Esta ideia também esbarrava frontalmente em problemas práticos, como a metodologia do cálculo do valor, sendo que muito provavelmente também iria apenas resultar na devolução de quantias praticamente irrisórias para a grande maioria dos consumidores-titulares. Phillip Hacker, "Regulating the Economic Impact of Data as Counterperformance: From the Illegality Doctrine to the Unfair Contract Terms Directive", pp. 46 a 76, Data as Counter-Performance – Contract Law 2.0?", Nomos 2020.

[79] Guiseppe Versaci, "Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection", *ERCL*, Vol. 14(4) 2018, pp. 382 a 391.

[80] Concordando com as posições de Versaci e Hacker, ver Martim Farinha, "Os limites da Proteção dos Consumidores no regime do Tratamento de Dados Pessoais como Contraprestação (…)", Almedina 2022, pp. 163-170.

[81] M.J. Radin, "Market-Inalienability", *Harvard Law Review*, 1987, pp. 1849 a 1937.

[82] Se compararmos a letra do Art. 8 e a Art. 3(2), *a contrario*, é identificável uma aparente distinção entre os regimes de exploração económica dos direitos de personalidade corpóreos e incorpóreos, proibindo expressamente os primeiros, e não se pronunciando sobre os segundos.

O RGPD não tem como objetivo proibir a exploração económica dos dados, mas sim assegurar um maior e melhor nível de proteção dos mesmos, de assegurar a segurança jurídica e principalmente de devolver o controlo dos dados aos seus titulares[83]. Os direitos estabelecidos (informação, acesso, portabilidade, apagamento, oposição e retirada de consentimento), permitem que os titulares autorizem essa exploração económica de seus dados pessoais sem renunciar a esses direitos, mas sim expressando sua autodeterminação.

É necessário salientar a natureza da proteção de dados pessoais como direito de personalidade[84], reconhecida por grande parte da doutrina, "na medida que protege um bem de personalidade"[85].

Esta é especialmente relevante, uma vez que as tradições jurídicas dos Estados-Membros da União Europeia permitem a exploração económica dos direitos de personalidade, desde que estejam em conformidade com as normas estatutárias que restringem a autonomia privada e a liberdade contratual das partes, em benefício do titular (que proíbem sempre a transmissão e a atribuição destes)[86].

---

[83] Encontramos estas ideias logo nos primeiros considerandos do RGPD. Do 1.º ao 14.º encontramos enunciados vários dos objetivos dos RGPD, incluindo o "empoderamento" do titular dos dados, assegurar a circulação dos dados no mercado interno, desbloqueando o seu valor económico e assegurando a proteção equilibrada dos direitos fundamentais dos cidadãos.

[84] Sobre a relação do direito da proteção de dados com os direitos de personalidade, em especial no ordenamento jurídico português, ver A. Barreto Menezes Cordeiro, "*Direitos de personalidade e dados pessoais: o que sobra para o Código Civil?", RDC I (2023),* 1, pp. 45-63. Sobre a história dos direitos de personalidade: António Menezes Cordeiro, *Tratado de Direito civil*, IV, 5.ª ed., com colaboração de A. Barreto Menezes Cordeiro, Almedina: Coimbra (2019), pp. 45 e ss.

[85] Alexandre de Sousa Pinheiro, *Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional*, Almedina 2015, pp. 777. Mafalda Miranda Barbosa, "Proteção de Dados e Direitos de Personalidade: Uma Relação de Interioridade Constitutiva. Os Beneficiários da Proteção e a Responsabilidade Civil", AB Instantia Revista do Instituto do Conhecimento AB, 2017.

[86] Guiseppe Versaci, 2018, pp. 386 a 388. Sobre a limitação convencional dos direitos de personalidade e os limites da autonomia privada no direito português, ver Pedro Pais de Vasconcelos, *Teoria Geral do Direito Civil*, 7.ª ed. Almedina 2014, pp. 48 e seguintes. O art. 81.º-2 do Código Civil, estabelece a livre revogabilidade destes negócios jurídicos pelo titular, sendo que a obrigação de indemnizar refere-se apenas aos "prejuízos causados às legítimas expetativas da outra parte".

Os princípios que regem a exploração económica dos direitos de personalidade são a especificidade e determinabilidade do consentimento do titular, a interpretação restritiva do objeto do contrato em benefício do titular, e a revogabilidade do consentimento (ainda que em certos ordenamentos jurídicos, esta tenha de ser fundamentada e o seu exercício possa implicar que titular esteja sujeito à condição de indemnizar a contraparte por danos causados[87]).

Esta posição, que permite a exploração económica dos dados pessoais[88] enquanto direitos de personalidade, não permite a restrição do exercício dos direitos dos titulares através de renúncia destes mesmos direitos, como parece sugerir o EDPS. Não são mutuamente exclusivas[89]. Estes direitos são garantidos por normas imperativas, que levam à invalidade das cláusulas contratuais que estipulem esse tipo de renúncias. Além disso, o RGPD, pelo efeito do primado, implica a inaplicabilidade de quaisquer normas de direito nacional que entrem em conflito com os direitos plasmados RGPD.

Se tomarmos como exemplo o ordenamento português, como um dos casos em que normas nacionais impõem ao titular o dever de indemnizar, (o art. 81.º n.º 2 do Código Civil), vemos este confronto facilmente resolvido. O consentimento pode ser livremente retirado pelo titular pois o RGPD tem primazia sobre o Código. Adicionalmente, dificilmente a retirada pelo tratamento conseguiria preencher o requisito da violação das legítimas expectativas, seja quanto à prova e quantificação dos prejuízos causados, face à letra crua do considerando 42 RGPD sobre o

---

[87] G. Resta, "The New Frontiers of Personality Rights and the Problem of Commodification: European and Comparative Perspectives", *Tulane European & Civil Law Forum*, 2011, pp. 62 a 65; T. Gisclard, "Limitations of Autonomy of the Will in Conventions of Exploitation of Personality Rights", *International Review of Intellectual Property and Competition Law*, 2014, pp. 22 e seguintes.

[88] Sobre a exploração económica dos dados pelos titulares, numa visão de Direitos Reais, ver N. Purtova, "*Property rights in personal data: A European Perspective*", The Hague: Kluwer Law International 2011; V. Bergelson, "It's Personal But is it Mine? Toward Property Rights in Personal Information", *University of California Davis Law Review*, 2003, p. 379-451.

[89] J. Metzger, 'Data-Related Aspects of the Digital Content Directive', *JIPITEC* Vol.9 2018, pp. 93 e segs.;

RGPD ("não puder recusar nem retirar o consentimento sem ser prejudicado"). Aqui a questão vai muito além de "perda de qualidade do serviço" ou perder acesso ao serviço, é literalmente causar danos económicos diretos na esfera jurídica do titular de dados pelo exercício do direito.

4.2 O consentimento livre no RGPD

Entre as críticas do EDPS no âmbito dos procedimentos legislativos da DCD e da Diretiva Omnibus[90], a questão que foi recorrentemente colocada como obstáculo, que também é imperativa para considerar a admissibilidade dos modelos "*pay or consent*", é a questão do consentimento como base de licitude, art. 6.º n.1 aliena a RGPD.

O consentimento é definido no art. 4.º n.º 11, devendo ser obtido de acordo com os requisitos do art. 7.º, interpretados com auxílio dos considerandos 32, 38, 40, 42, 43. Temos ainda de considerar a jurisprudência do TJUE, que ao longo dos anos teceu em várias decisões sobre o mesm[91]o (sendo que vários aspetos do consentimento no RGPD resultam da codificação de precedentes sobre o mesmo na anterior Diretiva 95/46/CE).

O consentimento é uma manifestação de vontade livre, específica, informada e explícita, pela qual o titular de dados aceita, mediante uma declaração ou ato positivo inequívoco, que os seus dados pessoais sejam objeto de tratamento[92]-[93].

---

[90] Ver Axel Metzger, "Data as Counter-Performance: What Rights and Duties (…)", 2017, p. 5.

[91] C-61/19, Orange Romania SA, ECLI:EU:C:2020:901, C673/17, Planet49, EU:C:2019:801, C-129/21 Proximus EU:C:2022:833, C-252/21 Meta Platforms, entre outros.

[92] Kuner et al., "*The EU General Data Protection Regulation (GDPR)*" Oxford University Press 2020, p. 181; EDPB, "*Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679 Versão 1.1*", Comité Europeu para a Proteção de Dados (EDPB), 2020, pp. 7 e seguintes, e WP29, "*Orientações do Grupo de Trabalho do Artigo 29.º relativas ao consentimento na aceção do Regulamento (UE) 2016/679*", WP29, rev. 01, 2018, p. 5.

[93] Marco Botta and Danielle da Costa Leite Borge, "User Consent at the Interface of the DMA and the GDPR. A Privacysetting Solution to Ensure Compliance with ART. 5(2) DMA", European University Institute Robert Schuman Centre for Advanced Studies Centre for a Digital Society Working Paper.

Para o consentimento ser válido, tem de ser informado, o titular tem de estar plenamente informado de modo inteligível, de acordo com todos os deveres de informação do art. 13.º. Tem de ter fácil acesso a todas as informações relevantes, desde os dados tratados, finalidades, duração do armazenamento, medidas de segurança, etc.

O consentimento nunca poderá ser considerado válido se for "obtido" através do silêncio, omissão e opções pré-validadas[94]. Deve resultar do preenchimento ativo dessa opção pelo titular, e, no contexto de relações contratuais, recolhido separadamente à aceitação do contrato.

O busílis da questão coloca-se quanto ao elemento "livre" do consentimento. Este deve resultar de uma verdadeira escolha do titular, em que este não tenha sido coagido ou pressionado a aceitar. Para este ser livre, não importa apenas o momento em que é obtido, da manifestação da vontade: o consentimento deve poder ser livremente retirado. O titular não pode ser pressionado a "manter" o consentimento, não deve ser ameaçado de consequências futuras, não pode ficar preso.

Este elemento é decomposto em em quatro subelementos: desequilíbrio de poder, condicionalidade, granularidade e prejuízos[95].

Quanto ao desequilíbrio de poder, segundo o considerando 43, esta avaliação passa geralmente por analisar o contexto da relação entre titular e responsável, para compreender se existe um desnível entre as suas posições, que implique a restrição da liberdade de escolha do titular. Este subelemento pode ser colocado em causa quando se verifica uma dependência jurídico-económica, institucional ou hierárquica, associada ou não a um temor reverencial, quando existe a perceção do titular de ser prejudicado pela sua escolha[96].

---

[94] C-61/19, Orange Romania SA, ECLI:EU:C:2020:901, para. 35 a 40. C673/17, Planet49, EU:C:2019:801, para. 74. EDPB, "*Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679 Versão 1.1*", Comité Europeu para a Proteção de Dados (EDPB), 2020, pp. 7 e seguintes. Alexandre Sousa Pinheiro e vários, "*Comentário ao Regulamento Geral de Proteção de Dados*", Almedina 2018, p. 170.

[95] EDPB, "*Diretrizes 05/2020 (...)",* 2020, pp. 7 e seguintes.

[96] Kuner et al., "*The EU General Data Protection Regulation (GDPR)*" 2019, p. 182.

O subelemento da condicionalidade, que encontramos patente no art. 7.º n.º 4 e no considerando 43, indica que o consentimento não será livre se este estiver "associado", "agregado" ou "subjugado" à aceitação da proposta contratual. Parte significativa das críticas à noção dos dados como contraprestação partia deste elemento: a letra do art. 7.º n.º 4 seria incompatível e proibiria este tipo de mecanismos e esquemas.

No entanto, se analisarmos atentamente o art. 7.º n.º 4, não vamos encontrar uma proibição, mas antes uma presunção.

Segundo o EDPB, esta presunção de invalidade do consentimento visa impedir que a finalidade do tratamento dos dados esteja assim forçosamente "agregada" (ou mesmo camuflada) à execução de um contrato ou prestação do serviço. O titular não pode ser obrigado a concordar com o tratamento dos dados além do necessário nestes termos, pois isto corresponderia, funcionalmente, a uma espécie de "fusão" de duas bases de licitude do tratamento distintas, o contrato e o consentimento[97].

Nos casos excecionais em que a condicionalidade não implicasse a invalidade do consentimento, o responsável ficaria com um dever de escrutínio e cuidado especial ("com a máxima atenção") de assegurar a viabilidade deste, ficando ainda com o ónus da prova de demonstrar o cumprimento deste requisito[98].

O EDPB teorizou uma possibilidade válida para a concretização deste preceito. O consentimento para o tratamento de dados para outros fins que não o cumprimento do contrato seria válido se o mesmo responsável dessa a escolha ao titular entre esta opção e outra, um serviço equivalente, que não requer estes tratamentos de dados. No entanto, tal já não se verificaria se o serviço equivalente fosse oferecido por outro responsável, pois não seria verdadeiramente equivalente, estando dependente de outros agentes no mercado[99].

---

[97] EDBP, "*Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679*", 2020, pp. 11 e 12.

[98] EDPB, "*Diretrizes 05/2020 (...)*", 2020, pp. 12 e 13.

[99] EDPB, "*Diretrizes 05/2020 (...)*", 2020, p. 13.

O TJUE já se pronunciou sobre alguns pontos deste raciocínio. No caso StWL Städtische Werke Lauf (C-102/20)[100], o tribunal confirmou que o consentimento para o tratamento de dados para fins complementares ao contrato (nomeadamente, o envio de publicidade), era válido, ao existir a opção como como alternativa de aceder ao mesmo serviço, mediante o pagamento de uma quantia monetária. No caso Planet49 (C-673/17), o advogado-geral reafirmou a necessidade de separar os atos de aceitação do contrato da obtenção do consentimento, e que o segundo deveria ser apresentado com igual importância, que não deve ser considerado como meramente complementar do primeiro[101].

Quanto ao subelemento da granularidade, o consentimento deve abranger todas as atividades de tratamento com o mesmo objetivo, sendo que se houver múltiplas finalidades complementares, o titular dos dados deve ter a opção de consentir ou recusar separadamente cada uma[102].

Quanto ao subelemento dos prejuízos, o titular dos dados deve poder retirar livremente o consentimento, sem sofrer quaisquer prejuízos, sem lhe implicar prejuízo[103].

É neste contexto, que o EDPB tem defendido uma interpretação bastante restritiva do conceito de consentimento livre[104], quando aos subelementos da condicionalidade e dos prejuízos (neste último, qualquer perda de qualidade devida à retirada do consentimento (quanto mais a interrupção do serviço) implicará a invalidade deste. Na acessão deste órgão, o art. 7.º n.º 4 do RGPD praticamente contém uma proibição expressa da noção de dados como contrapartida, quando os dados

---

[100] C-102/20, StWL Städtische Werke Lauf, ECLI:EU:C:2021:954, para. 58 e 59. A opinião do Advogado-Geral Jean De La Tour, vai no mesmo sentido, não levantando dúvidas à possibilidade do uso do consentimento como base de licitude para a exibição de publicidade, enquanto condição da gratuidade do serviço de email. Conclusões AG C-102/20, ECLI:EU:C:2021:518, para. 64 e 65.

[101] Conclusões AG C-673/17, Planet49, para. 66, 68 e 99.

[102] Conforme descrito nos considerandos 43 e 32.

[103] Considerando 42.

[104] EDPB, "*Diretrizes 05/2020 (...)*", 2020, p. 14 e 15.

pessoais tratados para finalidades que não sejam necessárias à execução do contrato se baseiem no consentimento do titular[105].,

A nossa posição[106] tem sido bastante contrária a esta noção, o art. 7.º n.º 4 não consagra uma proibição expressa, mas antes um ónus, um especial dever do responsável pelo tratamento de dados e dos tribunais de ("com o máximo de atenção") de assegurar que o consentimento do titular é verdadeiramente voluntário quando enquadrado numa relação contratual[107].

É assim necessário realizar sempre uma análise casuística de vários indicadores para ponderar a existência de possíveis restrições à liberdade do titular em consentir. Entre os possíveis indicadores destacamos a existência de serviços equivalentes fornecidos pelo mesmo prestador sem o tratamento de dados, serviços equivalentes de concorrentes (especial destaque para o estrutura do mercado, grau de equivalência e facilidade n migração/portabilidade), se o serviço em causa é essencial ou dispensável, se é recreacional e lazer ou profissional[108], o tipo de dados pessoais tratados, as finalidades, especialmente ao tipo de dados tratados (em especial quanto às categorias especiais do art. 9.º RGPD), a criação e extensão dos perfis criados, a sujeição a decisões individuais automatizadas, a partilha de dados com terceiros, transferência de dados para países terceiros.

Para esta análise, especialmente quando à análise do subelemento do desequilíbrio entre as partes[109], é especialmente útil[110] recorrer a

---

[105] Madalena Narciso, "Dados Pessoais como Contraprestação em Contratos de Consumo – Breve Reflexão", 2019, p. 145 e 146.

[106] Martim Farinha, "Os limites da Proteção dos Consumidores no regime do Tratamento de Dados Pessoais como Contraprestação (…)" Jorge Morais Carvalho et al., *Diretivas 2019/770 e 2019/771 e Decreto-Lei n.º 84/2024 (...),* Almedina 2022, pp. 143-187.

[107] A. Metzger, "Data as Counter-Performance: What Rights (…)", *JIPITEC* Vol. 8(2) 2017, p. 4.

[108] A. Metzger, "Data as Counter-Performance: What Rights (…)", *JIPITEC* Vol. 8(2) 2017, p. 4 para. 12.

[109] Guiseppe Versaci, "Personal Data and Contract Law: Challenges and Concerns about Economic Exploitation of the Right to Data Protection", ERCL Vol. 14(4) 2018, 374-393, pp. 389 e 390.

[110] (mesmo quando não diretamente aplicáveis por o titular de dados não se tratar de um consumidor).

noções de carácter abusivo[111], desleal, enganador, intrusivo, presentes no *acquis* de Direito do Consumo Europeu, na Diretiva das Práticas Comerciais Desleais[112], Diretiva das Cláusulas Contratuais Abusivas[113] e na Diretiva dos Direitos dos Consumidores[114].

Quanto à retirada do consentimento e a questão dos prejuízos causados, no âmbito da transposição da DCD colocaram-se vários desafios sobre esta matéria nas transposições. No contexto contratual, poderá o profissional-responsável pelo tratamento, considerando a exceção de não cumprimento, não cumprir com a sua prestação, interrompendo o fornecimento dos conteúdos e serviços digitais? Poderá resolver o contrato? Como alternativa, poderá exigir o pagamento de um preço e ou exigir uma indeminização ao consumidor-titular de dados?

Como referimos anteriormente (na secção dos direitos de personalidade), à luz do RGPD é patente que qualquer norma que atribua responsabilidade civil ao titular de dados pelo exercício do direito de retirada do consentimento será considerada incompatível com o RGPD e inaplicável. De igual forma, qualquer tentativa de associar a retirada do consentimento a uma cobrança automática de um valor pecuniário não aceite expressamente pelo titular deverá ser inadmissível.

A *contrario*, já nos parece admissível que a retirada do consentimento possa resultar na interrupção do acesso a conteúdos e serviços digitais, ou que estes passem para uma versão alternativa com menos

---

[111] Sobre a utilização da Diretiva das Cláusulas Contratuais Desleais como limite aos abusos dos dados pessoais como contraprestação, ver Phillip Hacker, "Regulating the Economic Impacto of Data as Counterperformance: From the Illegality Doctrine to the Unfair Contract Terms Directive", p. 61, In Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer, "*Data as Counter-Performance – Contract Law 2.0?*", Nomos 2020.

[112] Diretiva 2005/29/CE do Parlamento Europeu e do Conselho, de 11 de Maio de 2005, relativa às práticas comerciais desleais das empresas face aos consumidores no mercado interno e que altera a Diretiva 84/450/CEE do Conselho, as Diretivas 97/7/CE, 98/27/CE e 2002/65/CE e o Regulamento (CE) n.° 2006/2004 («directiva relativa às práticas comerciais desleais»)

[113] Diretiva 93/13/CEE do Conselho, de 5 de Abril de 1993, relativa às cláusulas abusivas nos contratos celebrados com os consumidores

[114] Directiva 2011/83/UE do Parlamento Europeu e do Conselho, de 25 de Outubro de 2011, relativa aos direitos dos consumidores, que altera a Directiva 93/13/CEE do Conselho e a Directiva 1999/44/CE do Parlamento Europeu e do Conselho e que revoga a Directiva 85/577/CEE do Conselho e a Directiva 97/7/CE do Parlamento Europeu e do Conselho

qualidade, perdendo funcionalidades e características. Seria assim, uma verdadeira versão "gratuita".

Ambas estas soluções foram admitidas (titular não pode ser castigado mas pode ver o seu acesso cortado) e consagradas na transposição. Esta parece ser a solução adotada expressamente em Espanha (onde a palavra contraprestação é mesmo utilizada)[115]-[116], Estónia[117], Lituânia[118], Países Baixos e Alemanha[119], enquanto outros Estados-Membros preferiram o silêncio (como Portugal[120], Itália[121]- e França) onde o resultado prático da interseção das normas do RGPD com o Direito das Obrigações resulta no tratamento dos dados pessoais ser tratado como uma contraprestação *sui generis*.

4.2.1 A decisão do TJUE no caso C-252/21 Meta Platforms

Recentemente, o TJUE veio a reforçar parte do nosso entendimento, com a decisão no caso C-252/21 Meta Platforms. Neste caso, que representou a interseção entre o Direito da Concorrência com o

---

[115] Sergio Cámara Lapuente, "*Un primer balance de las novedades del RDL 7/2021, de 27 de abril, para la defensa de los consumidores en el suministro de contenidos y servicios digitales*", Diariolaley 2021. José Antonio Castillo Parrilla, "Los datos personales como contraprestación en la reforma del TRLGDCU", *La Ley Mercantil*, julio-agosto 2021, No. 82, 1 de jul. de 2021, Editorial Wolters Kluwer.

[116] Esther Arroyo Amayuelas, "The Implementation of the EU Directives 2019/770 and 2019/771 in Spain", *EuCML* Vol. 11(2) 2022 pp. 35-40, v. p. 36 e 37.

[117] Irene Kull, "Transposition Of The Digital Content Directive (EU) 2019/770 Into Estonian Legal System", *JIPITEC* 12, 2021, pp. 249 e segs., v. pp. 254 a 256.

[118] Laurynas Didžiulis, "EU Digital Content Directive And Evolution Of Lithuanian Contract Law", JIPITEC 12, 2021, p. 260 e segs., v. p. 268, para. 42.

[119] M. Loo, "The (Proposed) Transposition of the Digital Content Directive in the Netherlands", *JIPITEC* 12, 2021, pp. 229 e segs.

[120] No Decreto-Lei 84/2021, ver Jorge Morais Carvalho, Manual de Direito do Consumo, 2022.

[121] Alberto De Franceschi, "Italian Consumer Law after the Transposition of Directives (EU) 2019/770 and 2019/771", *Journal of European Consumer and Market Law*, Vol. 11(2) 2022, pp. 72-76.

[V.] Ordonnance n° 2021-1247 du 29 septembre 2021 relative à la garantie légale de conformité pour les biens, les contenus numériques et les services numériques, disponível em https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044125847.

Direito da Proteção de Dados[122], o Tribunal foi confrontado com várias questões sobre a cooperação de autoridades de controlo e autoridades da concorrência, o mercado relevante para efeitos jusconcorrenciais de vários dos serviços da Meta, a possibilidade de uma violação do RGPD poder constituir também um abuso de posição dominante, a natureza das bases de licitude de tratamento utilizadas pela Meta e a prática de "juntar" os dados pessoais dos diferentes serviços da Meta e de serviços de terceiros como condição de acesso aos serviços da Meta.

Ao analisar as questões da admissibilidade dos tratamentos de dados efetuados pela Meta para várias funcionalidades, incluindo a publicidade personalizada, o TJUE metodicamente considerou (e descartou) várias bases de licitude além do consentimento: os dados serem necessários para a execução do contrato[123], serem necessários para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento[124], cumprimento de obrigações jurídicas[125], necessário para a defesa de interesses vitais do titular dos dados[126] e necessário ao exercício de funções de interesse público[127].

Quanto ao consentimento, o TJUE seguiu em parte a posição do Advogado-Geral Rantos na sua opinião[128], em que a posição dominante

---

[122] Analisando a interação entre estas duas áreas do Direito na decisão do TJUE, ver Inge Graef, "Meta platforms: How the CJEU leaves competition and data protection authorities with an assignment", Maastricht Journal of European and Comparative Law 2023, Vol. 30(3) 325–334. Or Brook e Magali Eben, "Another Missed Opportunity? Case C-252/21 Meta Platforms V. Bundeskartellamt and the Relationship between EU Competition Law and National Laws", Journal of European Competition Law & Practice, 2023, Another Missed Opportunity? Case C-252/21 Meta Platforms V. Bundeskartellamt and the Relationship between EU Competition Law and National Laws (gla.ac.uk)

[123] Concluiu que não são estritamente necessários, parágrafos 98-99 e 101-104.

[124] Os interesses e direitos fundamentais dos consumidores suplantam estes interesses e não é expectável a extensão do tratamento para os consumidores, mesmo que o serviço seja gratuito, para. 117–118, nem para "melhorar o serviço", para. 122-123.

[125] A cooperação com autoridades só se coloca em situações específicas e não está relacionada com a atividade económica da Meta, para. 124.

[126] Não é válido, para. 137.

[127] Nesta base, o TJUE duvidou seriamente dos motivos apresentados e da sua admissibilidade, deixando ao tribunal nacional a verificação no caso concreto, para. 132-133.

[128] Opinion of Advocate General Rantos in Case C-252/21 Meta Platforms v. Bundeskartellamt, para. 75.

da Meta no mercado afeta seriamente a possibilidade do consentimento ser livre, ao criar um desequilíbrio manifesto (considerando 43 RGPD) entre o titular de dados e o responsável pelo tratamento[129]. Segundo o TJUE, será muito difícil o consentimento nestes casos cumprir com as exigências do art. 7.º n.º 4 do RGPD[130] devido à possibilidade de o responsável impor requisitos que não são estritamente necessários para a execução do contrato.

Devido à extensão e amplitude do tratamento de dados e o seu impacto significativo nos utilizadores do Facebook, o TJUE apontou que seria mais adequado se os titulares de dados tiverem a possibilidade de consentir separadamente a várias operações específicas de tratamento de dados (sejam estes dados recolhidos dentro da rede social Facebook e ou fora do Facebook, de outros serviços da Meta e de terceiros), sem que a recusa em prestar este(s) consentimento(s) constitua uma renuncia ao acesso à rede social. No âmbito do processo contratual, para usufruírem desta liberdade de poder recusar consentir a estas operações de tratamento específicas, deve ser dada a possibilidade dos titulares de dados de optar por 1) uma alternativa equivalente, 2) não acompanhada destas operações de tratamento de dados, 3) que pode ser mediante o pagamento de uma "remuneração adequada"[131].

Sem esta possibilidade, o consentimento para o tratamento de dados fora do Facebook não pode ser considerado válido[132].

Com estes dois parágrafos, 150 e 151, o TJUE propõe diretamente à Meta a adoção de um modelo de "*pay or consent*" de forma a assegurar que o consentimento seja livre. Este "*obiter dictum*" confirma as nossas posições anteriormente defendidas, solidificando assim estes 3 critérios cumulativos para a opção paga.

O TJUE não teceu este juízo em relação a um responsável pelo tratamento qualquer, em relação a um simples serviço digital, mas em

[129] Ver para. 147-148 da decisão.
[130] Ver para. 149 da decisão.
[131] Ver os para. 150 e 151.
[132] Ver para. 151.

relação a uma das maiores empresas e a um dos serviços mais influentes no mundo e no mercado único digital europeu (sendo que questões de concorrência foram até consideradas no mesmo caso). A Meta já tinha sido designada em abril[133] pela Comissão Europeia como fornecedora de plataformas em linha de muito grande dimensão ("*Very Large Online Platform* – VLOPs") para efeitos do Regulamento dos Serviços Digitais[134]. Uns meses depois da decisão, para surpresa de absolutamente ninguém, a Meta foi também designada como controlador de acesso (*Gatekeeper)*[135] e os seus serviços como serviços essenciais de plataforma (*core services)*[136] no âmbito do Regulamento dos Mercados Digitais[137].

A fasquia não podia ter sido colocada mais alta. O TJUE com esta decisão admitiu que modelos de "*consent or pay*" que sigam os critérios indicados (o que nos parece que seja o problema da Meta em concreto), serão admissíveis, mesmo para os casos dos fornecedores privados de serviços digitais de maior dimensão possível, onde o desequilíbrio entre titular de dados e responsável pelo tratamento dificilmente poderia ser maior.

---

[133] Comissão Europeia, "Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines", 25 abril 2023, disponível em https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413 e https://ec.europa.eu/newsroom/dae/redirection/document/101005

[134] 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)

[135] Comissão Europeia, "Digital Markets Act: Commission designates six gatekeepers", 6 setembro 2023, https://ec.europa.eu/commission/presscorner/detail/en/IP_23_4328 e https://digital-markets-act.ec.europa.eu/gatekeepers_en

[136] Para ver as decisões, disponível em https://ec.europa.eu/competition/digital_markets_act/cases/202346/DMA_100044_138.pdf

[137] Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho de 14 de setembro de 2022 relativo à disputabilidade e equidade dos mercados no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828 (Regulamento dos Mercados Digitais)

5. O escrutínio do modelo "*Pay or Okay*" ou "*Consent or Pay*"

5.1 O caso Meta

E assim chegamos ao momento mais recente desta saga: as queixas das ONG às autoridades de controlo nos vários Estados-Membros e a consulta do EDPB.

A NOYB ("*Non-of-your-business"*)[138] é a ONG focada nos direitos digitais e privacidade que mais reclamações e ações judiciais tem colocado contra a Facebook/Meta, desafiando repetidas vezes a validade e legitimidade do seu modelo de negócio.

Se analisarmos o historial das ações entre ambos, conseguimos traçar um fio condutor de diferentes "testes" à validade da utilização de diferentes bases de licitude do tratamento de dados pessoais, desde o consentimento "dissimulado", interesses legítimos e a necessidade para a execução do contrato.

Logo na entrada em vigor do RGPD, em maio de 2018, a NOYB apresentou uma queixa à autoridade de controlo austríaca contra o alegado consentimento "forçado" que o Facebook impunha ("*take it or leave it*") aos seus utilizadores para a publicidade personalizada[139]-[140]. O Facebook tinha alterado os seus termos e condições de forma a poder afirmar quer este tratamento de dados era necessário para o cumprimento do contrato, tentando usar assim o art. 6.º n.º 1 alínea b) para a publicidade personalizada.

No seguimento desta queixa, o processo arrastou-se durante vários anos, conhecendo várias reviravoltas. A autoridade de controlo irlandesa (que demorou mais de 4 anos a investigar o caso) apresentou um

---

[138] Para mais informações sobre a NOYB, consulte as FAQs no seu site: https://noyb.eu/en/faqs

[139] NOYB, "noyb.eu filed complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook", 25 maio 2018, disponível em https://noyb.eu/en/noybeu-filed-complaints-over-forced-consent-against-google-instagram-whatsapp-and-facebook

[140] A reclamação da NOYB em questão está disponível em https://noyb.eu/sites/default/files/2020-05/complaint-facebook.pdf

projeto de decisão inicialmente favorável à Facebook, mas o procedimento foi remetido para o EDPB. Entretanto foram publicadas as Diretrizes 2/2019 do EDPB sobre os limites do art. 6.º n.º 1 alínea b) como base de licitude de tratamento no contexto dos serviços digitais.

Em dezembro de 2022, quanto à disputa submetida pela autoridade irlandesa e a Meta, o EDPB proferiu duas decisões vinculativas[141]-[142] ao abrigo do art. 65.º, confirmando o sentido das queixas, que o art. 6.º n.º1 alínea b) não seria uma base de licitude válida para os serviços. A Meta ficou assim permanentemente banida de continuar com esta prática. A subsequente decisão da autoridade irlandesa[143] foi assim vista como uma vitória (mas não completa para a NOYB[144]-[145]).

Durante o ano de 2023, a Meta anuncia uma nova tática, mudar a base de licitude da execução do contrato para os interesses legítimos[146]-[147]. Porém, esta decisão não sobreviveu muito tempo. Além

---

[141] EDPB, "Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR)", disponível em https://www.edpb.europa.eu/system/files/2023-01/edpb_bindingdecision_202203_ie_sa_meta_facebookservice_redacted_en.pdf

[142] EDBP, "Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR)", disponível em: edpb_binding_decision_202204_ie_sa_meta_instagramservice_redacted_en.pdf (europa.eu)

[143] Data Protection Commission, Decision Facebook 31st day of December 2022 https://noyb.eu/sites/default/files/2023-01/DPCDecision_Facebook.pdf

[144] NOYB, "BREAKING: Meta prohibited from use of personal data for advertising", Janeiro 2023, disponível em https://noyb.eu/en/breaking-meta-prohibited-use-personal-data-advertising

[145] NOYB, "Meta Advertising Ban – Decision Published", Janeiro 2023, disponível https://noyb.eu/en/meta-advertising-ban-decision-published

[146] Natasha Lomas, "Meta tries to keep denying EU users a free choice over tracking – but change is coming", março 2023, disponível em https://techcrunch.com/2023/03/30/meta-facebook-gdpr-ads-tracking/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2x-lLmNvbS8&guce_referrer_sig=AQAAABtULgAOtUhH7QmkN7Mb2_k2C1UB4PGMrXiqXCAwuAP3J-tIxatl8FGxYg3YQccVtbBO8mkbicec5IRrQx4gBsGEUVgWgZh4Kkl0Yu-nlaszXSz5XdaB2Z_n3ma7h3I_jyCmUNSXDPBFpQXOvDJR2cJCHCH7hi0mo-TcT8SNdSL6g

[147] "(…) for the purpose of serving behavioural advertisements in Europe (…) we are changing the legal basis that we use (…) from 'Contractual Necessity' to 'Legitimate Interests'" in Meta, "How Meta Uses Legal Bases for Processing Ads in the EU", versão de 30 de março 2023, posteriormente alterada. A consulta é possível utilizando a wayback machine, com a hiperligação: https://about.fb.com/news/2023/01/how-meta-uses-legal-bases-for-processing-ads-in-the-eu/

da decisão C-252/21 do TJUE, que já abordámos, em outubro o EDPB emite uma decisão vinculativa urgente (01/2023)[148] a pedido da autoridade de controlo norueguesa, declarando que as operações de tratamento de dados para a publicidade personalizada não se podiam basear nos interesses legítimos art. 6.º n.º 1 alínea f) nem na execução do contrato, alínea b). Esta combinação veio a colocar o modelo da Meta numa verdadeira encruzilhada.

É neste ponto que a Meta admite assim, finalmente, mudar a sua base de licitude para o consentimento[149]. No entanto, como sabemos, há um *caveat*…

Como foi explicado na introdução, a Meta decidiu adotar um modelo de "*Consent or Pay*" ou "*Pay or Okay*", de permitir aos utilizadores-titulares de dados a possibilidade de optar entre conferirem o consentimento ou efetuarem pagamentos mensais monetários de forma a manterem o acesso aos serviços.

Como referido na introdução, a NOYB apresentou a sua queixa, atacando o modelo empregue pela Meta, como sendo uma forma de iludir o RGPD. A NOYB refere que o consentimento ao *tracking* e à publicidade personalizada não pode ser considerado livre quando, para ambos os serviços da Meta, a alternativa tem um custo que por titular pode chegar aos 251,88€ por ano. Segunda a NOYB, estes valores contrastam de forma com os relatórios de contas da Meta, que, para os seus acionistas, estima que o valor gerado mensalmente pela publicidade por utilizador seja de 16,79 dólares americanos na Europa[150].

Adicionalmente, a NOYB afirma que vários estudos indicam que embora apenas uma pequena maioria queira publicidade personalizada,

---

[148] EDPB, "Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR)", outubro 2023, https://www.edpb.europa.eu/system/files/2023-12/edpb_urgentbindingdecision_202301_no_metaplatformsireland_en_0.pdf

[149] Dan Milmo, "Meta to ask EU users' permission to show targeted advertising", Agosto 2023, disponível em https://www.theguardian.com/technology/2023/aug/02/meta-to-ask-eu-users-permission-to-show-targeted-advertising-facebook-instagram

[150] NOYB, "noyb files GDPR complaint against Meta over "Pay or Okay"", novembro 2023, disponível em https://noyb.eu/en/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay

cerca de 99,9% dos titulares aceitam esta opção quando confrontados com o pagamento de um custo de 1,99€.

Finalmente, a NOYB afirma que, caso a Meta tenha sucesso, outros prestadores de serviços (como o Tiktok) inevitavelmente vão seguir o exemplo. O efeito de múltiplas aplicações a pedirem o pagamento de subscrições mensais pode resultar em despesas de vários milhares de euros por individuo. Para as famílias, o custo pode chegar aos 35,000€ anuais, o que é, naturalmente, um preço absolutamente proibitivo para um direito fundamental. A privacidade torna-se num privilégio dos ricos[151].

Depois desta, a NOYB ainda apresentou mais uma queixa já em 2024, afirmando que o sistema da Meta cria dificuldades no procedimento de retirada do consentimento, devido não só ao facto de que são obrigados a passar para a opção paga, como têm de passar por múltiplas páginas e pop-ups até o conseguirem, em clara violação do art. 7.º n.º 3 RGPD[152]. Esta queixa, digamos, é significativamente mais direta e *straightforward* que a primeira, seja praticamente incontornável para a Meta.

A BEUC, na sua queixa, optou por uma estratégia assente no Direito do Consumo Europeu[153], recorrendo à Diretiva das Cláusulas Contratuais Abusivas e à Diretiva das Práticas Comerciais Desleais. Na sua queixa, a BEUC (e o consórcio de associações de defesa dos direitos dos consumidores que representa) alega que o mecanismo de bloquear parcialmente o uso do Facebook e do Instagram até que os utilizadores tenham selecionado uma das opções, constitui uma prática comercial agressiva. Através da persistência e da criação de uma sensação de urgência, a Meta força os consumidores a tomar uma decisão

[151] NOYB, "noyb files GDPR complaint against Meta over "Pay or Okay"", novembro 2023.

[152] NOYB, "Meta ignores the users' right to easily withdraw consent", Janeiro 2023.

[153] BEUC, "Choose to lose with Meta – An assessment of Meta's new paid-subscription modelfrom a consumer law perspective", novembro 2023, disponível em https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-156_Annex_Legal%20assessment_Choose_to_lose_with_Meta_Legal_analysis.pdf

que pode ir contra a sua vontade, sem lhes sequer possibilitar tempo de reflexão[154].

A Meta fornece informações incompletas e enganosas aos consumidores que não lhes permitem fazer uma escolha informada. A empresa apresenta ainda a escolha como sendo entre uma opção paga e uma opção "gratuita", mas esta última opção não é realmente gratuita, pois os consumidores acabam por pagar à Meta com os seus dados pessoais.

Finalmente, devido ao enorme poder que a Meta detém no mercado e devido ao network *effect* das redes sociais, os consumidores não têm verdadeira uma escolha, já que deixar esses serviços resultaria na perda de todos os seus contatos e interações construídas ao longo dos anos. O valor elevado da subscrição "sem anúncios" é desencorajador para os consumidores, o que significa que não têm realmente uma escolha livre.

5.2 Outros casos anteriores de *Consent or Pay*, *Cookie Walls* e *Paywalls*

Este tipo de modelos não é novo, tendo até se popularizado bastante durante o verão de 2023, especialmente na Alemanha. Um dos maiores sites de notícias *tech*, o heise.de, adotou precisamente este modelo, enquanto na Áustria, outro site de notícias, o derStandard.at, fez o mesmo.

Em ambos os casos, a prática foi considerada ilícita.

No caso derStandard, a cookie banner que bloqueava o acesso aos conteúdos exigia o consentimento para simultaneamente publicidade personalizada e *data sharing* (com cerca de 125 entidades terceiras) ou o pagamento de uma mensalidade, que poderia resultar em 96 € anuais. A prática foi considerada ilícita a 29 de abril 2023 pela autoridade

[154] BEUC, "Consumer groups file complaint against Meta's unfair pay-or-consent model", novembro2023,disponívelemhttps://www.beuc.eu/press-releases/consumer-groups-file-complaint-against-metas-unfair-pay-or-consent-model

controlo austríaca, devido à falta de granularidade do consentimento, e, portanto, sujeita a uma coima[155]-[156].

No caso heise.de também era utilizado um modelo "*pay or consent*" através da sua *cookie banner*, que tratava dados pessoais para múltiplas funcionalidades além da publicidade, incluindo a partilha de dados com terceiros. A autoridade de controlo da Baixa Saxónia (*Lower Saxony*) conclui que houve múltiplas violações do RGPD, desde o tratamento de dados com a instalação de cookies se iniciar imediatamente assim que o utilizador visitava o site pela primeira vez, incumprimento de deveres de informação, *dark patterns* na obtenção do consentimento que não respeitava a granularidade, etc. O custo da opção paga não foi considerado como um fator nesta decisão[157].

O caso dinarmaquês do GulogGratis, em que autoridade de controlo considerou que o modelo de "*consent or pay*" do *marketplace* GulogGratis era parcialmente válido. O consentimento era recolhido para o tratamento de dados com a finalidade de publicidade personalidade e fins estatísticos. Apenas a recolha de dados para fins estatísticos é que foi considerada problemática por não estar devidamente justificada/não ser necessária e o consentimento não cumprir com a granularidade quanto a esta finalidade[158]-[159].

A Conferência das Autoridades Independentes de Controlo da Proteção de Dados da Alemanha ("*Konferenz der unabhängigen Datenschutzaufsichtsbehörden*" que inclui todas as autoridades de controlo dos vários *Lander*) publicou linhas de orientação em março de 2023 que permitem, em teoria, a validade de um modelo em que haja a

---

[155] Uma análise da decisão está disponível no GDPRhub, "DSB (Austria) – 2023-0.174.027", disponível https://gdprhub.eu/index.php?title=DSB_(Austria)_-_2023-0.174.027

[156] A decisão original, em alemão, disponível em https://noyb.eu/sites/default/files/2023-04/Standard_Bescheid_geschw%C3%A4rzt.pdf

[157] Decisão original em alemão, disponível em https://noyb.eu/sites/default/files/2023--07/11VerwarnungPurAboModellfinalgeschwrztp_Redacted.pdf

[158] Resumo da decisão no GDPRhub disponível em https://gdprhub.eu/index.php?title=Datatilsynet_(Denmark)_-_2021-31-4871

[159] Versão original em dinarmaquês disponível em https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/feb/gul-og-gratis-brug-af-cookie-walls

opção de pagamento de uma subscrição mensal em alternativa ao pagamento[160]. Segundo este documento, os modelos serão admissíveis se

a) Ambas as opções entre o serviço pago ou com consentimento forem alternativas equivalentes.
b) O custo for o standard do mercado.
c) No caso de serem efetuadas múltiplas operações de tratamento de dados com finalidades substancialmente distintas, os requisitos do consentimento (segundo as Diretrizes 05/2020 do EDPB), têm de ser respeitados, nomeadamente a granularidade. Os titulares de dados não podem ser obrigados a fornecer o seu consentimento a um "*bundle*", devem ter a opção de consentir de forma separada consoante as finalidades (modelo de *opt-in*).

Em França, encontramos um entendimento similar após uma tentativa de proibição de cookie walls pela CNIL[161]. Na sequência de uma ação proposta por parte de associações da indústria, especialmente editores de imprensa e de meios de comunicação, o Conseil d'État emitiu uma decisão em 19 de junho de 2020[162] que determinou que a CNIL não poderia impor esta proibição total. O tribunal enfatizou que a obtenção de consentimento gratuito para o processamento de dados deve ser avaliada caso a caso, considerando diversas situações e contextos.

Como resultado, a CNIL reviu as suas diretrizes de cookies em setembro de 2020[163], admitindo que a validade das *cookies walls* ou

---

[160] "Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 22. März 2023 Bewertung von Pur-Abo-Modellen auf Websites" março 2023, disponível em: https://www.datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf

[161] Deliberation no. 2019-093 of 4 July 2019 adopting guidelines on the application of Article 82 of the amended Act of 6 January 1978 to read and write operations on a user's terminal (in particular "cookies and other tracers")

[162] Décision n° 434684 du Conseil d'Etat du 19 juin 2020, 10ème et 9ème Chambres réunies https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-06-19/434684

[163] Deliberation no. 2020-091 of 17 September 2020 adopting guidelines on the application of Article 82 of the amended Act of 6 January 1978 to read and write operations on a user's terminal (in particular "cookies and other tracers") and repealing deliberation no. 2019-093 of 4 July 2019

paywalls em relação ao requisito de liberdade de consentimento. Este deve ser avaliado caso a caso, atendendo aos seguintes critérios:

a) Oferecer uma alternativa justa à aceitação de cookies;
b) Fornecer um serviço equivalente pelo mesmo prestador;
c) Definir um preço razoável para as alternativas;
d) Limitar os propósitos dos cookies apenas aos que são justificados.

Em relação a cookie walls, as autoridades de controlo de Espanha[164] e Itália[165] também têm seguido esta tendência decisória, com linhas de orientação e diretrizes similares.

5.3 As previsões na antecipação da Opinion 8/2024 do EDPB

Atendendo às posições que defendemos anteriormente quanto aos dados como contraprestação na DCD e na Diretiva *Omnibus*, é do nosso entendimento que é possível, em teoria e (com algumas dificuldades) na prática, utilizar o consentimento como base de licitude que condiciona o acesso a conteúdos e serviços digitais. A análise deverá sempre ser feita de forma casuística, atendendo ("com a máxima atenção") à justificação apresentada para cada tratamento de dados e a sua finalidade, e permitindo a granularidade do consentimento. Certos tratamentos de dados serão considerados mais ou menos "abusivos" ou excessivos, consoante o contexto de cada serviço digital.

Esta construção e raciocínio são, naturalmente, aplicáveis aos modelos de *consent or pay*, sejam eles baseados em *cookie walls* ou *paywalls*. As objeções que são frequentemente colocadas à

[164] AEPD, Guía sobre el uso de las cookies, 2024, disponível em https://www.aepd.es/guias/guia-cookies.pdf Depois da publicação da Opinion 8/2024 do EDPB, a AEPD alterou este guia, mas ainda é possível encontrar a versão que permite a utilização de modelos pay or consent utilizando a wayback machine e consultando versões do webiste de fevereiro de 2024. Como exemplo, ver http://web.archive.org/web/20240213234318/https://www.aepd.es/guias/guia-cookies.pdf

[165] Garante, "Guidelines on the use of cookies and other tracking tools – 10 June 2021", 2021, disponível em https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876#english

admissibilidade destes modelos focam-se em erros, falhas e abusos dos casos concretos – por exemplo, no caso concreto da Meta, levantam-se sérias dúvidas quanto ao preço (até que ponto é que será "remuneração adequada"), a forma como as informações são apresentadas e o consentimento recolhido (poderão constituir uma prática comercial desleal pelo uso de "grátis" e o carácter abusivo, intrusivo e agressivo) e as dificuldades práticas na retirada do consentimento.

Devido a isto, consideramos que a ação coordenada pela Comissão, liderada pela Direção-Geral da Concorrência, do Consumo e da Repressão da Fraude da França, levada a cabo no seguimento das queixas apresentadas pela BEUC e o seu consórcio[166], com base nas violações do Direito Europeu do Consumo, eram a abordagem mais "forte" e com melhores possibilidades de sucesso.

Ainda assim, mesmo considerando a tendência decisória em proteção de dados até abril 2024[167], das autoridades de controlo à jurisprudência do TJUE, as principais previsões (com que alinhávamos) apontavam para que o resultado mais provável fosse que o EDPB adotasse uma posição bastante mais conservadora, que colocasse mais enfâse nos requisitos e salientasse o carácter excecional da admissibilidade do consentimento nestes casos, possivelmente propondo alternativas.

Estas previsões atendiam ao facto da decisão se focar nas práticas no contexto das plataformas online de muito grande dimensão (e mesmo *gatekeepers*), referindo que o mais provável era que o EDPB apontasse várias problemas, que na prática poderiam colocar constituir entraves de tal forma que o resultado fosse que estes modelos não sejam tendencialmente admissíveis – abrindo a porta, no entanto que outros prestadores de serviços possam implementar este modelo, seguindo as recomendações redobradas.

---

[166] Comissão Europeia, Commission coordinates action by national consumer protection authorities against Meta on 'pay or consent' model", 22 julho 2024, disponível em https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3862

[167] Como analisámos na secção anterior.

Caso o EDPB opte por uma postura excessivamente mais "puritana", em que feche de tal forma a "porta" a inviabilizar de todo modelos "*consent or pay*" em plataformas de muito grande dimensão como a Meta (seja por pressões políticas ou quaisquer outras motivações dos seus membros), é necessário relembrar que tal orientação entra em choque direto com a jurisprudência do TJUE em C-252/21. Uma decisão nesta linha teria várias implicações.

Devido à diversidade de previsões e as grandes implicações das mesmas, nas vésperas da decisão houve um "turbilhão" de apelos de ambos os lados[168].

5.4 A Opinion 08/2024 on Valid Consent

O EDPB emitiu a sua decisão sobre os modelos "Consent or Pay" em 17 de abril de 2024. Quando comparado com as previsões feitas até aí, o EDPB foi bastante mais longe que o esperado.

A decisão é bastante extensa, em 42 páginas e aborda diversas questões e matérias que requerem, por sua vez, uma análise muito aprofundada. Neste espaço vamos apenas apontar as principais questões[169].

O EDPB concluiu que, na generalidade dos casos em que os utilizadores de grandes plataformas sejam apenas confrontados com uma escolha binária entre consentirem a publicidade personalizada e pagarem uma mensalidade, que o consentimento não seria válido.

---

[168] Ver as cartas da IAB Europe, a defender a admissibilidade dos modelos, e do lado oposto, da aliança liderada pela EDRI: https://iabeurope.eu/wp-content/uploads/20240319-Letter-to--EDPB-upcoming-opinion-and-guidelines-on-the-consent-or-pay-model.pdf e https://edri.org/wp-content/uploads/2024/04/NGOs-Letter-Pay-or-Consent-April-2024.pdf

[169] Para mais análises ver Arthur Cox, "White Paper Critical Analysis Of The European Data Protection Board's Opinion 08/2024 On Consent Or Pay Models" 1719315867013 (licdn.com), José Antonio Castillo Parrilla, Jorge Morais Carvalho, "'Pay or ok'. Pagar con datos personales tras la Directiva 2019/770: una visión comparada entre España y Portugal" RED Revista Electrónica de Direito 2024, Vol. 34 (2), DOI 10.24840/2182-9845_2024-0002_0007. Peter Craddock, Op-Ed: A critical analysis of the EDPB's "Pay or Consent" Opinion", em https://www.linkedin.com/pulse/op-ed-critical-analysis-edpbs-pay-consent-opinion-peter-craddock-obl3e/

Para sustentar esta conclusão, o EDPB navega sobre as principais questões relevantes para o consentimento. Este deve respeitar todos os requisitos do RGPD, sublinhando o princípio da responsabilidade, da necessidade, proporcionalidade, limitação de finalidades, minimização de dados e lealdade.

Além dos requisitos da informação, granularidade e especificidade, foca-se bastante no consentimento ser livre e de analisar o impacto do desequilíbrio de poder entre o responsável pelo tratamento e os titulares. Aqui destaca a posição de mercado da plataforma, o network effect, a dependência do serviço (por exemplo, para fins profissionais) e o público-alvo.

Os titulares não são assim capazes de realizar uma escolha genuína e livre, pois se não aceitarem consentir ao tratamento de dados para a publicidade personalizada, podem sofrer prejuízos, seja pela perda de acesso ao serviço de que estão dependentes, ou pelos custos financeiros da opção paga.

Com base nestas considerações, o EDPB fecha a porta à admissibilidade da escolha binária entre consentimento e pagamento. No entanto, a decisão acrescenta ainda uma série de recomendações que poderiam "salvar" o consentimento, permitindo que este possa ser válido.

Além de medidas como reforçar a transparência e compreensão das operações de tratamento, facilitar a retirada do consentimento (e a possibilidade de implementar um modelo em que este tenha de ser renovável!), e assegurar a granularidade ao invés da agregação de tratamentos distintos, o EDPB foca uma parte considerável da decisão numa proposta extraordinariamente inovadora: uma terceira alternativa equivalente gratuita, sem tratamento de dados para publicidade personalizada ("*Free Alternative Without Behavioural Advertising*" também conhecida como FAWBA).

Segundo o EDPB, para os responsáveis pelo tratamento que prestam serviços que tratam dados para personalidade personalizada assegurarem que os titulares de dados conseguem fazer uma escolha genuína e livre, devem também oferecer esta alternativa equivalente que seja verdadeiramente gratuita, FAWBA, em que haja bastante menos ou

nenhum tratamento de dados pessoais. Neste modelo, a publicidade não pode ser personalizada, só pode ser contextual, geral ou baseada em tópicos escolhidos previamente pelo titular de uma lista. Só com esta opção adicional é que se consegue assegurar a liberdade de escolha ("a real choice") do titular.

5.5 Principais críticas à decisão do EDPB

Embora vários celebrassem a decisão do EDPB, como a NOYB (que ainda assim considerou que a decisão podia ter sido assertiva), rapidamente começaram a surgir muitas críticas sobre a decisão do EDPB devido a várias partes da decisão.

Em primeiro lugar, o EDPB cunha um novo conceito, extremamente inovador para o Direito Europeu, o de grandes plataformas em linha ("*large online platforms*"). Embora tenha sido chamar a pronunciar-se sobre o modelo da Meta, o EDPB decide expandir o escopo da sua decisão. Além das plataformas de muito grande dimensão (VLOPs) do DSA e dos controladores de acesso do DMA, o EDPB decide que a decisão também se deve aplicar a outras plataformas que, embora não cumpram os requisitos do art. 33.º DSA, sse encaixem neste novo conceito de grande plataforma. Segundo o EDPB, é necessário uma análise casuístca que considere a presença (indicativa) de elementos como: tem um grande número de titulares de dados, se tem uma posição considerável no mercado relevante, se realiza operações de tratamento de grande escala, a sua escala geográfica, entre outros.

O EDPB cria assim um novo conceito de "VLOP" para o RGPD, com uma definição pouco clara, elástica e adaptável a um grande volume de casos, que ultrapassam muito o caso da Meta, e cria bastante incerteza jurídica.

O EDPB já tinha comunicado anteriormente em fevereiro que iria preparar guidelines para serviços de menor dimensão das grandes plataformas, que utilizassem este modelo. Ao revisitar este comunicado, compreendemos que a utilização de "grandes plataformas" não se referia apenas aos serviços equivalentes à Meta, mas a um universo muito

maior. A fronteira entre os serviços que caem na Opinion 8/2024 e os das futuras guidelines é incerta e difusa.

A criação desta categoria não encontra base jurídica em na ordem jurídica, não está no RGPD, no DSA, no DMA, no Data Act ou Data Governance Act, etc., e afasta-se da prática decisória das autoridades de controlo e do TJUE.

A decisão põe severamente em causa a aplicação harmoniosa entre o RGPD e DCD, assim como a Diretiva Omnibus, ignora a aplicação da Diretiva da Privacidade, e é diretamente imcompatível com várias decisões do TJUE, em especial o acórdão C-252/21. O EDPB gasta uma parte considerável da sua decisão a "tentar reescrever-reinterpretar--corrigir" esta decisão.

A proposta da FAWBA deve ser destacada como o ponto mais frágel e absolutamente criticável da decisão. Em momento nenhum o TJUE afirmou que esta "terceira" alternativa era necessária, tendo antes sido bastante claro quanto à admissibilidade de um única alternativa equivalente ao consentimento que fosse paga.

Ao exigir esta "terceira" alternativa equivalente para que as outras (consentimento e pagamento) sejam admissíveis, o EDPB não está apenas explicitamente a violar o precedente do TJUE, está também a violar as suas competências e a separação dos poderes.

Esta postura do EDPB e das suas autoridades de controlo pode ser vista como uma verdadeira tentativa destes reguladores/supervisores de tentarem legislar, sem competência para tal, de forma a procurar "corrigir" a orientação do TJUE.

Ora, o RGPD não proíbe a publicidade personalizada (se devia, ou não, devido aos seus múltiplos efeitos nocivos para a sociedade, é toda outra questão) nem o modelo de negócio subjacente. O EDPB e os seus membros não têm competência, um mandato democrático, para decidir tal matéria[170].

---

[170] Assumindo veemente esta posição e altamente crítico de posições de "overreach" das autoridades de controlo, Martin Nettesheim, "GDPR Overreach? The Challenges of Regulating Pay--or-Consent Models through Data Protection Law", VerfBlog, 2024/4/15, https://verfassungsblog.de/gdpr-overreach/ DOI: 10.59704/de7ffdfea30b45f1.

Mas exigir FAWBA é uma proibição do modelo de publicidade personalizada? Sim, consubstancia o mesmo resultado. Dado que não podem condicionar o acesso ao serviço com o requisito do consentimento para estas operações de tratamento só por si, nem com alternativa paga adicional, os prestadores dos serviços ficam obrigados a garantir que o serviço tem de ser prestado de forma gratuita, com a qualidade equivalente ao serviço pago.

Na prática, uma esmagadora maioria dos consumidores irão optar[171] pela opção gratuita, sem qualquer prejuízo. Ora, isto irá implicar o fim do modelo de negócio destes serviços. De um prisma contratual, quase que será possível apontar que os titulares de dados poderão se encontrar numa posição de enriquecimento sem causa: vão usufruir de serviços sem terem realizado qualquer contrapartida[172].

Este aspecto terá mais efeitos que, de forma, poderão acabar a afetar negativamente os titulares de dados. A exigência da FAWBA pode implicar que estes prestadores mudem para um modelo com uma única opção: o pagamento monetário. De repente, milhões de titulares de dados deixarão de ter acesso aos serviços digitais que pretendem usufruir porque a versão com publicidade personalizada sem pagamento deixou de estar disponível. Foram negativamente afetados. para o bem deles. Porque não eram capazes de prestar o consentimento de forma admissível.

Mesmo admitindo que algumas destas "grandes plataformas" realizem a transição para um modelo gratuito, será que são capazes de sobreviver a isso? Estarão dispostas a isso? E porquê?

Estas questões apontam para dois temas. Em primeiro, a crítica mais frágil da decisão, que o EDPB estava perante um conflito de

---

[171] Serão poucos os titulares de dados bondosos que irão aceitar fornecer os seus dados pessoais para se submeterem a publicidade e serão ainda menos os que aceitam pagar uma mensalidade. Não é arriscado afirmar que aqueles que não optem pela FAWBA provalvelmente estivam distraídos ou a ser manipulados por dark patterns (também já proibidos no DSA).

[172] José Antonio Castillo Parrilla e Jorge Morais Carvalho, ""Pay or ok". Pagar con datos personales tras la Directiva 2019/770: Una visión comparada entre España y Portugal", RED Vol. 34(2) 2024, pp. 128-131 e 136-140.

direitos fundamentais e que desconsiderou completamente esta questão. O EDPB analisou a questão unicamente considerando o direito fundamental à proteção de dados, art. 8.º CDFUE, e ignorou a liberdade das empresas, protegido como direito fundamental no art. 16.º da CDFUE. Mesmo que consideremos que os direitos das pessoais individuais naturais sejam, naturalmente, mais merecedoras de proteção, a verdade é que o próprio RGPD reconhece que a proteção dos dados pessoais não é um direito absoluto[173].

Numa situação de conflito entre estes, em que o EDPB pretende, sem base jurídica, contradizendo o TJUE, reescrever uma parte considerável do ordenamento jurídico europeu para proibir um modelo de negócio já bastante implantado e disseminado na economia moderna e na sociedade atual, é difícil não referir que este ponto também foi ignorado, talvez com a consequência a solução mais equilibrada e mais acertada.

O último ponto é menos uma crítica da decisão, mas uma reflexão que surge apartir desta e requer que seja feita aprofundada noutro texto. Se queremos, enquanto sociedade democrática, que opções como o FAWBA sejam a regra/que a publicidade personalizada seja proibida, temos de estar preparados para as consequências dessa decisão. Isto inclui realizar as escolhas posteriores necessárias.

Se, por exemplo, quisermos que as redes sociais e grandes plataformas digitais sejam gratuitas (no sentido completo) e que se mantenham em funcionamento devido ao seu papel, seja na liberdade de expressão, no acesso a informação, como as "*townsquares* digitais da nossa sociedade", então temos de reconhecer o seu papel enquanto serviços essenciais – isso implica escolhas como perceber qual o modelo de governança e financiamento que queremos para estes serviços.

---

[173] Considerando 4 do RGPD.

5.6. Implicações futuras

Finalmente, temos de compreender quais as implicações futuras desta decisão.

O principal resultado da Opinion 08/2024 será muita litigância. As autoridades de controlo vão tentar aplicar coimas à Meta, sendo que esta vai sempre contestar judicialmente a sua validade. Em paralelo também vão ainda decorrer, quem sabe, ações colocadas pela NOYB e outras ONG, que poderão até ser ações coletivas com base nas transposições da Diretiva 2020/1828. No Direito do Consumo, já referimos que a ação coordenada entre as autoridades de consumo, baseada nas queixas da BEUC, parecem muito auspiciosas, com probabilidade de sucesso.

Tanto os processos de *public* e *private enforcement* nestas matérias vão resultar em reenvios prejudiciais para o TJUE, que irá, "certamente", procurar encerrar esta questão "de vez" (tudo isto num horizonte de 2-3 anos).

Além desta litigância, tudo indica que a Comissão Europeia irá também utilizar outras as ferramentas disponíveis, em especial o art. 5.º do DMA[174]-[175], para apertar o cerco à Meta. Os problemas da granularidade do consentimento e junção dos dados do Facebook e do Instagram são particularemente difíceis de defender.

Quanto guidelines que devesão publicadas no último trismetre de 2024, aplicáveis aos serviços que não alcançam a classificação de "large online platforms", há ainda muita incerteza quanto ao seu conteúdo. É possível que não exijam FAWBA, mas também é possível que sim. Até conhecermos o seu conteúdo, afirmamos novamente que estas não

---

[174] Comissão Europeia, "Commission sends preliminary findings to Meta over its "Pay or Consent" model for breach of the Digital Markets Act", Julho 2023, https://digital-markets-act.ec.europa.eu/commission-sends-preliminary-findings-meta-over-its-pay-or-consent-model-breach-digital-markets-act-2024-07-01_en

[175] Marco Botta e Danielle Borges, "User Consent at the Interface of the DMA and the GDPR. A Privacy-setting Solution to Ensure Compliance with ART. 5(2) DMA", Dezembro 2023. Robert Schuman Centre for Advanced Studies Research Paper No. 2023_68, Available at SSRN: https://ssrn.com/abstract=4650373 or http://dx.doi.org/10.2139/ssrn.4650373

poderão contradizer frontalmente a *rationale* do TJUE e a posição que defendemos neste texto sem sofrerem de graves falhas.

6. Conclusão

Do ponto de vista económico, é possível observar várias transformações ao longo dos anos nos modelos de negócio de diversos serviços digitais (e dos que estão a fazer a transição para o digital, como a imprensa e o jornalismo), em especial no que toca com a relação com a publicidade personalizada e o pagamento de subscrições mensais.

Algumas plataformas de partilha de conteúdos digitais criados pelos utilizadores (*User-generated content*, conhecido como UGC), como o Youtube, estão há vários anos a promover opções pagas sem anúncios (e alguns conteúdos *premium*) junto dos seus utilizadores, porém com reduzido sucesso. Outros, como os serviços de streaming de vídeo (Netflix, Disney+, e muitos outros concorrentes), que começaram sem quaisquer anúncios, estão agora no processo de aumentar a generalidade dos seus preços[176], criando "*tiers*" de subscrição com mensalidades mais baixas, onde, porém os utilizadores são confrontados com anúncios, tipicamente personalizados. No *streaming* de música e podcasts, muitos utilizadores também já estavam familiarizados com este modelo no *Spotify*, assim como no *streaming* de videojogos, com o *Twitch*.

A imprensa, o "quarto poder" em democracias, confrontado com quebras contínuas de receitas e de recursos, tem experimentado com ambos os modelos, em separado e de forma híbrida.

Não é aparente que haja um modelo que seja necessariamente mais viável que o outro, depende muito do caso concreto, do serviço, do mercado, da marca, e mesmo de *trends* macroeconómicas (relembrando a

[176] Sobre as mudanças no mercado de streming, ver Martim Farinha, "A Mudança De Planos Da Netflix – Como Se Chegou Até Aqui?", março 2023, https://novaconsumerlab.novalaw.unl.pt/tag/netflix/

forma como diferentes modelos prosperaram ou caíram em desgraça na *Dot-com bubble*, na recessão de 2008, durante a década dos 2010s, durante os confinamentos da covid-19, no pico de infração, etc.).

Independentemente da escolha do modelo de negócio pelo profissional-responsável pelo tratamento, entre optar pela publicidade personalizada ou o pagamento de subscrições, a realidade é que estes serviços têm de ser "pagos" de alguma forma.

Se considerarmos o caso do jornalismo, as editoras estão bastante dependentes da receita que consegue obter para cobrir os custos resultantes dos salários de jornalistas e funcionários, infraestrutura, armazenamento de dados, licenças, custos de investigação, etc. Sem publicidade personalizada e opções de "pagamento" dos utilizadores, estas empresas dificilmente sobreviveriam. Estes modelos pretendem assegurar que estes serviços são financeiramente viáveis.

Esta argumentação de escopo mais económico é apenas um complemento auxiliar da reflexão já realizada, mas que não pode ser esquecida.

Como demonstrámos ao longo do presente texto, a noção dos dados como contraprestação, por muito "desconforto" que possa causar, não só não é proibida pelos Tratados Europeus e pela Carta dos Direitos Fundamentais, como é compatível com os princípios e normas do RGPD, em especial o consentimento.

Os modelos de *paywall*, *ad-free subscription* ou "*consent or pay*" (conforme a denominação preferida) levantam questões quanto à validade do consentimento e a liberdade de escolha dos titulares, que são, como é possível aferir da prática decisória das autoridades de controlo e da jurisprudência do CJEU, acauteláveis na concretização prática.

Entre as considerações apontadas ao longo do texto para a obtenção de um consentimento válido, destacamos o carácter equivalente entre as diferentes versões dos serviços, o custo monetário da alternativa ser adequado, e ser assegurada a granularidade do mesmo. Adicionalmente, ainda que em certos casos não exista uma relação de consumo entre titular de dados e responsável pelo tratamento, é

recomendado que o modelo contratual, a política de privacidade e a própria forma como toda a informação é comunicada e o consentimento obtido, estejam em conformidade com os princípios da Diretiva das Cláusulas Contratuais Abusivas e a Diretiva das Práticas Comerciais Desleais. Estas medidas asseguram assim que não se levantam questões quanto ao possível carácter abusivo, enganador ou predatório do modelo – o que colocaria em causa a liberdade de escolha dos titulares de dados.

A recente Opinion 8/2024 do EDPB não veio a cumprir o objetivo de pacificar esta matéria e resolver as dúvidas interpretativas do RGPD. Pelo contrário, veio a criar muita incerteza jurídica seja pelo escopo da sua aplicabilidade (às "grandes plataformas em linha") e pelo seu conteúdo excessivamente criativo e inovador, sem base jurídica e contradizendo o TJUE.

Ao invés de esclarecer, esta decisão só veio a assegurar que a litigância irá continuar, que a atuação futura dos reguladores fique incerta[177] e que outros prestadores de serviços com uma dimensão nada comparável à Meta vejam os seus modelos de negócio colocados no limbo.

A privacidade não é "comprada" neste modelo, como muitos afirmam. Aliás, com base nos argumentos e recomendações que avançámos, acreditamos que seja possível prevenir a proliferação excessiva e abusiva destes modelos no futuro.

[177] A autoridade de Hamburgo terá aconselhado o jornal DER SPIEGEL a utilizar o modelo "consent or pay". Ver NOYB, "'Pay or OK' at DER SPIEGEL: noyb sues Hamburg DPA", Agosto 2024, https://noyb.eu/en/pay-or-ok-der-spiegel-noyb-sues-hamburg-dpa

Brain-computer interfaces and the decoding of thoughts as personal mental data[1]

Diogo Miguel de Brito Fonseca[2]

Resumo: A neurotecnologia é um campo em constante metamorfose que se encontra a redefinir a nossa compreensão do cérebro, principalmente através de Interfaces Cérebro-Computador (ICC) que permitem interpretar sinais elétricos ou modificar a atividade cerebral. Existindo o risco dos ICC poderem aceder à mente, e por consequência, ler pensamentos, o presente artigo pretende analisar esta questão à luz do Regulamento Geral de Proteção de Dados (RGPD). Na nossa opinião os pensamentos são Dados Mentais pessoais, com um elevado grau de sensibilidade, que devem ser tutelados pelo RGPD através da expansão do artigo 9.º deste regulamento pela decisão do Tribunal Europeu C-184/20.

Palavras-chave: *Dados Mentais; Interface Cérebro-Computador; Pensamentos; Regulamento Geral sobre a Proteção de Dados*.

Abstract: Neurotechnology is a field in constant metamorphosis that is redefining our understanding of the brain, mainly through Brain-Computer Interfaces (BCI) that makes it possible to interpret electrical signals or modify brain activity. Since there is a risk that BCI could access the mind and, consequently, read thoughts, this article aims to

[1] This reflection is the result of an academic work carried out under the supervision of Professor Maria da Graça Canto Moniz.

[2] Graduated in Law from the Faculty of Law of the University of Lisbon. Advanced Post-Graduation Course in Data Protection Law by Lisbon Centre for Research in Private Law. Master in Law with a specialization in Business Law and Technology from NOVA School of Law.
Contact: diogodebritofonseca@outlook.pt

analyse this issue in the light of the General Data Protection Regulation (GDPR). In our opinion, thoughts are personal Mental Data, with a high degree of sensitivity, which should be protected by the GDPR through the expansion of Article 9 of this regulation by European Court decision C-184/20.

***Key Words**: Brain-Computer Interfaces; General Data Protection Regulation; Mental Data; Thoughts*

1. Introduction

Most of the media examples, from the movie *The Matrix*[3] to *Inception*[4] and the series *Black Mirror*[5], generally paint a dystopian future for Brain Interface Technologies. They tell us a story of thought manipulation or behavioural mind control, a loss of humanness through an over reliance on technology, the ability for others to peer into our thoughts and memories or other dangerous effects when we express it in devices connected directly to our brains.

Since 2013[6], billions of euros have been allocated towards studying the human brain in the European Union, the United States of America and even China. This focus can be determined by the 'natural progression of behavioral studies that aim to demystify the unknown mechanisms behind the interaction of billions of neurons that make up the human brain'.[7] As there are at least a billion people on the planet who have

[3] Chicago. Wachowski, Lana, and Lilly Wachowski. 1999. The Matrix. United States: Warner Bros.

[4] Chicago. Nolan, Christopher. 2010. Inception. United States: Warner Bros.

[5] "The History of You", Black Mirror, Brian Welsh, Jesse Armstrong, season 1 episode 3, december 2011.

[6] Sten Grillner et al., "Worldwide Initiatives to Advance Brain Research," Nature Neuroscience 19, no. 9 (August 26, 2016): 1118–22. Available at: https://www.nature.com/articles/nn.4371.

[7] "Neurotechnologies: Connecting Human Brains to Computers and Related Ethical Challenges (ATP) – Policy Briefs & Reports – EPTA Network," (May 2019). Available at: https://eptanetwork.org/database/policy-briefs-reports/1792-neurotechnologies-connecting-human-brains-to-computers-and-related-ethical-challenges-atp.

disabilities,[8] it becomes a relevant opportunity to improve the lives of these people through technology capable of pursuing the interest of public and private health, however expensive research in the neuronal area, like for example Alzheimer's disease research,[9] may be.

'Neurotechnologies are emerging technologies that establish a connection pathway to the human brain through which human neuronal activity can be recorded and/or altered'[10] and are already being used, among others, to map brain regions related to different neuronal functions, to provide an image of the brain, and to repair its specific damaged areas.[11] These 'innovations have been found to facilitate the communication between the brain'[12] and the machines, such as orthoses and prostheses that have proven to be efficient and effective for the treatment of Parkinson's, blindness and other diseases and limitations by interpreting data from brain activity.

The brain is a physiological organ composed of nervous tissue, that commands task-evoked responses, movement, senses, emotions, language, communication, thinking, and memory.[13] Brain activity is the basis of cognitive, affective, and survival state, being relevant to the extent that in many countries, 'death is legally defined by irreversible

[8] World Health Organization, "World Report on Disability 2011, page 11. Available at: https://apps.who.int/iris/handle/10665/44575.

[9] Alzheimer's association, 'Alzheimer's Breakthrough Act', august 2012. Available at: https://act.alz.org/site/DocServer/2012_ABA_Fact_Sheet.pdf;jsessionid=00000000.app20005a?docID=1921&NONCE_TOKEN=275A51DABCD7F1949DACF9680ADD25D1.

[10] Committee on Bioethics (DH-BIO) of the Council of Europe and Marcello Ienca, "Neurotechnologies and Human Rights Framework: Do We Need New Rights?," October 2021, page 6. Available at: https://rm.coe.int/report-final-en/1680a429f3.

[11] "Neurotechnology: Premises, Potential, and Problems," Routledge & CRC Press, n.d., page 2-3. Available at: https://www.routledge.com/Neurotechnology-Premises-Potential-and--Problems/Giordano/p/book/9781439825860.

[12] Raimundo Roberts, "Neurotechnologies: Connecting Human Brains to Computers and Related Ethical Challenges," Biblioteca Del Congreso Nacional De Chile / BCN, May 2019, available at: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/28289/1/If01_Neurotechnologies_BCN_eng.pdf.

[13] Maldonado, Kenia A., and Khalid Alsayouri. 2023. "Physiology, Brain." StatPearls – NCBI Bookshelf. March 17, 2023. https://www.ncbi.nlm.nih.gov/books/NBK551718/.

cessation of brain activity'[14] or the brainstem functions.[15] The centrality of this notion to others like human identity, freedom of thought, autonomy, privacy, and human well-being means that the ethical, legal and societal impact of recording and/or modulating brain activity through various devices and procedures is vitally important to consider.[16]

The neurotechnology that is revolutionizing 'our understanding of the brain and its interaction with technology'[17] is the Brain-Computer Interface (BCI). BCI manifest themselves in a collaboration between the human brain and an electronic device that receives signals from the brain to command an external activity, more specifically, 'a system that measures central nervous system (CNS) activity and converts it into an artificial output (response) that replaces, restores, complements, or enhances the output of the natural CNS and thereby modifies the ongoing interactions between the CNS and its external or internal environment'.[18]

The examination of how data from Brain-Computer Interfaces is categorized under data protection laws becomes complex when considering that not all data revealing physiological conditions of the brain can be directly linked to sensitive data, in the provisions of article 9 of the GDPR. This complexity arises because the source of this data is the brain or the mental state of the data subject, which does not automatically imply sensitivity. According to the definition of article 4(1) of the

---

[14] International Bioethics Committee, "Report of the International Bioethics Committee of UNESCO (IBC) on the Ethical Issues of Neurotechnology," December 2021, page 6. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000378724, page 4.

[15] As defined in the Portuguese legal framework in Law 141/99 of 28 August that establishes the principles upon which the verification of death is based.

[16] Report of the International Bioethics Committee of UNESCO (n 14), page 4.

[17] Neuroscience News, "Interfacing Minds and Machines: An Exploration of Neural Implants and Brain-Computer Interfaces," June 17, 2023. Available at: https://neurosciencenews.com/brain-computer-interfact-neural-implants-23492/.

[18] Jonathan R. Wolpaw et al., "Brain–Computer Interfaces for Communication and Control," Clinical Neurophysiology 113, no. 6 (June 1, 2002): 767–91. Available at: https://doi.org/10.1016/s1388-2457(02)00057-3 in Raimundo Roberts (n 13), page 2-3.

GDPR, as in WP29 Guidelines[19], and the Court of Justice of the European Union, CJEU, cases Breyer[20] and Nowak[21] data that is related to the 'human brain and mind are always personal data if they allow to single out the data subject at stake'.[22] There is also a discussion in the doctrine regarding the relationship between Mental Data and brain data[2324] within the fact that 'not all brain data are Mental Data as brain data can be processed to infer not only mental states but also basic brain anatomy and physiology, without disclosing mental states and processes'.[25]

---

[19] ARTICLE 29 DATA PROTECTION WORKING PARTY, "Opinion 05/2014 on Anonymisation Techniques," April 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[20] JUDGMENT OF THE COURT (Second Chamber), "Patrick Breyer v Bundesrepublik Deutschland in Case C-582/14," October 2016, [30]. https://curia.europa.eu/juris/document/document.jsf;jsessionid=C46DB40CAC700B9AE3435EF04893B20C?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1228188

[21] Judgment of the Court (Second Chamber), "Peter Nowak v Data Protection Commissioner in Case C-434/16," December 2017, https://curia.europa.eu/juris/document/document.jsf?text=&docid=198059&pageIndex=0&doclang=en&mode=lst&dir=&occ=-first&part=1&cid=1229492.

[22] Frederik J. Zuiderveen Borgesius, "Singling out People without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation," Computer Law & Security Review 32, no. 2 (April 1, 2016): page 32, https://doi.org/10.1016/j.clsr.2015.12.013 in Marcello Ienca and Gianclaudio Malgieri, "Mental Data Protection and the GDPR," Social Science Research Network, January 1, 2021, page 8, https://doi.org/10.2139/ssrn.3840403.

[23] Authors that argue that neural data have a direct causal link with mental processes: Marcello Ienca, Pim Haselager, and Ezekiel J. Emanuel, "Brain Leaks and Consumer Neurotechnology," Nature Biotechnology 36, no. 9 (October 1, 2018): 805–10, https://doi.org/10.1038/nbt.4240; Marcello Ienca and Roberto Andorno, "Towards New Human Rights in the Age of Neuroscience and Neurotechnology," Life Sciences, Society and Policy 13, no. 1 (April 26, 2017), https://doi.org/10.1186/s40504-017-0050-1; Marcello Ienca and Karolina Ignatiadis, "Artificial Intelligence in Clinical Neuroscience: Methodological and Ethical Challenges," Ajob Neuroscience 11, no. 2 (March 31, 2020): 77–87, https://doi.org/10.1080/21507740.2020.1740352; Rafael Yuste et al., "Four Ethical Priorities for Neurotechnologies and AI," *Nature* 551, no. 7679 (November 1, 2017): 159–63, https://doi.org/10.1038/551159a.

[24] Example of an author that criticizes the division of neural data from brain data due to limited accuracy and reliability of the current available neurodevices: Anna Wexler, "Separating Neuroethics from Neurohype," Nature Biotechnology 37, no. 9 (August 9, 2019): 988–90, https://doi.org/10.1038/s41587-019-0230-z.

[25] Marcello Ienca and Gianclaudio Malgieri (n 22) page 7.

However, when considering the content, context, and purpose of data processing,[26] it's possible that these types of data might reveal information related to the sensitive categories defined in Article 9(1) of the GDPR. This creates a conceptual and normative gap,[27] as authors have discussed regarding the protection gap in all Mental Data and the definition of 'special categories of data' being either purpose-based[28] or mostly contextual.[29]

This article aims to qualitatively and descriptively analyse the legal and ethical issues related to BCI and the possible use of mental data, based on secondary sources and normative and jurisprudential legal interpretation. I intend to critically analyze the intersection of data captured and managed by Brain-Computer Interfaces, with 'the most comprehensive and progressive piece of data protection legislation in the world, updated to deal with the implications of the digital age',[30] the GDPR, addressing the complex challenges and implications arising from these technological advancements, to be able to answer the following pivotal questions: Does the technological capacity of BCI extend to the point of processing human thoughts? Are thoughts, in essence, mental or brain/neural data? Are thoughts personal data under the GDPR? Let's examine.

---

[26] Paul Quinn and Gianclaudio Malgieri, "The Difficulty of Defining Sensitive Data–The Concept of Sensitive Data in the EU Data Protection Framework," German Law Journal 22, no. 8 (December 1, 2021): 1583–1612, https://doi.org/10.1017/glj.2021.79; Karen McCullagh, "Data Sensitivity: Proposals for Resolving the Conundrum," Neliti, 2007, https://www.neliti.com/publications/28727/data-sensitivity-proposals-for-resolving-the-conundrum.

[27] Stephen Rainey et al., "Is the European Data Protection Regulation Sufficient to Deal with Emerging Data Concerns Relating to Neurotechnology?," Journal of Law and the Biosciences 7, no. 1 (January 1, 2020), https://doi.org/10.1093/jlb/lsaa051.

[28] Ibid, page 14, 16 and 17.

[29] Marcello Ienca and Gianclaudio Malgieri (n 22) states that 'According to the contextual approach in the GDPR, all personal data should be assessed against the background of the context that determines their processing, as determined by several contextual factors (eg the specific interests of the controller, the potential recipients of the data, the aims for which the data are collected, the conditions of the processing and its possible consequences for the persons involved). In contrast, the purpose-based approach essentially looks at the intention of the data controller and asks whether the controller intends to draw conclusions from the processing of particular data that could be regarded as being sensitive in nature.'

[30] "Data Protection," European Data Protection Supervisor, January 25, 2024, https://edps.europa.eu/data-protection_en.

2. Brain-Computer Interfaces and the Decoding of Brain Signals

The goal of a BCI is to detect and quantify the characteristics of brain signals that indicate the user's intentions and to translate those characteristics in real time into device commands that fulfil the user's intention. The interaction between the user's brain and the BCI system is made in a four-step cycle: input (signal acquisition), measurement and recording of brain activity (feature extraction), decoding and classification (feature translation) and the device output.[31] The input is the generation of specific brain activity, when the user is in certain cognitive state or performs a certain mental task, in response to a stimulus.[32] Brain activity is measured using a particular sensor modality, like the scalp or intracranial electrodes for electrophysiologic activity[33], being amplified to levels suitable for electronic processing, digitized and transmitted to the computer. After the broadcast the brain activity is measured, recorded, and analysed to distinguish pertinent signal characteristics during a cognitive process or the performance of a mental task, to differentiate noise,[34] random or unwanted electrical signals that distort the intended to be captured, and extraneous content from the user's intent. 'The recorded measurement can be implemented in different ways depending on the type of BCI in use'[35] being the most common way to extract the signal, a BCI time-triggered by

[31] Jerry J. Shih, Dean J. Krusienski, and Jonathan R. Wolpaw, "Brain-Computer Interfaces in Medicine," Mayo Clinic Proceedings 87, no. 3 (March 1, 2012): 268–79, https://doi.org/10.1016/j.mayocp.2011.12.008.

[32] Report commissioned by the Committee on Bioethics (DH-BIO) of the Council of Europe (n 11), page 16.

[33] Jerry J. Shih, Dean J. Krusienski, and Jonathan R. Wolpaw, "Brain-Computer Interfaces in Medicine," Mayo Clinic Proceedings 87, no. 3 (March 1, 2012): 268–79, https://doi.org/10.1016/j.mayocp.2011.12.008.

[34] Mohammad Javad Jafari et al., "The Effect of Noise Exposure on Cognitive Performance and Brain Activity Patterns," Open Access Macedonian Journal of Medical Sciences 7, no. 17 (August 30, 2019): 2924–31, https://doi.org/10.3889/oamjms.2019.742.

[35] Committee on Bioethics of the Council of Europe (n 10), page 16.

Electroencephalogram (EEG) or Electrocorticography (ECoG)[36] response latencies and amplitudes or firing rates of individual cortical neurons.

The characteristics of the neural data resulting from the brain signal obtained needs to be decoded to the feature translation algorithm so it can be usable by the BCI. The data is processed to obtain specific determined brain signals 'to increase the signal-to-noise ratio and to filter out the most relevant aspects of each signal for further processing'.[37] 'The translation algorithm should be dynamic to accommodate and adapt to spontaneous or learned changes in the signal features and to ensure that the user's possible range of feature values covers the full range of device control'[38], something that showcases the relevance of Artificial Intelligence and Machine Learning that provides algorithms that are trained to decode the neural signals in an increasingly accurate manner and 'behaviour accurately from time-varying neural oscillations'.[39] The final step represents 'the execution of the action initially intended or desired or deemed beneficial to the user through the control of the applications interfaced by the BCI'.[40] The algorithm commands operationalise the external device, providing functions depending on the goal of the application of the technology, supplying the feedback of the previous cycle, closing the control loop,[41] starting the next cycle for the following external action arise and only then we possess the data relatively clean to train the computers to recognize certain patterns to accomplish different tasks.

---

[36] ECoG is an "intracranial recording of EEG but in this case subdural grids are placed directly on the surface of the cortex to record electrical activity from the cerebral cortex" in Jonathan Curot, Thomas Busigny, Luc Valton, et al, "Memory scrutinized through electrical brain stimulation: A review of 80 years of experiential phenomena", Neuroscience & Biobehavioral Reviews, volume 78, 2017, pages 161-177, https://doi.org/10.1016/j.neubiorev.2017.04.018.

[37] Committee on Bioethics of the Council of Europe (n 10), page 17.

[38] Jerry J. Shih (n 33).

[39] Venkatesh Elango, "Sequence Learning for Brain Computer Interfaces," 2017, https://escholarship.org/uc/item/6gn763m3.

[40] Committee on Bioethics of the Council of Europe (n 10), page 17.

[41] James C. Wright et al., "A Review of Control Strategies in Closed-Loop Neuroprosthetic Systems," Frontiers in Neuroscience 10 (July 12, 2016), https://doi.org/10.3389/fnins.2016.00312.

2.1 From Brain to Speech: Decoding of Neural Activity

The current state of this technology, as well as all its potential and splendor, is mirrored in the pivotal scientific study "A high-performance speech neuroprosthesis"[42] focusing on the use of microelectrode arrays[43] to read ECoG of a participant with amyotrophic lateral sclerosis.

These arrays are crucial for capturing spiking activities of neurons in regions linked to speech production. The high-resolution data obtained from these arrays enable detailed and precise recording of neural patterns, forming the backbone of the neuroprosthesis functionality. The decoding process in this study is a sophisticated application of neural engineering and machine learning. At the heart of this process is a five-layer recurrent neural network[44] (RNN) decoder,[45] designed to interpret neural signals associated with speech attempts. This RNN operates by predicting the probability of each phoneme, or sound unit, being spoken at specific time intervals. Every 80 milliseconds[46], the decoder updates its prediction, providing a dynamic and continuous interpretation of the neural data. These phoneme probabilities are then intricately merged with a language model. This model utilizes the statistical characteristics of the English language to deduce the most likely sequence of words that corresponds to the neural signals. This integration is crucial, as it not only decodes the raw neural data into phonemes but also contextualizes these phonemes within the framework of coherent and grammatically accurate language.

---

[42] Francis R. Willett et al., "A High-Performance Speech Neuroprosthesis," Nature 620, no. 7976 (August 23, 2023): 1031–36, https://doi.org/10.1038/s41586-023-06377-x.

[43] 'The MEA system enables simultaneous extracellular recordings from multiple sites in the network in real time, increasing spatial resolution and thereby providing a robust measure of network activity' in Andrew F.M. Johnstone et al., "Microelectrode Arrays: A Physiologically Based Neurotoxicity Testing Platform for the 21st Century," NeuroToxicology 31, no. 4 (August 1, 2010): 331–50. Available at: https://doi.org/10.1016/j.neuro.2010.04.001.

[44] 'A recurrent neural network (RNN) is a type of artificial neural network which uses sequential data or time series data' in "What Are Recurrent Neural Networks? | IBM," n.d., https://www.ibm.com/topics/recurrent-neural-networks.

[45] Francis R. Willett et al. (n 42), page 1033.

[46] Ibid, page 1032.

By the final stages of the study, the trained RNN demonstrates remarkable proficiency in decoding speech from neural data in real--time, even for sentences it was never exposed to during training. The evolution of the RNN's capabilities, from initial training to its final high-performance state, is a testament to the potential of machine learning in enhancing neuroprosthetic technologies.

The study's ability to translate neural activities, particularly those associated with speech, into language, highlights the potential of BCI to access and interpret thoughts, on this case a specific subset of thoughts (those related to speech and communication) but the technology operates on the same basic principles: 'they record neural activity – usually electrical activity – associated with a function such as speech or attention; interpret what that activity means; and use it to control an external device or simply provide it as information to the user'.[47] The ability of the BCI system to decode neural signals associated with attempted speech into coherent language offers a glimpse into the possibilities of accessing and interpreting internal speech – a proxy for thought. This finding bridges the gap between the neural activity and complex cognitive processes, indicating that internal speech, an integral part of human thought, could be externalized and understood through advanced BCI systems.

3. Personal Data from the Mind: The Legal Status of Thoughts under the GDPR

Thought is one of the most subjective, intriguing, and complex realities of the human being, to the extent that there is no consensus on its definition. There are authors who say that thought needs to contain

[47] Liam Drew, "The Rise of Brain-Reading Technology: What You Need to Know," Nature 623, no. 7986 (November 8, 2023): 241–43, https://doi.org/10.1038/d41586-023-03423-6.

language or symbolic representation,[48] which makes it a capacity that is exclusively ours, but there are those who say that *flora* can also be capable of thinking.[49] 'Altogether what we have so far are quite remarkable decoding of the input and output signals'[50] which means that modern society cannot yet understand the abstract reality that lies between these signals and that manifests itself in thoughts. Nevertheless, it is necessary, at least attempt, to conceptualize and define the nature of thoughts grasping the relevant scientific contributions of neuroscience and psychology.

From a neuroscientific standpoint, thoughts are understood as the outcome of complex neural processes within the brain, according to the neural theory proposed by Santiago Ramón y Cajal and Camilo Golgi,[51] and how their complex networks and interactions result in the formation of thoughts. When humans think, there is a cascade of electrical and chemical activities in the brain – neural impulses travel through synapses, facilitated by neurotransmitters.[52] Neuroscientists examine the brain's physical and chemical processes to understand how thoughts are formed, mapping specific brain regions[53] and activities associated

---

[48] Lera Boroditsky, "How Language Shapes the Way We Think," IRL @ UMSL, n.d., https://irl.umsl.edu/oer/13/.

[49] Monica Gagliano, "The Mind of Plants: Thinking the Unthinkable," Communicative & Integrative Biology 10, no. 2 (February 17, 2017): e1288333, https://doi.org/10.1080/19420889.2017.1288333.

[50] Sapien Labs, "Reading a Thought – Sapien Labs | Neuroscience | Human Brain Diversity Project," Sapien Labs | Neuroscience | Human Brain Diversity Project, August 29, 2022, https://sapienlabs.org/lab-talk/reading-a-thought/.

[51] Santiago Ramón y Cajal, "*Textura del sistema nervioso del hombre y de los vertebrados: estudios sobre el plan estructural y composición histológica de los centros nerviosos adicionados de consideraciones fisiológicas fundadas en los nuevos descubrimientos*", Volumen III, 1904, https://digibug.ugr.es/handle/10481/69715; Camillo Golgi, "*Sulla fina anatomia del cervelletto umano*", Editore Libraio Milano, Milan, Italy, 1874.

[52] David M. Lovinger, "Communication Networks in the Brain: Neurons, Receptors, Neurotransmitters, and Alcohol," ResearchGate, January 1, 2008, https://www.researchgate.net/publication/236181567_Communication_networks_in_the_brain_Neurons_receptors_neurotransmitters_and_alcohol.

[53] Shazia Veqar Siddiqui et al., "Neuropsychology of Prefrontal Cortex," Indian Journal of Psychiatry 50, no. 3 (January 1, 2008): 202, https://doi.org/10.4103/0019-5545.43634, Joel L. Voss et al., "A Closer Look at the Hippocampus and Memory," Trends in Cognitive Sciences 21, no. 8 (August 1, 2017): 577–88, https://doi.org/10.1016/j.tics.2017.05.008.

with different types of thinking.[54] In contrast, psychological studies indicate the subjective experience of thoughts and their role in human behaviour and cognition, being conceptualized as complex mental constructs formed through the interplay of various cognitive unique processes, shaped by a combination of sensory perceptions, memories, experiences, and cultural influences. They represent a dynamic and integral aspect of human cognition, therefore involves not only the individual mind, but also the wider social and cultural context in which the individual operates, being influenced by social and cultural factors in their thought processes, as these are not formed in isolation, but are moulded by social norms, cultural backgrounds, and the social interactions experienced.[55]

Combining these perspectives, I recognise that thoughts are a multifaceted phenomenon: they represent a culmination of various neural activities and interactions, reflecting the complexity of the human cognitive experience, emotional states[56], environmental stimuli[57], and individual differences in brain structure and function,[58] so 'the content of our thoughts and the form they take varies in a complex manner across people, places, and time'.[59] 'Thinking leaves traces in the brain so exploring the mind by studying brain states might be like exploring

---

[54] The prefrontal cortex, for instance, plays a key role in higher-order cognitive functions like decision-making, problem-solving, and planning. Meanwhile, areas like the hippocampus are crucial for memory formation and retrieval, a critical aspect of how we think and process information.

[55] "People's Thoughts and Behaviors: Influence of Cultural and Social Factors | Free Essay Example," StudyCorgi, December 3, 2022, https://studycorgi.com/peoples-thoughts-and-behaviors-influence-of-cultural-and-social-factors/.

[56] Chai Meei Tyng et al., "The Influences of Emotion on Learning and Memory," Frontiers in Psychology 8 (August 24, 2017), https://doi.org/10.3389/fpsyg.2017.01454.

[57] Kathryn E. Schertz et al., "Environmental Influences on Affect and Cognition: A Study of Natural and Commercial Semi-Public Spaces," Journal of Environmental Psychology 83 (October 1, 2022): 101852, https://doi.org/10.1016/j.jenvp.2022.101852.

[58] Jenny Gu and Ryota Kanai, "What Contributes to Individual Differences in Brain Structure?," Frontiers in Human Neuroscience 8 (April 28, 2014), https://doi.org/10.3389/fnhum.2014.00262.

[59] Jonathan Smallwood et al., "The Neural Correlates of Ongoing Conscious Thought," iScience 24, no. 3 (March 1, 2021): 102132, https://doi.org/10.1016/j.isci.2021.102132.

an elephant by studying its footprints'[60] so I can affirm that thoughts are not just the product of brain activity, but rather the *a priori* cause of manifested brain activity.

Each individual's thought processes are a unique blend of their neural patterns, cognitive functions, emotional experiences, personal social constraints, but also information that are physically encoded in matter,[61] where the 'software' of the mind takes precedence over the 'hardware' of the brain.[62] Therefore, the brain is a facilitator of thought processes, supporting and realizing the mind's cognitive functions, functional capacities and emergent properties, but not being the sole originator of thoughts themselves.

Based in what I have outlined, neural activity in the brain forms the substrate from which thoughts emerge, suggesting a causal link between brain function and the generation of thoughts, but just as these have emerged, they are not simply reduced to their neurological underpinnings, occupying a distinct realm within the mind, characterized by subjective experience and qualitative richness that neural processes alone cannot fully encapsulate.[63] The brain then engages in further processing of these thoughts, integrating them with sensory input, emotional states, and memories. This processing, while rooted in the physical, navigates and influences the realm of the mental, reflecting the dual nature of human cognition as both a physical and a mental phenomenon.

---

[60] Bernhard Kutzler, "Thoughts Are Not Products of the Brain – Mind Cafe – Medium," Medium, March 28, 2022, https://medium.com/mind-cafe/thoughts-are-not-products-of-the-brain-a488b6690c99.

[61] Ralph Lewis, "What Actually Is a Thought? And How Is Information Physical?," Psychology Today, October 2023, https://www.psychologytoday.com/us/blog/finding-purpose/201902/what-actually-is-a-thought-and-how-is-information-physical.

[62] Kanchan Roy, "A Discussion on Computational Functionalism of Mind," Www.Academia.Edu, November 3, 2018, https://www.academia.edu/37697725/A_discussion_on_Computational_Functiona lism_of_Mind.

[63] For example, a mental state like 'pain' is identified not by its neurophysiological features but by how it functions in the organism – its causes (like tissue damage), and its effects (like withdrawal from harm, distress, and pain behaviour), "Multiple Realizability, Mind and | Internet Encyclopedia of Philosophy," n.d., https://iep.utm.edu/mult-rea/.

The relevance of these findings in the context of BCI decoding is profound. The current state of neuroimaging and BCI technologies, as exemplified by studies like *Gallant* lab's fMRI-based image reconstruction[64] and *Moses* et al.'s ECoG-based speech dialogue decoding,[65] demonstrates significant progress in decoding the input and output signals of the brain. However, the true essence of 'thought' – what happens between these inputs and outputs – remains elusive. This gap in understanding underscores the challenges faced by BCI in accurately interpreting and translating the intricate workings of the human mind. The realization that thoughts are not entirely constructible from electrical activity alone suggests that BCI might need to evolve beyond current methodologies to fully capture and interact with human thought processes, grounding legal and ethical discussions regarding privacy and personal data protection.

3.1 Brain and Neuronal Information Converted into Personal Data

The GDPR, which came into effect on May 25, 2018, within the European Union, establishes a framework for the processing of personal data, 'in the context of the activities of an establishment in the EU regardless of whether the processing takes place in the Union or not',[66] under all the changes causes by the rapid development of technologies and globalisation.[67] It defines personal data as 'any information that

---

[64] Kendrick Kay et al., "Identifying Natural Images from Human Brain Activity," Nature 452, no. 7185 (March 1, 2008): 352–55, https://doi.org/10.1038/nature06713.

[65] David A. Moses et al., "Real-Time Decoding of Question-and-Answer Speech Dialogue Using Human Cortical Activity," Nature Communications 10, no. 1 (July 30, 2019), https://doi.org/10.1038/s41467-019-10994-4.

[66] "Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) – Version Adopted after Public Consultation | European Data Protection Board," n.d., https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en.

[67] Recital 6 of the Official Journal of the European Union, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)," 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

relates to an identified or identifiable natural person',[68] being considered a "data subject". Personal data under the GDPR encompasses a wide range of information, including obvious subject identifiers such as names, identification numbers, and location data. It also covers less direct identifiers, like an online service provider that can be used to identify a person when combined with other information, such as the 'physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.[69] Despite these references to physical, physiological, and mental identifiers, the GDPR does not explicitly mention brain or neural information. This raises a critical question with regard to the applicability of the regulation with regard to brain information that it is not health data, nor stemming from medical devices.[70]

The neuron's ability to generate an action potential, electrical signal, and propagate it along the axon to the synapse, where it can trigger the release of neurotransmitters into the synaptic cleft, is fundamental to brain function. This synaptic transmission is the primary mechanism for neuron-to-neuron communication. The patterns and frequencies of these action potentials and the resulting neural networks they form are measured and considered as neural data.

The technical explanation of the neurotechnology applied in the scientific study already displayed, showed that the extrapolated information consists of two different components: (i) untouched physiological values that are manifested by the brain's electrical activity; (ii) the interpretation that experts make of the untouched values. These interpretations transform basic physiological measurements into crucial data that can be

[68] Article 4(1) of the GDPR defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

[69] Ibid.

[70] Stephen Rainey et al. (n 27), page 17.

concerned to an individual's health status or, based on the particular brain regions analysed, their racial and ethnic[71] background. As such, ECoG signals, just like EEG signals, have no meaning in themselves; they need to be read and decoded in order to be translated into meaningful information about the individual. To utilize brain recordings effectively, it is necessary to isolate signals pertinent to a specific objective from the overall recorded data, which means, to render brain recordings practical for a specific use, undergoing the processing of key features that are extracted and relevant signals categorized based on identifiable characteristics of a certain brain activity that is converted to digital data.

To understand what sets brain information apart as a distinct category of personal data, it's essential first to examine if data derived from the human brain through the neurotechnologies fits within the EU's data protection legal framework's definition of personal data. The author Dara Hallinan and his colleagues have previously addressed this question under the Data Protection Directive[72] (DPD), analysing it as the term "neurodata". Given the DPD's broad scope, their conclusion was that neural data falls under the umbrella of personal data.[73] This broad approach in data protection law is intentional, designed to ensure robust protection of individual rights.[74] Consequently, the term "personal data" in EU law is interpreted expansively, covering almost any data linked to an identifiable individual.[75] The development of the right to data

[71] Peipeng Liang et al., "Construction of Brain Atlases Based on a Multi-Center MRI Dataset of 2020 Chinese Adults," Scientific Reports 5, no. 1 (December 18, 2015), https://doi.org/10.1038/srep18216.

[72] Official Journal of the European Communities, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," 1995, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046.

[73] Dara Hallinan et al., "Neurodata and Neuroprivacy: Data Protection Outdated?," Surveillance and Society 12, no. 1 (November 20, 2013): 55–72, https://doi.org/10.24908/ss.v12i1.4500.

[74] Nadezhda Purtova, "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law," Law, Innovation and Technology 10, no. 1 (January 2, 2018): 40–81, https://doi.org/10.1080/17579961.2018.1452176.

[75] ARTICLE 29 DATA PROTECTION WORKING PARTY, "Opinion 4/2007 on the Concept of Personal Data," June 2007, https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf.

protection, culminating in the adoption of the GDPR, has largely been driven by the need to align legal tools with societal and technological advancements. As a result, the scope of EU data protection law has expanded.[76] By applying this rationale to brain data under GDPR, which has an even wider scope than the DPD, the same conclusion emerges.

While there is not an agreed definition of neural data, which is also referred as brain data,[77] the UNESCO International Bioethics Committee Report on Neurotechnology utilizes the term to describe it as 'personal brain data', [78] while the Council of Europe's Bioethics Committee identifies it as 'human brain data'.[79] Pursuant, also, to the Organisation for Economic Co-operation and Development understanding[80], personal brain or neural data are 'data relating to the functioning or structure of the human brain of an identified or identifiable individual that includes unique information about their physiology, health, or mental states'.[81] As for the Information Commissioner's Office is concerned, the concept of neural data is extended not only to information collected from the brain, but also from the nervous system, defining it as 'first order data gathered directly from a person's neural systems (inclusive of both the brain and the nervous systems) and second order inferences based directly upon this data'.[82]

In our opinion, in the balance of the two definitions identified

---

[76] See Recital 6 of the GDPR.

[77] Information Commissioner's Office, "ICO Tech Futures: Neurotechnology," June 2023, https://ico.org.uk/media/about-the-ico/research-and-reports/ico-tech-futures-neurotechnology-0-1.pdf.

[78] Report of the International Bioethics Committee of UNESCO (n 14).

[79] See Report commissioned by the Committee on Bioethics (DH-BIO) of the Council of Europe (n 10), page 23: "These quantitative data about the structure, activity and function of the human brain can be called 'human brain data'. Human brain data can reveal information about a person health status (e.g., neurological, or psychiatric health) and, to some extent, support inferences about mental processes".

[80] Hermann Garden et al., "Responsible Innovation in Neurotechnology Enterprises," OECD Science, Technology and Industry Working Papers, October 11, 2019, https://doi.org/10.1787/9685e4fd-en.

[81] "OECD Legal Instruments," n.d., https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0457.

[82] Information Commissioner's Office (n 77).

above, the concept of neural data used by the ICO is more complete, largely sufficient for the protection of the intended personal data of the subjects, with regard to the range of personal data involved in the brain, but it is also the most applicable to the reality in question. The definition given by UNESCO does not castrate other personal data that can be obtained by the brain, but it does imply that the data that can be obtained comes from physiological or health data. The problem actually lies in the consideration of "mental states"[83] as brain/neural data, when these states are more appropriately inferred from the mind, being referred to a range of cognitive conditions and processes, but not exclusively, as will be seen further ahead. Brain data processing involves various methods, including adaptive, unsupervised processes, where purpose-specific information is extracted from general brain activity recordings, which comes from brain states. This processing can yield diverse information from the same recording for different purposes, and adaptive filtering and classifying may evolve, potentially revealing more or different information than initially intended by researchers or users, opening a window to the potential of brain recordings to predict user behaviour, brain states, and identity-related activities[84] that needs data protection and privacy scrutiny, leading to increasing calls for international regulation as consumer neurotechnology gains broader market entry.[85]

Effectively, brain data gives us insight into the macro-level activities and states of the brain, but also draws us into the micro-level, revealing the intricacies of how neurons communicate and function, offering a detailed lexicon of the brain's language encoded in action potentials and synaptic transmissions, through the neural system,

[83] "We define 'mental state' any conglomeration of mental representations and propositional attitudes that corresponds to the experience of thinking, remembering, planning, perceiving, and feeling" in Marcello Ienca and Gianclaudio Malgieri (n 22).

[84] Philipp Kellmeyer, "Big Brain Data: On the Responsible Use of Brain Data from Clinical and Consumer-Directed Neurotechnological Devices," Neuroethics 14, no. 1 (May 19, 2018): 83–98, https://doi.org/10.1007/s12152-018-9371-x.

[85] Marcello Ienca, Pim Haselager, Ezekiel Emanuel (n 22).

acting as the granular manifestation of the brain's activity, capturing the bioelectrical and biochemical phenomena that constitute the essence of neural processing. To sum it up, brain data are the first order data gathered directly from a person's neural system, inclusive of both the brain and the nervous system and second order inferences based directly upon this data.

But what has been shown is that, regardless of the definition that can be attributed to neural data, it is not sufficient to correspond with data that comes from a combination of various internal factors that interrelate the neuronal connections with phenomenon that are rooted in the brain's neural processes, experienced and interpreted through the lens of psychological processes, and ultimately originate in the mind's complex, abstract realm, like thoughts.

2.2 Deciphering Thoughts: Distinguishing Mental Data from Brain Data collected by "Mind-Reading" BCI Technology

The UNESCO's report of the International Bioethics Committee, published in 2021, states that 'the specificity of brain data lies in the inferences that can be drawn from their analysis about actual consciousness, emotional state or even thoughts'.[86] What actually transpires from this statement is that the brain data comes from the information obtained through an analysis not only of consciousness and emotional state, but also through thoughts, necessarily making the brain data later than the true core of the information, creating the possibility of being accused that thoughts represent a distinct type of data surpassing traditional brain data or the neural system claimed by the ICO report.

'The term "mind-reading" has been used to describe the mechanisms employed by BCI and neural decoding using neurotechnologies.'[87]

---

[86] Report of the International Bioethics Committee of UNESCO (n 14) page 36.

[87] Stephen Rainey et al., "Brain Recording, Mind-Reading, and Neurotechnology: Ethical Issues from Consumer Devices to Brain-Based Speech Decoding," Science and Engineering Ethics 26, no. 4 (April 30, 2020): 2295–2311, https://doi.org/10.1007/s11948-020-00218-0.

BCI can decode neural activity associated with specific mental states or intentions, such as imagined speech or movement intentions. This procedure has been popularized as "mind-reading"[88], but it generally just entails the creation of dependable statistical correlations between brain activity, function, structure, and mental information, such decoding is based on identifying patterns in brain activity and is not equivalent to accessing or "reading" the full complexity of thoughts, manifesting itself in the translation of specific brain signals into actionable results rather than understanding their subjective and nuanced content.

Mind-reading surpasses the brain data to be interpreted by the BCI.[89] Considering the scientific study presented, as well as others, but with less positive results,[90] a speech decoder Brain-Computer Interface focus specifically on interpreting the neural mechanisms associated with speech production. These BCI utilize advanced algorithms to analyse patterns of brain activity, particularly those that occur during speech or speech-related processes. The technology effectively maps these neural patterns to corresponding speech sounds or textual representations. However, it does not delve into the personal, subjective content of thoughts or emotions, but they consist in educated guesses based on data patterns; BCI rely on pattern recognition technologies that associate specific neural activity patterns with predefined outcomes or commands. The capability of these systems is grounded in the physical realm of brain activity, translating specific neural signals into speech or text based on probabilistic models that are limited to the scope defined by the training data, and not in interpreting or 'reading' the abstract, if

---

[88] Matthias Gamer, "Mind Reading Using Neuroimaging," European Psychologist 19, no. 3 (January 1, 2014): 172–83, https://doi.org/10.1027/1016-9040/a000193.

[89] Kathinka Evers and Mariano Sigman, "Possibilities and Limits of Mind-Reading: A Neurophilosophical Perspective," Consciousness and Cognition 22, no. 3 (September 1, 2013): 887–97, https://doi.org/10.1016/j.concog.2013.05.011.

[90] Brumberg, "Classification of Intended Phoneme Production from Chronic Intracortical Microelectrode Recordings in Speech-Motor Cortex," Frontiers in Neuroscience, May 12, 2011, https://doi.org/10.3389/fnins.2011.00065; Stéphanie Martin et al., "Word Pair Classification during Imagined Speech Using Direct Brain Recordings," Scientific Reports 6, no. 1 (May 11, 2016), https://doi.org/10.1038/srep25803.

there is such a thing, subjective nature of individual thoughts or internal mental states, which proves the point, for now, that the technology still available is unable to gauge information directly from thoughts, unless scientifical evolution proceeds to "bless" us with a Mind--Computer Interface.

Ienca and Malgieri define Mental Data as 'any data that can be organized and processed to infer the mental states of a person, including their cognitive, affective, and conative states'.[91] Furthermore, mental representations are the closest psychological and neurobiological substrate for fundamental ethical-legal notions such as freedom of thought, personal identity, personal autonomy, mental integrity and others.[92] Thoughts, as part of mental representations, form an integral part of an individual's psychological makeup and are essential to their sense of self and autonomy. Therefore, thoughts as Mental Data are not only central to cognitive processes but are also fundamental to the core aspects of safeguarding human rights and personal freedom.

Additionally, this complexity and depth might position thoughts as a unique category of data inserted in Mental Data, with implications that extend beyond the physiological or structural aspects typically associated with brain data, considering that (i) Mental Data is not brain data, since information about mental states and processes can be inferred from non-neural data, such as behavioural data; and (ii) not all brain data is Mental Data, since brain data can be processed to infer not only mental states, but also the basic anatomy and physiology of the brain, without revealing anything related to mental states and processes.[93]

---

[91] Marcello Ienca and Gianclaudio Malgieri (n 22), page 4.

[92] Caplan A. L. (2017). Joseph J. Fins' Rights Come to Mind: Brain Injury, Ethics and the Struggle for Consciousness. Cerebrum: Orsolya Friedrich et al., "An Analysis of the Impact of Brain-Computer Interfaces on Autonomy," Neuroethics 14, no. 1 (April 18, 2018): 17–29, https://doi.org/10.1007/s12152-018-9364-9.

[93] Marcello Ienca and Gianclaudio Malgieri (n 22), page 7.

2.3 Thoughts as Personal Data under GDPR

Returning to the concept of personal data under the GDPR,[94] it can be divided into four cumulative requirements: (i) 'any information'; (ii) 'relating to'; (iii) 'an identified or identifiable'; (iv) 'individual'. In order to understand whether thoughts can be personal data under the Regulation, let's take a closer look at the fulfilment of the requirements.

The concept of 'personal data' under GDPR is intentionally broad, encompassing 'any information' even seemingly trivial data.[95] Personal data includes both objective and subjective information, in form of opinions for example,[96] whether it concerns private life, professional activities, or social behaviour, and does not need to be true, proven, or complete,[97] as long as it is related to a person. This definition covers all forms of data, regardless of medium, adhering to a technology-neutral approach, safeguarding all data types, ensuring robust privacy rights. Considering the fact that the GDPR is prepared to include information that is considered subjective, it is not opposed to considering the nature of thoughts as a statement about any person which takes the form of reading and interpreting information.

The European Regulation requires that information must pertain – 'relating to' – to an individual to be considered personal data. The CJEU, guided by WP29,[98] states that the information's content, purpose, or effect must be linked to a specific person,[99] i.e., if it directly concerns the particular individual or allows inferences about them, like wealth

---

[94] Article 4(1) of the GDPR (n 65).

[95] COMMISSION OF THE EUROPEAN COMMUNITIES, "COM(90) 314 Final – SYN 287 and 288 Brussels," September 1990, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51990DC0314.

[96] ARTICLE 29 DATA PROTECTION WORKING PARTY (n 70), page 6.

[97] Ibid.

[98] Ibid, page 10.

[99] Judgment Of The Court (Second Chamber), Case C434/16, Peter Nowak v Data Protection Commissioner, 2016. Available at: https://curia.europa.eu/juris/document/document.jsf?text=&doc_id=198059&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1067970.

from property value or driving behaviour from car service records.[100]Central to the application of personal data is the capacity to identify directly or indirectly, the data subject, a concept known as linkability.[101] When defining the scope of personal data and assessing linkability, there is scholarly debate over the use of 'objective' versus 'relative' criteria.[102] When considering the protection of thoughts as personal data, the abstract theory, or objective criterion, emerges as the more suitable approach. This theory advocates that personal data encompasses all information potentially linkable to an individual, independent of the particular context or the specific knowledge of the data processor or controller.[103] Such an inclusive definition is crucial for thoughts, given their deeply personal and intricate nature. Thoughts encapsulate a person's innermost experiences and ideas, which, if not broadly protected, could be vulnerable to misuse or exploitation. The concrete theory, or relative criterion, in comparison, bases personal data designation on the ability of a specific actor to associate the data with an individual in given circumstances.[104] This narrower view could lead to inconsistent protection of thoughts, as it hinges on the varying capabilities and resources of different data processors. By adopting the abstract theory, a more uniform and expansive safeguard is provided, ensuring that thoughts are consistently recognized and protected, thus minimizing their potential exploitation for economic or other purposes.

Identification of a data subject, a key GDPR component, hinges on whether the person is 'identified or identifiable.' Identification occurs through unique characteristics like name, location, or physical traits, not necessarily requiring a person's name, as other identifiers may be

---

[100] ARTICLE 29 DATA PROTECTION WORKING PARTY (n 70), page 10.

[101] Judgment of the Court (Second Chamber), "Peter Nowak v Data Protection Commissioner in Case C-434/16," (n 27), [61]-[63].

[102] JUDGMENT OF THE COURT (Second Chamber), "Patrick Breyer v Bundesrepublik Deutschland in Case C-582/14 (n 26).

[103] Oskar Josef Gstrein, "Mobile Devices as Stigmatizing Security Sensors: The GDPR and a Future of Crowdsourced 'Broken Windows,'" 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3105228.

[104] Ibid.

more distinctive.[105] Identifiability involves potential identification through information combinations.[106] This assessment considers various factors like technology and resource availability, emphasizing the realistic likelihood of identification rather than mere hypothetical possibilities. For instance, in the Breyer v Germany case, mentioned on the footnotes, the CJEU deliberated on IP addresses as personal data, illustrating how context influences data classification. This ruling suggests that dynamic IP addresses can be personal data when additional details enable individual identification.[107] This case extends beyond IP addresses, potentially widening the scope of data needing protection. The focus on the possibility, not the probability, of identification implies that data types like identifiers in neurotechnology, unless entirely anonymized, might be deemed personal data under GDPR, as anonymization would negate the functional purpose of consumer neurotechnology devices.[108] Based on this ruling it's plausible to argue that thoughts could be identified or identifiable with the data subject. If thoughts, as interpreted by neurotechnology, can be combined with other information that identifies the specific individual, creating an inter dependency and connecting between the data subject and the technology. This aligns with the CJEU's emphasis on the potential for identification, rather than the direct identification, broadening the scope of what may be categorized as personal data. For example, if a brain recording device is designed to respond to unique brain signals of a user for device control, it needs to be specifically calibrated for that individual.[109] The device's classification or filtering algorithms will then function in a manner tailored to the user's distinct brain patterns. In such cases, the use of these

[105] See ARTICLE 29 DATA PROTECTION WORKING PARTY (n 70), page 12.

[106] Ibid.

[107] JUDGMENT OF THE COURT (Second Chamber), "Patrick Breyer v Bundesrepublik Deutschland in Case C-582/14" (n 26), [49].

[108] Stephen Rainey et al. (n 27), page 7.

[109] Dennis J. McFarland and Jonathan R. Wolpaw, "Brain–Computer Interface Use Is a Skill That User and System Acquire Together," PLOS Biology 16, no. 7 (July 2, 2018): e2006719, https://doi.org/10.1371/journal.pbio.2006719.

calibrated algorithms creates a direct link between the data set and the specific user, allowing a data controller to associate the algorithm's operation with the individual data subject. Extending this logic to thoughts, if such devices can interpret and respond to individual thought patterns, then brain signals, could potentially be linked to a specific user. This implies that in certain contexts, thoughts can be identifiable and thus may fall under the scope of personal data as defined by GDPR.

The right to data protection under Article 8 of the EU Charter of Fundamental Rights[110] applies to all natural persons, not limited by nationality. This protection typically extends from birth until death,[111] with deceased persons' data generally not considered personal.[112] However, member states may enact rules to protect deceased persons' data, and genetic data may indirectly receive protection through relatives. Information on legal entities is usually not personal data,[113] but exceptions exist, especially when such data can reveal details about natural persons, like in small or family-run businesses, where company information might relate to an individual. The factor of a natural person being central to the definition of personal data under GDPR directly applies to thoughts as personal data. Since thoughts are inherently personal and originate from natural persons, they align with the GDPR's protection scope. This implies that any data, including thoughts, generated, processed, or inferred from a natural person's brain activity falls under the umbrella of personal data protection, provided it relates to an identifiable individual.

Under Article 4(1) of the GDPR thoughts inherently meet these requirements, as they provide information which is unique to individuals and can be linked to them, either directly or indirectly through neurotechnology. Thoughts reflect personal experiences, preferences,

---

[110] United Nations, "Universal Declaration of Human Rights | United Nations," n.d., https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[111] ARTICLE 29 DATA PROTECTION WORKING PARTY (n 70), page 23.

[112] See Recital 27 of the GDPR (n 65).

[113] Ibid, Recital 14.

and emotions, making them distinctive to each person. Therefore, when captured, interpreted, or processed through technologies like BCI, thoughts can be considered personal data as they provide identifiable information about a natural person, aligning with the GDPR's definition and scope. 'What remains is a discussion of how significant this data may be, how existing regulations ought to be interpreted, and what further regulation may be required'.[114] It could be argued that a thought does not necessarily result in information that identifies, directly or indirectly, the data subject, but in fact the reasoning done would only result in an *a posteriori* consequence of the thought, because, as already discussed, thought is what lies in the middle between the input, the neuronal mechanism that reacts to the stimulus of individual experience, and the output, which manifests itself in the reading and interpretation of the information collected from the brain signals, as such, thought always comes from a singular procedure that uniquely identifies the individual, that is, personal data of the data subject. Furthermore, if it is proven that brain patterns captured through EEG or fMRI provide unique and personalised information about the individual,[115] and these are the result of a set of factors in the consequential interrelationship between the mind and the brain, then thoughts are also personal and identify the person.

After understanding that thoughts are Mental Data that fall within the scope of the GDPR, it is important to determine if it has any additional protection under a special category of personal data.

---

[114] Stephen Rainey et al. (n 27), page 9.

[115] "Are Your Thoughts Your Own?:"Neuroprivacy" and the Legal Implications of Brain Imaging," Member & Career Services | NYC Bar, n.d., https://www.nycbar.org/member-and-career-services/committees/reports-listing/reports/detail/are-your-thoughts-your-ownneuroprivacy-and-the-legal-implications-of-brain-imaging.

3. Mental Data as a limit of the scope of sensitive data processing: CJEU Decision C-184/20

The next legal issue to consider is whether data related to the human mind can be classified as special categories of personal data. While the GDPR uses the term "special categories of personal data" to refer to what is commonly known as "sensitive data", it does not explicitly define sensitive data as a separate concept, instead this term is often used in broader discussions about data privacy to refer to any that that could cause harm to an individual if disclosed or misused, which includes but is not limited to the special categories of personal data defined by the GDPR. The user's privacy concerns and their willingness to disclose information are affected by the perceived sensitivity of that information and the advancements of technology entail the continuous creating of enormous amounts of personal data.[116] The GDPR defines sensitive data in the recital (51):

> *"Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms".*[117]

However, various other factors also contribute to how users perceive the sensitivity of data. These include the perceived risk, potential for harm, and the public availability of the data, all of which can influence the perception of information as being sensitive.[118] The existing

---

[116] Paul Quinn, "The Anonymisation of Research Data – A Pyric Victory for Privacy That Should Not Be Pushed Too Hard by the Eu Data Protection Framework?," European Journal of Health Law 24, no. 4 (October 19, 2017): 347–67, https://doi.org/10.1163/15718093-12341416.

[117] GDPR (n 65).

[118] John Rumbold and Barbara K. Pierscionek, "What Are Data? A Categorization of the Data Sensitivity Spectrum," Big Data Research 12 (July 1, 2018): 49–59, https://doi.org/10.1016/j.bdr.2017.11.001.

EU data protection framework, particularly the GDPR, has specific measures designed to offer enhanced protection for such special categories of personal data. These categories, due to their inherent nature, can significantly impact individuals' lives when processed,[119] and thus the GDPR ensures they receive additional safeguards, consequently the processing of sensitive data is permissible only under certain conditions and with the implementation of specific protective measures.[120] Accordingly to the article 9 (1) of the GDPR, special categories of data, also known as sensitive data, encompass information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, also including genetic data, biometric data for uniquely identifying a person, health-related data, and data concerning a person's sex life or sexual orientation. [121] 'The data related to the brain, despite all the peculiarities and related risks previously highlighted, are not explicitly mentioned within them'.[122]

It is known that information that can reveal a condition of pathological mental status is sensitive data, because it is associated with health data. Article 4(15) of the GDPR defines this type of data as 'personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status',[123] being further developed in recital 35 that 'all data pertaining to the health status of a data

[119] "The rationale behind regulating particular categories of data in a different way stems from the presumption that misuse of these data could have more severe consequences on the individual's fundamental rights, such as the right to privacy and non-discrimination, than misuse of other, "normal" personal data" in ARTICLE 29 DATA PROTECTION WORKING PARTY, "Advice Paper on Special Categories of Data ('Sensitive Data')," April 2011, https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf.

[120] Ibid.

[121] GDPR (n 65).

[122] Sara Latini, "To the Edge of Data Protection: How Brain Information Can Push the Boundaries of Sensitivity A Doctrinal Legal Analysis of EEG and fMRI Neurotechnologies under EU Data Protection Law" (MA thesis, 2018), page 38.

[123] GDPR (n 65).

subject which reveal information relating to the past, current or future physical or mental health status of the data subject'.[124] This definition, generally associated with 'mental health status,' encompasses not just pathological conditions but also the physiological state indicating the absence of mental pathology. Thus, biological parameters typically used to identify mental illnesses qualify as sensitive data even when indicating normal brain function, implying that the concept of mental health should be broadly interpreted to include various cognitive processes and emotional states of an individual.[125] The analysis becomes much more complicated if the information collected does not directly or indirectly reveal non-physiological conditions such as information related to emotions and thoughts, however if these types of data are collected using emotion detection tools that employ biometric methods, like facial recognition technology,[126] a correlation is established with biometric data which is considered sensitive personal data for the GDPR.

So, what I can identify after these considerations is that the regime for considering data as sensitive is too restricted considering current technological advances, and for some authors,[127] data that reveals information about the holder's thoughts is not necessarily sensitive, just because it only refers to the subject's mental sphere, but taking into account the content, context and purpose of the data processing,[128] it is possible that these types of data could reveal information about the sensitive data[129] contained in Article 9(1) of the GDPR. Considering these insights, it's evident that there is a distinct conceptual and normative gap: despite a public consensus on the intimate and sensitive nature of

---

[124] Ibid.

[125] In this path see Giovanni Comandé and Giulia Schneider, "Regulatory Challenges of Data Mining Practices: The Case of the Never-Ending Lifecycles of 'Health Data,'" European Journal of Health Law 25, no. 3 (April 18, 2018): 284–307, https://doi.org/10.1163/15718093-12520368.

[126] Damian Clifford, "Citizen-Consumers in a Personalised Galaxy: Emotion Influenced Decision-Making, a True Path to the Dark Side?," Social Science Research Network, January 1, 2017, https://doi.org/10.2139/ssrn.3037425.

[127] Marcello Ienca and Gianclaudio Malgieri (n 22), page 10.

[128] Paul Quinn and Gianclaudio Malgieri (n 26).

[129] Stephen Rainey et al. (n 27), page 11.

Mental Data, not all such data are safeguarded under the strict provisions of the GDPR for sensitive data. Furthermore, a thorough assessment of the sensitive nature of Mental Data requires an examination of their inherent qualities and potential, especially when integrated with advanced interpretative methods and technologies. This analysis extends beyond the conventional scope, pushing the boundaries of GDPR's traditional definition of sensitivity to potentially encompass Mental Data as well, and for this it is necessary to analyse the case C-184/20 of the Court of Justice of the European Union decision that opens the scope of sensitive personal data under the GDPR.

3.1 CJEU Case C-184/20 – Concept of Sensitive Data widened *de jure* and *de facto*

The Court of Justice of the European Union case C-184/20 addresses several significant issues related to the processing of personal data under the GDPR, specifically focusing on the concept of sensitive data. The case arose from proceedings between an individual, OT, and the Chief Official Ethics Commission in Lithuania, concerning OT's failure to lodge a declaration of private interests,[130] declaration aimed at fighting corruption and ensuring good government,[131] as administrator of a company that received EU funding, prompting legal proceedings that questioned the intersection of national data processing requirements with the broader scope of the GDPR and the Charter of Fundamental Rights of the European Union. The CJEU's position may be understood as resolving the disagreement between Norway's Data Protection Authority, which advocated for a broad interpretation of "special

[130] Judgment of the Court (Grand Chamber), "Vilniaus Apygardos Administracinis Teismas – Lithuania) – OT v Vyriausioji Tarnybinės Etikos Komisija in Case C-184/20," August 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62020CA0184&from=EN.

[131] Aly Marczynski José María Marín, "Compendium of Good Practices on Anti-Corruption for OGP Action Plans," December 18, 2018, https://apo.org.au/node/252866.

categories of personal data" in the Grindr case,[132] and Spain's Data Protection Agency, which conversely determined that no special category of personal data was processed in the identical context.[133]

The disclosure of personal data through declarations of private interests could potentially infringe upon individuals' rights to privacy. Such disclosures might inadvertently reveal sensitive information about a person's living arrangements, sexual orientation, and intimate family and personal relationships. This aspect of the case highlighted the sensitive nature of the data in question and the need for careful legal scrutiny in its handling. At the heart of the CJEU's analysis were two questions for the court to answer and decide: (i) To what extent could the online publication of the OT's declaration of private interests be based on Article 6(1) and (3) of the GDPR as a valid legal basis for data processing;[134] (ii) the publication of the name of the OT partner may or may not be processed in accordance with the limits and conditions set out in Article 9(1) and 9(2)(g) of the GDPR.[135] Restricting the court's good decision to the analysis in this thesis, let's just look at the scope of the second issue.

In addressing the second question, the CJEU's examination centres on data that, while not categorically classified as 'sensitive' under Article 9 of the GDPR, nonetheless carry the potential to disclose sensitive information, like sexual orientation. The Court scrutinized the nature of data specifically related to the spouse, cohabitee, or partner of the declarant.[136] It was noted that such data could inadvertently expose details about the individual's sex life or sexual orientation, as well as that of their partner.[137] To arrive at such sensitive revelations, the Court

---

[132] "Grindr Has Appealed the Administrative Fine Imposed by the NO DPA," Datatilsynet, n.d., https://www.datatilsynet.no/en/news/aktuelle-nyheter-2022/datatilsynet-har-mottatt-klage-pa-overtredelsesgebyr-i-grindr-saken/.

[133] "AEPD (Spain) – E/03624/2021," GDPRhub, n.d., https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_E/03624/2021.

[134] JUDGMENT OF THE COURT (Grand Chamber), Case C184/20 (n 129), [60].

[135] Ibid [117].

[136] Ibid [119].

[137] Ibid [118,119].

highlighted the necessity of an "intellectual operation involving comparison or deduction".[138] This process is identified as a key criterion for applying the heightened protection regime, typically reserved for inherently sensitive data, to personal data that are not inherently sensitive but have the potential to reveal sensitive aspects of an individual's private life.

Unfortunately, the Court does not discuss any further how this "intellectual operation involving comparison or deduction" should be conducted, whether certain criteria should be considered or whether it could be merely – and legitimately – based on stereotypes and common sense.[139] The Court's rationale is primarily based on ensuring consistency in interpreting the provisions related to sensitive data. It also emphasizes the importance of upholding a high standard of data protection, particularly concerning certain facets of private life.[140] This concept of intellectual operation is instrumental in evaluating how data is handled, focusing on whether the processing involves complex mental tasks such as comparing or deducing information from the available data.

The Court takes a contextual approach[141] in its analysis but stops short of detailing the specific criteria for identifying potentially sensitive personal data. Instead of relying solely on this contextual method, the Court could have benefited from a more nuanced approach, incorporating elements of a purpose-based analysis. It would have been pertinent for the Court to acknowledge that the administrative authority in question did not aim, either directly or indirectly, to gather information about the sexual orientation of individuals under transparency obligations. 'Moreover, the Court does not provide a taxonomy of personal data, either concerning the same data subject or third parties,

---

[138] Ibid [120].

[139] Giacomo Delinavelli, "Comment to Case C-184/20 and the Perils of a Broad Interpretation of Art. 9 GDPR," European Law Blog, September 21, 2022, https://europeanlawblog.eu/2022/09/21/comment-to-case-c-184-20-and-the-perils-of-a-broad-interpretation-of-art-9-gdpr/.

[140] JUDGMENT OF THE COURT (Grand Chamber), Case C184/20 (n 130), [125,126].

[141] Ibid [124].

that combined among them would reveal sensitive information', undermining legal certainty to data controllers.[142]

As a result of the evolving legal and practical understanding of sensitive data, heightened by advancements on the Internet of Things and increasing interconnectivity, there is a growing likelihood that more personal data will be classified as sensitive.[143]

3.2 Expanding Sensitivity to Mental Data

'If it is possible to indirectly deduce sensitive characteristics about a person from a reading of other personal data, the personal data in question will qualify as special category data – and no amount of risk mitigation measures to that data can remove its classification as special category data'.[144] The CJEU's interpretation of the "intellectual operation of comparison or deduction" provides an essential framework for the possibility of extending the concept of sensitive data to cover Mental Data, and therefore thoughts, suggesting that the process of inferring sensitive information from data involves intellectual operations like comparison or deduction. When applied to thoughts as Mental Data, this implies that the analysis or processing of such data to infer personal information, such as emotional states, intentions, or preferences, would require a similar level of intellectual operation, involving the possibility to deduce personal characteristics or predispositions from the patterns or nature of an individual's thoughts.

The CJEU's broad interpretation of special categories of data in this judgment establishes a high threshold that, in practice, may prove challenging to effectively manage. Regardless of the rationality of the

---

[142] Giacomo Delinavelli (n 139).

[143] Michela Galea, "CJEU Widens the Scope of Sensitive Personal Data under the GDPR," Data Protection – Worldwide, October 4, 2022, https://www.mondaq.com/data-protection/1236466/cjeu-widens-the-scope-of-sensitive-personal-data-under-the-gdpr.

[144] Andre Walter, "EU Court: Data Attributes Revealing Sensitive Personal Data Can Be 'Special Category' Data," Pinsent Masons, August 5, 2022, https://www.pinsentmasons.com/out-law/news/eu-court-data-attributes-sensitive-personal-data-special-category.

approach taken by the CJEU, what I can deduce regarding the perception of sensitive data is that it is necessary to analyse whether the data in question can, underlining can, reveal information related to the sensitive data listed in Article 9(1) of the GDPR by means of an intellectual operation involving comparison, inference, or deduction. Considering the great possibility of Mental Data being able to reveal the thoughts of each individual with regard to any sensitive personal data contained in the last rule invoked, I can say that, through an intellectual operation where the level of protection of Mental Data is compared with some sensitive data, the great possibility of their protection being equal to that of sensitive data is inferred and deduced, because otherwise it would result in distinctions being drawn according to the type of sensitive data at issue, thus diminishing the standard of protection which is intended to be afforded to special categories of personal data.

The following question could arise from the possibility of neurotechnology being able to decode thoughts and then realise, if it is possible by advanced technological capabilities for accurately processing and interpreting Mental Data, that if they can isolate thoughts referring to personal data and sensitive personal data, then humans would have thoughts, or Mental Data, with a sensitive nature and others not? I do not consider that this distinction would be positive for the data subject. Considering the actual complex, dynamic, deeply subjective and fluid nature of thoughts,[145][146] making such a differentiation would not consider the constantly evolving and interweaving connections of thought, so it would complicate even more any attempt to categorize them rigidly. Furthermore, the current state of technology, even with advanced data processing and AI, is not sufficiently developed to distinguish between sensitive and non-sensitive thoughts accurately and reliably, creating a significant risk of

[145] John Paul Minda, "The Fluidity of Thought," John Paul Minda, PhD, June 11, 2018, https://jpminda.com/2018/06/11/the-fluidity-of-thought/.

[146] "Fluid Intelligence: Definition, Examples, & Psychology," The Berkeley Well-Being Institute, n.d., https://www.berkeleywellbeing.com/fluid-intelligence.html.

misinterpretation and error, which could lead to inappropriate processing of sensitive data.

A challenging scenario also arises as to the legal basis for processing this type of data. Before processing a special category data, controllers must fulfil certain requirements that exceed the standards for processing "ordinary" personal data. This includes identifying a lawful basis as per Article 6 of the GDPR and satisfying an additional condition for processing under Article 9 of the GDPR, but also following specified, explicit and legitimate purposes.[147] When it comes to the "indirect" processing of the special category data, organizations might often need to seek explicit, informed and free consent of the data subject. This necessity arises because explicit consent is frequently the only applicable legal basis under Article 9(2) of the GDPR, mainly when the processing of these type of data has a commercial nature. [148]

When the processing of Mental Data serves not just the commercial goals of the data controller but also aligns with the personal interests of the data subjects (such as self-monitoring, self-quantification, mental activity exploration, or cognitive training), the likelihood increases that the data subjects' consent is given freely, therefore valid.[149] However, research has shown that the collection and processing of information data from neurotechnology and digital phenotyping applications often takes place under weak consent regimes,[150] this is due to the fact that the Terms of Service of these digital tools are (i) rarely read by users, (ii) typically uninformative about the whole data lifecycle and the specifics of data processing, and (iii) often based on presumed consent rather than affirmative consent.[151] Taking into account that neurotechnology is able to access both conscious and subconscious brain processes, individuals that, for example, participate in neuroimaging

[147] GDPR (n 65), article 5(1)(b).
[148] Ibid, page 11.
[149] Marcello Ienca and Gianclaudio Malgieri (n 22), page 12.
[150] Marcello Ienca, Pim Haselager, Ezekiel Emanuel (n 22).
[151] Marcello Ienca and Gianclaudio Malgieri (n 22), page 12

studies, might unknowingly provide access to data that would not want to share with third parties. This leaves the question if the modern society should consider acceptable to consent for the collection of Mental Data that the individual is unaware of.

The processing of Mental Data is not limited to commercial purposes; it also encompasses non-commercial scenarios such as medical diagnosis, scientific research, or activities in the public interest. For example, when Mental Data is processed for healthcare purposes, like diagnosis or therapy, article 9(2)(h) of the GDPR permits such processing without the need for specific additional condition.[152] In the context of processing Mental Data for scientific research, Article 9(2)(j) of the GDPR permits such activities, provided they adhere to specific conditions. This includes the requirement for authorization under a Union or Member State law, ensuring proportionality to the research aim, respecting the right to data protection, and implementing measures to protect the fundamental rights and interests of the data subjects. The appropriateness of such intrusive research, particularly when it delves into the mental sphere of subjects, is subject to scrutiny.

However, the European Data Protection Supervisor in a preliminary opinion on scientific research, expressed that behavioural experiments generally fall outside the scope of the research exemption in Article 9(2)(j) of the GDPR.[153] This is because they often lack an established ethical framework to justify their proportionality under the GDPR. In essence, the social and scientific benefits are often outweighed by the potential infringement on the privacy and data protection rights of the research subjects.[154] The applicability of this statement to

---

[152] Giulia Schneider, "OUP Accepted Manuscript," International Data Privacy Law, January 1, 2019, https://doi.org/10.1093/idpl/ipz015 in Marcello Ienca and Gianclaudio Malgieri (n 22), page 11.

[153] "Preliminary Opinion on Data Protection and Scientific Research," European Data Protection Supervisor, January 25, 2024, https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en.

[154] Mason Marks, "Artificial Intelligence-Based Suicide Prediction," Scholarship Repository, n.d., https://ir.law.fsu.edu/articles/732/.

other research areas involving Mental Data, which currently may not have a well-established ethical framework to guarantee proportionality, is a subject of discussion. For instance, Marcello Ienca points out that there is an argument that areas like cognitive monitoring and self--administered neuromodulation, especially when using non-medical digital mind technologies, may not yet possess a solid ethical framework necessary to ensure their proportionality and justification.[155]

3.3 DPIA as first safety gate of 'risky' processing of Mental Data

I believe that there are ways that lead to appropriate and safer Mental Data processing for the data subject, but the solution does not necessarily lie in "multi-layered sensitivity" as has already been proposed,[156] that could indivertibly stifle innovation and research introducing more complexity in enforcement and compliance, but rather in recognising it as high-risk data that requires specific and tailored Data Protection Impact Assessments (DPIA). By requiring this assessment prior to processing, DPIAs serve as a proactive measure, helping to identify and mitigate risks at an early stage. Consecrated in article 35 of the GDPR, it involves a thorough assessment and mitigation of data processing impacts, which must be conducted prior to processing and regularly updated as risk levels change.[157] This process is particularly relevant for Mental Data due to their sensitive nature and significant implications. The advantages of implementing a Mental DPIA for thoughts as a form of Mental Data are substantial. Firstly, it ensures a rigorous evaluation of potential risks associated with processing such thoughts, safeguarding against any undue infringement on privacy and

---

[155] Marcello Ienca, Pim Haselager and Ezekiel Emanuel (n 22); Sara Goering and Rafael Yuste, "On the Necessity of Ethical Guidelines for Novel Neurotechnologies," Cell 167, no. 4 (November 1, 2016): 882–85, https://doi.org/10.1016/j.cell.2016.10.029.

[156] Sara Latini (n 122), page 47.

[157] Dariusz Kloza et al., "Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals," D.Pia. Lab Policy Brief No. 1/2017, October 9, 2020, https://doi.org/10.31228/osf.io/b68em.

personal freedoms. Secondly, the regular review mandated by DPIAs ensures ongoing vigilance and responsiveness to any changes in risk levels, ensuring that protections remain robust over time. This is particularly important for Mental Data like thoughts, which may vary in evaluation of sensitivity depending on context and use.

The European Data Protection Board complemented the three high risks parameters at Article 35(3) with ten risk indexes where two of these apply, the data processing should be considered at high risk and the DPIA should be done.[158] Within this list there are various risks that can be applied to the processing of Mental Data, but considering that I am raising this issue from the point of view of the use of BCI, even though they are not yet capable of accessing thoughts, it is clear that the risk that is raised with the use of innovative technology, defined in "accordance with the achieved state of technological knowledge", recital 91, can trigger the need to carry out a DPIA, 'because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms'.[159] Reconciling this risk with what has already been presented and defended with regard to the sensitivity of Mental Data, it becomes clear that this processing is at high risk and the data controller must, according to Ienca and Malgieri, (i) describe the processing and description of the logic of the technology used;[160] (ii) perform a balancing test based on necessity and proportionality of the data processing in relation to the corresponding purposes;[161] (iii) assessing the risks for fundamental

[158] 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679', European Data Protection Board, 2017.

[159] Ibid, page 10.

[160] Kaminski, Margot E., and Gianclaudio Malgieri. 2020. "Algorithmic Impact Assessments Under the GDPR: Producing Multi-layered Explanations." International Data Privacy Law 11 (2): 125–44. https://doi.org/10.1093/idpl/ipaa020.

[161] Kloza, Dariusz, Alessandra Calvi, Simone Casiraghi, Sergi V. Maymir, Nikolaos Ioannidis, Alessia Tanas, and Niels van Dijk. 2020. "Data Protection Impact Assessment in the European Union: Developing a Template for a Report from the Assessment Process." LawArXiv. October 9. doi:10.31228/osf.io/7qrfp.

rights and freedoms; (iv) presenting suitable measures to address and mitigate those risks.[162]

Furthermore, the Data Protection Agency can play a crucial role in enhancing the protection of Mental Data. If a controller, after conducting a DPIA, concludes that it is not possible to find adequate solutions to mitigate identified risks, it can seek guidance from the relevant data protection agency. This agency has the capability to provide advice, recommendations, or even impose obligations through discussions with the controller, putting interpreters and stakeholders focus on the processing characteristics, rather than just on the category of data at issue.

Conclusion

It is clear that the modern society stands on the brink of a new era in human-machine interaction, our legal frameworks must be both reactive and proactive. Thoughts are not just binary or linear; they are multi-dimensional, influenced by a myriad of factors like emotions, context, and subconscious elements. Current BCI, while making significant strides, still struggle with capturing this multidimensionality. Nevertheless, law must be vigilant to these technological advances, ensuring that individuals' rights are preserved even as new forms of data emerge. At the same time, it must proactively promote responsible innovation, guiding neurotechnology development in a direction that enhances societal welfare without compromising personal integrity and 'fundamental aspects of human existence, including mental integrity, human dignity, personal identity, freedom of thought, autonomy, and privacy'.[163]

---

[162] Marcello Ienca and Gianclaudio Malgieri (n 22), page 18.

[163] "Unveiling the Neurotechnology Landscape: Scientific Advancements Innovations and Major Trends," UNESCO, July 20, 2023, https://www.unesco.org/en/articles/unveiling-neurotechnology-landscape-scientific-advancements-innovations-and-major-trends.

The GDPR's robust approach to personal data protection provides a strong foundation, but it may require further specificity when applied to the nuances of these types of data. For instance, how can consent be meaningful when data subjects may not fully grasp the future implications of sharing their brain and Mental Data? How can privacy be preserved when thoughts and emotions could potentially be decoded and exposed? The answers to these questions lie in a concerted effort by lawmakers, technologists, and ethicists to forge new legal instruments or adapt existing ones to better fit the digital and neural age. This endeavour is not solely about constraining technology but about harnessing its potential responsibly. In the end, the goal of any adaptation in the legal system should be to safeguard the individual's right to cognitive liberty and mental privacy. This means ensuring that people retain control over their own brain and neural data and that they are protected from any form of coercion or discrimination based on that data. It also means fostering an environment where neurotechnology can flourish in a way that is beneficial and ethical, contributing positively to healthcare, education, and beyond.

The CJEU decision presented in this article provides a significant development in data protection law, particularly when it comes to the opening of applicability to thoughts as Mental Data. This decision effectively brings thoughts under the umbrella of sensitive data, recognizing their intrinsic value and the need for stringent protection. By interpreting the processing of Mental Data through the lens of the GDPR, particularly in light of special categories of data, thoughts, as a form of Mental Data, can reveal sensitive information by its own inherent individuality. This interpretation aligns with the broader objectives of the GDPR to protect personal integrity and privacy. Consequently, thoughts are not just seen as mere personal data but are given the elevated status of sensitive data, warranting higher standards of protection. This landmark decision by the CJEU marks a pivotal shift in data protection law, ensuring that thoughts, as intimate reflections of the Self, are safeguarded with the utmost care and diligence in line with the GDPR's principles.

The significance of this development is further amplified by the role of the DPIA, or Mental Data Protection Impact Assessment,[164] as a crucial tool in this context, providing a systematic approach to evaluating and mitigating risks associated with processing such sensitive data. It ensures that any processing of thoughts, now recognized as sensitive data, is preceded by a thorough assessment of potential impacts on privacy and fundamental rights.

One thing is for sure, when brains and machines merge, concepts such as intention and responsibility can become blurred, especially when BCI might act on transient thoughts, leading to disputes over intended actions. Moreover, with the lack of legislation protecting how Mental Data is used, it flags the danger of erosion of testimonial authority and discrimination if biases are built into BCI algorithms.[165]

Given how limited the literature has yet been written on this subject, this article aimed at further intensify the debate on possible technological access to data as personal as that which interrelates in the human mind and the proactive need to have applicable legislation that keeps pace with technological development without unexpectedly falling into a reality where humanity could end up with Mind-Computer Interfaces, for which it is not prepared.

[164] Marcello Ienca and Gianclaudio Malgieri (n 22), page 19.

[165] McBain, Sophie. 2024. "Are You Ready for Elon Musk to Read Your Mind?" New Statesman, January 30, 2024. https://www.newstatesman.com/science-tech/big-tech/2024/01/mind-reading-elon-musk-neuralink.

Metadados, direitos fundamentais e o novo regime português

Beatriz Assunção Ribeiro
Associada, VdA
bea@vda.pt

Iakovina Kindylidi
Senior International Advisor, VdA
imk@vda.pt

Resumo:
Na sequência do Acórdão Digital Rights Ireland do Tribunal de Justiça da União Europeia e do Acórdão n.º 268/2022 do Tribunal Constitucional, o regime dos metadados tem sido objeto de discussão nos últimos anos, da qual resultou a aprovação de um novo regime a este respeito. Este artigo visa sobretudo discutir e explicar os conceitos básicos associados à temática dos metadados, bem como analisar algumas questões associadas ao regime entretanto aprovado em Portugal.

Palavras-chave:
PT: Metadados, privacidade, segurança, direitos fundamentais
EN: Metadata, privacy, security, fundamental rights

1. INTRODUÇÃO

Em qualquer comunicação é possível distinguir entre o seu conteúdo, isto é, a informação propriamente dita que essa comunicação pretende transmitir, e uma série de outros elementos que envolvem essa

comunicação, que a delimitam (no espaço e no tempo) e lhe dão suporte[1]. Estes elementos são comummente descritos como *dados sobre dados* – metadados – e incluem informação sobre, por exemplo, a localização de emissão dessa comunicação, o seu tempo, e a sua origem e destino. Em suma, os metadados correspondem a toda informação que pode ser recolhida a respeito de uma comunicação, que não seja o próprio conteúdo em si.

A Diretiva 2006/24/CE do Parlamento Europeu e do Conselho de 15 de Março de 2006, 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, e que altera a Diretiva 2002/58/CE ("Diretiva 2006/24") visava harmonizar as disposições dos EstadosMembros relativas à conservação de determinados dados gerados ou tratados pelos fornecedores de serviços de comunicações eletrónicas, procurando garantir a disponibilidade desses dados para efeitos de investigação, de deteção e de repressão de infrações graves, tais como crime organizado e terrorismo, no respeito dos direitos consagrados nos arts. 7.° e 8.° da Carta dos Direitos Fundamentais da União Europeia ("CDFUE").

Face às necessidades de uma década marcada por eventos trágicos no que respeita ao terrorismo e à necessidade urgente de se combater esta realidade, esta Diretiva nunca foi verdadeiramente colocada em causa até 2014, momento em que o Tribunal de Justiça da União Europeia ("TJUE") declarou a sua invalidade, no Acórdão Digital Rights Ireland[2].

---

[1] Acórdão n..º 403/2015, § 9, associado ao processo n..º 773/15, cujo relator é Conselheiro Lino Rodrigues Ribeiro, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20150403.html

[2] Tribunal de Justiça da União Europeia, Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, datado de 8 de abril de 2014, processos apensos C293/12 e C594/12, disponível em https://curia.europa.eu/juris/document/document.jsf;jsessionid=3CE25888D6478AA3CC9ED7B78735A64F?text=&docid=150642&pageIndex=0&doclang=pt&mode=req&dir=&occ=first&part=1&cid=2712231

Neste seguimento, o tema dos metadados sofreu um revés significativo, gerando uma incerteza que dura até aos dias de hoje. Ainda que novas leis tenham sido aprovadas, um pouco por toda a Europa, com a missão de resolver as questões levantadas pelo TJUE no Acórdão, não é totalmente evidente se as soluções encontradas são definitivas e suficientes.

Ora, com a declaração da invalidade da Diretiva 2006/24, o enquadramento europeu relativamente a esta matéria voltou à base, isto é, à Diretiva 2002/58/CE do Parlamento e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, mas também à CDFUE, que serve de pano de fundo interpretativo a toda a questão dos metadados, especialmente nos seus arts. 7.º (Respeito pela vida privada e familiar), 8.º (Proteção de dados pessoais), 11.º (Liberdade de expressão e de informação) e, na interpretação que lhes deve ser dada e compatibilização, quando necessária, o 52.º (Âmbito e interpretação dos direitos e dos princípios).

Concretamente em Portugal, este enquadramento era feito, mesmo após a declaração de invalidade da Diretiva 2006/24 pelo TJUE, pela Lei n.º 32/2008, de 17 de julho, sobre a conservação de dados gerados ou tratados no contexto oferta de serviços de comunicações eletrónicas ("Lei n.º 32/2008"). Eventualmente, os arts. 4.º (Categorias de dados a conservar), 6.º (Período de conservação) e 9.º (Transmissão dos dados) da Lei n.º 32/2008 acabaram declarados inconstitucionais, ainda que só em 2022, pelo Acórdão n.º 268/2022[3] do Tribunal Constitucional ("TC")[4].

Não se deve, contudo, olvidar que este não é o único enquadramento que pode ser feito a este respeito, o que significa que, mesmo

[3] Acórdão n..º 286/22, a respeito do processo n..º 828/2019, cujo relator é Conselheiro Afonso Patrão, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html

[4] De referir a este respeito que, apesar da Lei n..º 32/2008 em si mesma não ter sido considerada inconstitucional, é notório que os artigos afetados constituíam o verdadeiro núcleo do regime jurídico aqui em causa, e, sem eles, não era possível retirar-se qualquer consequência prática.

após o TC ter invalidado os artigos acima escritos, continuava a existir um enquadramento legal (ainda que parcial ou noutros termos) para os metadados. Efetivamente, as seguintes leis também se pronunciam sobre o assunto (com um âmbito mais ou menos restrito):

a. Lei n.º 109/2009, de 15 de setembro ("Lei do Cibercrime");
b. Lei n.º 41/2004, de 18 de agosto, sobre a proteção de dados pessoais e privacidade nas telecomunicações que transpôs a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho[5] ("Lei n.º 41/2004");
c. Lei Orgânica n.º 4/2017, de 25 de agosto, sobre o acesso dos oficiais de informações do SIS e do SIED a dados de telecomunicações e internet.

O presente artigo visa sobretudo analisar e explicar os conceitos básicos associados à temática, bem como analisar algumas questões associadas ao regime entretanto aprovado em Portugal.

2. QUESTÃO DE FUNDO E TIPOS DE METADADOS

À data da aprovação de qualquer declaração ou convenção dos direitos do homem, incluindo a europeia, bem como da Constituição da República Portuguesa ("CRP"), não existiam estes dispositivos eletrónicos que, hoje, nos seguem para todo o lado e constituem uma verdadeira extensão e materialização da nossa personalidade e consequentemente da nossa liberdade individual[6]. Mesmo as primeiras formas de telecomunicação criadas pela humanidade serviam tão-só para

[5] Uma pequena nota para destacar que esta lei, contrariamente à Lei n..º 32/2008, estabelece a possibilidade de os prestadores de serviços e comunicações eletrónicas conservarem certos tipos de dados mas não estabelece uma verdadeira obrigação.

[6] A única exceção a esta circunstância é, de facto, a CDFUE, que, proclamada pela primeira vez em 2000, já incluiu uma disposição específica relativa à proteção de dados pessoais (art. 8..º).

telecomunicar – i.e. expressar pensamentos por via telegráfica – mas não constituiam, na íntegra, um depósito portátil de cada ser humano como ocorre nos dias de hoje.

É esta a evolução que justifica que, em particular, o art. 34.º da CRP (Inviolabilidade do domicílio e da correspondência) seja lido a uma outra luz na era digital. É que a correspondência, que podia, à data da aprovação da CRP, corresponder a um mero reflexo esbatido da personalidade humana, revela hoje muito mais dessa personalidade do que alguma vez foi possível.

De facto, como bem refere o TJUE, a propósito de certos tipos de metadados, estes são hoje "suscetíveis de permitir tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados, como os hábitos da vida quotidiana, os lugares onde se encontram de forma permanente ou temporária, as deslocações diárias ou outras, as atividades exercidas, as relações sociais e os meios sociais frequentados"[7]. É precisamente por este motivo que estes dados são tão valiosos – porque a sua obtenção, no âmbito da investigação criminal, pode traduzir-se em avanços significativos nessa mesma investigação.

Ora, isto significa que qualquer ingerência que pudesse existir na correspondência, há cinquenta anos e no seu sentido literal de *correspondência*, não tem, nem pode ter, o significado atual: a ingerência nestas comunicações é, de forma inevitável, substancialmente mais grave.

Deste modo, a questão basilar e de fundo quanto ao tema dos metadados é essencialmente uma: a de concretizar o significado de correspondência e, deste modo, identificar o tipo de (meta)dados que, além do conteúdo, evidentemente abrangido pelo art. 34.º da CRP, fazem parte do núcleo duro deste direito constitucionalmente protegido

[7] Tribunal de Justiça da União Europeia, Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, § 27, datado de 8 de abril de 2014, processos apensos C293/12 e C594/12, disponível em https://curia.europa.eu/juris/document/document.jsf;jsessionid=3CE25888D6478AA3CC9ED7B78735A64F?text=&docid=150642&pageIndex=0&doclang=pt&mode=req&dir=&occ=first&part=1&cid=2712231

que é o da inviolabilidade da correspondência. Por outras palavras, que interpretação deve ser dada, à luz dos tempos em que vivemos, ao referido artigo, e de que forma deve ser alargado o significado de correspondência para abranger os dados que orbitam o conteúdo da correspondência propriamente dito?

Nem todos, como veremos, pertencerão a este leque privilegiado de dados que, pela ingerência na vida privada e interferência na personalidade que qualquer acesso[8] permitiria, acesso este que seria insuportável num estado de Direito democrático, são (relativamente) invioláveis.

É por este motivo que a primeira distinção que os tribunais portugueses fazem a este respeito, e que tem vindo a ser repetida decisão após decisão, decorre de uma classificação tripartida dos dados envolvidos em qualquer comunicação: (a) dados de conteúdo, (b) dados de base e (c) dados de tráfego. Esta distinção já se encontra estabelecida em Portugal há mais de duas dezenas de anos tendo tal discussão tido lugar Acórdão n.º 241/2002, de 29/05/2002, sendo que já antes, em 07.07.1994, a Procuradoria-Geral da República se havia pronunciado sobre o tema, no seu Parecer n.º 16/1994[9]. Esta noção tripartida foi posteriormente acolhida pelo TC, sendo utilizada até aos dias de hoje.

Esta classificação tripartida diz-nos que:

a. **Dados de conteúdo:** os dados de conteúdo, como o próprio nome indica, tratam-se de dados relativos ao próprio conteúdo da mensagem, da correspondência enviada através da utilização da rede. Não são metadados propriamente ditos, constituindo antes o cerne da mensagem. A conservação e acesso ao conteúdo de qualquer carta, mensagem ou forma de comunicação tem um

[8] De notar, contudo, que, pelo menos no mundo digital, conservação dos dados, em si mesma, é naturalmente uma ingerência a estes direitos e é por isto que a questão se coloca logo à partida, antes do próprio acesso aos mesmos dados, que é uma derrogação muito mais intensa do que a simples conservação e que, por isso, está sujeita, pelo menos na Europa, a regras muito restritas.

[9] Disponível em https://www.ministeriopublico.pt/pareceres-pgr/8715

impacto de tal modo intolerável na personalidade e liberdade humana que dificilmente se poderia aceitar uma compatibilização com outros interesses, sem mais[10] e por este motivo tem um regime especialíssimo relativamente ao restante (veja-se, por exemplo, o regime aplicável às escutas telefónicas).

b. Dados de base: os (meta)dados de base dizem respeito à conexão à rede e que são, do ponto de vista operacional, necessários para utilização própria do respetivo serviço, dizendo respeito aos dados através dos quais o utilizador tem acesso ao serviço. Dados de base são caracteres permanentes, tais como o número de telefone, pelo que a identificação do sujeito a que pertencem pode ser obtida independentemente de qualquer comunicação. Correspondem, de certa forma, à nossa identificação no âmbito das comunicações.

c. Dados de tráfego: Por fim, quanto aos (meta)dados de tráfego, são os dados considerados necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede para essa finalidade. São exemplos a localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência, dados de tráfego, necessários ou produzidos pelo estabelecimento da ligação da qual uma comunicação concreta é operada ou transmitida. Constituem elementos inerentes à própria comunicação, na medida em que permitem identificar, em tempo real ou *a posteriori*, os utilizadores, o relacionamento direto entre uns e outros através da rede, a localização, a frequência, a data, hora e a duração da comunicação.

---

[10] Como aliás explicita o TJUE no Acórdão Digital Rights Ireland "No que respeita ao conteúdo essencial do direito fundamental ao respeito da vida privada e dos outros direitos consagrados no art. 7.º da CDFUE, deve observarse que, embora a conservação dos dados imposta pela Diretiva 2006/24 constitua uma ingerência particularmente grave nesses direitos, não é suscetível de afetar o referido conteúdo, tendo em conta que, como resulta do seu art. 1.º, n.º 2, esta diretiva não permite tomar conhecimento do conteúdo das comunicações eletrónicas, enquanto tal".

Simplisticamente falando, se aquilo que se consegue retirar através de uma determinada informação for o conteúdo da mensagem – estaremos perante um dado de conteúdo; se o que é possível retirar da informação em causa é a identificação do utilizador que a origina – neste caso tratar-se-á de um dado de base; se está em causa qualquer informação que localize no tempo, no espaço e na rede aquela mensagem – então será um dado de tráfego[11].

De todo o modo, é curioso ver que, embora não seja totalmente claro de onde surgiu esta noção tripartida dos dados de uma comunicação, que dura até hoje, parece ter tido origem em doutrina francesa ou belga. Efetivamente, sem referenciar concretamente a fonte, o Parecer n.º 16/1994 menciona apenas que tal noção tripartida teve origem em Yves Poullet, reputado jurista belga, e Françoise Warran. Contudo, nem em França[12] nem na Bélgica[13], esta terminologia é utilizada, nem tão-pouco o TJUE faz uso dela, uma vez que não é utilizado pela legislação da UE, nem por outras legislações nacionais, pelo que é difícil identificar verdadeiramente origem desta noção tripartida.

Existem vários motivos que podem justificar esta circunstância, mas poderá estar relacionada com o facto de a divisão entre estas três categorias não ser totalmente linear. Com efeito, há casos em que um dado de base, pode ser simultaneamente um dado de tráfego, como ocorre, por exemplo, com o *Internet Protocol address* ("IP") e a localização.

---

[11] Note-se, claro, a bem do rigor científico, que estas se tratam de definições iminentemente práticas, porque a lei, na realidade, oferece definições teóricas destes conceitos, no art. 2..º, n..º 1 da Lei n..º 41/2004, de 18 de Agosto (Lei da Proteção de dados pessoais e privacidade nas telecomunicações).

[12] Em França, atualmente, os metadados são também denominados *donnés de connexion* que depois são subdivididos em cinco categorias: identidade (*Identité civile*), dados de contato e pagamento, dados relacionados a contratos e contas (*coordonnées de contact et de paiement, données relatives aux contrats et aux comptes*), endereços IP e equivalentes (*adresses IP et équivalents*), outros dados de tráfego e de localização (*autres données de trafic et données de localisation*); ver a este propósito o art. L34--1 do Código dos Correios e Comunicações Eletrónicas (*Code des postes et des communications électroniques*) e o relatório legislativo do senado a este propósito, disponível em https://www.senat.fr/rap/l20-694/l20-6946.html.

[13] Na Bélgica, os metadados a serem conservados estão listados no art. 126 da Lei relativa às comunicações eletrónicas, não sendo, de todo, agrupados em categorias.

A localização, como melhor explicado no Acórdão n.º 403/2015 do TC, diz respeito a *"dados tratados numa rede de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de telecomunicações, podendo incidir sobre a latitude, longitude ou altitude do equipamento, sobre a direção da deslocação, sobre a identificação da célula de rede em que o equipamento está localizado em determinado momento e sobre a hora de registo da informação de localização"*[14].

Ora, o TC, reconduzindo este conceito às categorias de metadados reconhecidas pelo próprio, defende que a informação relativa à localização (de um equipamento) pode enquadrar-se nos dados de base – quando identifica a posição geográfica do aparelho, independentemente de qualquer comunicação – ou nos dados de tráfego – quando esta identificação está associada a uma comunicação ou tentativa de comunicação. Ainda assim, o TC também argumenta, no Acórdão n.º 464/2019, que a primeira espécie dos dados de localização (a que não pressupõe comunicações em específico) é residual e que, por essa razão, tais dados de localização estão também incluídos no conceito mais amplo de *dados de tráfego*.

Esta posição baseou-se no parecer da Comissão Nacional de Proteção de Dados n.º 38/2017[15], que sustenta que, atualmente, ocorrem comunicações mesmo quando o utilizador do equipamento de comunicação não o aciona direta e intencionalmente, dando como exemplo o caso das atualizações efetuadas pelas aplicações de correio eletrónico ou outro tipo de mensagens, o que significa que a geração e troca de dados são praticamente constantes, mesmo quando os cidadãos utilizadores dos equipamentos nada fazem.

Em abstrato, esta justificação parece insuficiente para descartar, sem mais, a inclusão do dado *localização* – também – na categoria

[14] Acórdão n..º 403/2015, § 9, associado ao processo n..º 773/15, cujo relator é Conselheiro Lino Rodrigues Ribeiro, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20150403.html

[15] Parecer da Comissão Nacional de Proteção de Dados, a respeito do processo n..º 8243/2017, disponível em https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/105708

de dado de base, porque o facto de a geração e troca de dados ser constantes, sem necessidade de existência de envio de comunicações, não impede que (a) paralelamente, processos de identificação da localização, para outros efeitos, estejam a decorrer, nem que (b) num dado momento, ainda que temporalmente muito limitado, não existam comunicações a decorrer.

De resto, e embora criticável, de referir que também a doutrina portuguesa tem considerado que a localização está incluída, tal como o IP, no conceito mais amplo de dados de tráfego[16].

De facto, também o IP é uma questão controvertida, como bem mencionou o TC no Acórdão n.º 268/22, uma vez que pode não ter sempre a mesma qualificação. Os protocolos IP podem ser estáticos, o que significa que identificam, de forma permanente, um ponto de acesso à rede, ou dinâmicos, na medida em que são atribuídos a um certo dispositivo, no momento em que este faz a ligação à rede e apenas durante essa ligação. Por outras palavras, um protocolo IP dinâmico envolve informação da sua utilização num determinado momento, revelando informação sobre o utilizador, mas também sobre o uso da Internet num contexto específico.

Por este motivo, o Tribunal Constitucional Federal Alemão[17], entendeu que a identificação do titular de um protocolo IP dinâmico, ao pressupor uma consulta do tráfego para identificar o utilizador em dado momento, se enquadra nos dados de tráfego.

É esta a razão que justifica que também o TJUE muitas vezes analise autonomamente este tipo de dados[18]. Contudo, esta postura não foi acolhida pelo TC português no Acórdão n.º 268/22, que decidiu considerar o IP um dado base em qualquer circunstância.

---

[16] Veja-se, por exemplo, Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, Almedina, 2005, pág. 181.

[17] Acórdão do Tribunal Constitucional Alemão (Bundesverfassungsgericht – BVerfG), de 17 de julho de 2020, 1 BvR 1873/13 – 1 BvR 2618/13, §§ 101 e 102.

[18] Veja-se, por exemplo, o acórdão do Tribunal de Justiça da União Europeia, Tele2 Sverige AB contra Post och telestyrelsen, datado de 21 de dezembro de 2016, processo C203/15, disponível em https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=5157465.

Subjacente a esta posição reside a ideia de que *ainda que seja discutível a respetiva categorização* – uma vez que o apuramento do endereço de protocolo IP dinâmico pressupõe a análise do momento em que se realizou uma concreta comunicação – *a intensidade de agressão aos direitos à reserva da intimidade da vida privada e à autodeterminação informativa é similar ao dos demais dados de base,* não relevando, no entender do TC, *as circunstâncias da comunicação, a sua duração, a pessoa com quem se comunica ou os sites consultados; limita-se a identificar, tal como nos demais dados de base, o utilizador daquele computador.*

O TC sustenta ainda esta posição dizendo que tal conclusão é congruente com a orientação defendida pelo TJUE, no Acórdão *La quadrature du net*, quando este refere que *"*os endereços IP, apesar de fazerem parte dos dados de tráfego, são gerados sem estarem ligados a uma comunicação específica e servem principalmente para identificar (…) a pessoa singular proprietária de um equipamento terminal a partir do qual é efetuada uma comunicação através da Internet. Assim, em matéria de correio eletrónico e de telefonia através da Internet, desde que apenas sejam conservados os endereços IP da fonte da comunicação e não os do seu destinatário, esses endereços não revelam, enquanto tais, nenhuma informação sobre terceiros que tenham estado em contacto com a pessoa que está na origem da comunicação. Por conseguinte, esta categoria de dados tem um grau de sensibilidade menor que o dos outros dados de tráfego*"* [19].

Não parece ser totalmente clara esta ligação que é feita entre a semelhança da lesão nos direitos fundamentais que decorre da conservação e acesso a um dado de base e a natureza do próprio metadado. Ou seja, o TC parece utilizar o facto de uma lesão entre a utilização

[19] Acórdão do Tribunal de Justiça da União Europeia, Quadrature du net e outros contra Premier ministre, Ministère de la Culture, datado de 6 de outubro de 2020, § 152, processos apensos C511/18, C512/18 e C520/18, disponível em https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=5163305

de dados de base ser uma – e o facto de no caso dos endereços de IP a lesão ser semelhante – para depois contrariar o TJUE (que diz expressamente que o endereço IP é um dado de tráfego, tal como descrito no parágrafo anterior) argumentando que é um dado de base.

É que, a acrescer à diferença entre endereços IP estáticos/dinâmicos, melhor descrita acima, apesar de identificar o dispositivo – e, portanto, poder considerar-se um dado de base – o endereço IP está também presente no momento do envio ou da receção da comunicação, não podendo esta ser separada daquele. Isto significa que, pelo menos até determinado ponto, o endereço IP caracteriza a própria comunicação e esta não pode ocorrer, num dado momento, sem aquele. Em suma, concluir pelo enquadramento do IP como dado de base não tem real justificação, com a consequência, como veremos, da consagração de uma proteção menor a este tipo de dados.

No final, é difícil não concluir que esta distinção é mais prejudicial do que propriamente benéfica, sobretudo porque – face à confusão que se gera com esta classificação – acaba por ter muito pouca relevância prática.

De facto, levanta-se a questão de se saber a verdadeira utilidade da distinção quando, em primeiro lugar, e por um lado, como já foi referido, nem todos os metadados em causa se enquadram numa ou noutra categoria, o que significa que esta distinção levanta mais questões do que as que resolve.

Por outro lado, o próprio regime jurídico aplicável não parece retirar consequências práticas desta distinção, sem prejuízo de o TC o ter feito, conferindo mais ou menos proteção conforme o tipo de dados em causa. Na prática, e nomeadamente em Portugal, e noutros outros ordenamentos jurídicos tal como em França, ocorria que os metadados são listados e o seu regime é tipicamente definido em bloco[20], como aliás refere o próprio TC no Acórdão n.º 403/2015

[20] Salvo uma ou outra exceção específica, por exemplo para efeitos de determinação do prazo de conservação, como ocorre em França.

quando refere que "é nesse sentido que a Lei n.º 32/2008, de 17 de julho, que regula a conservação e transmissão dos dados de tráfego e de localização, reserva a mesma disciplina jurídica para ambos"[21].

De resto, a própria Lei n.º 32/2008, identicamente à Diretiva 2006/24, distinguia entre:

a. Dados necessários para encontrar e identificar a fonte de uma comunicação;
b. Dados necessários para encontrar e identificar o destino de uma comunicação;
c. Dados necessários para identificar a data, a hora e a duração de uma comunicação;
d. Dados necessários para identificar o tipo de comunicação;
e. Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento;
f. Dados necessários para identificar a localização do equipamento de comunicação móvel.

Ora, em nenhum momento parece decorrer esta distinção entre dados de base e dados de tráfego. Ocorre que, desta ficcionada distinção, conforme ficará patente na próxima secção, é de onde se retira a intensidade da proteção atribuída a cada uma das categorias como fez o Acórdão n.º 268/22 do TC.

3. A INGERÊNCIA NOS DIREITOS FUNDAMENTAIS

Como descreve o TC, "o direito ao livre desenvolvimento da personalidade abrange a faculdade de comunicar com segurança,

[21] Acórdão n..º 403/2015, § 9, associado ao processo n..º 773/15, cujo relator é Conselheiro Lino Rodrigues Ribeiro, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20150403.html

enquanto parte da sua liberdade de ação e de realização pessoal"[22]. É neste contexto também que se pode falar de um *direito à autodeterminação comunicativa* que se assume, também, como um direito de liberdade para comunicar, sem receio de que a comunicação ou as circunstâncias em que a mesma é realizada possam ser investigadas ou divulgadas.

Assim, mais do que uma questão intimamente relacionada com a privacidade propriamente dita, este direito demonstra-se de absoluta importância uma vez que, sem esta confiança, "o indivíduo sentir-se-á coartado na liberdade de poder comunicar com quem quiser, quando quiser, pelo tempo que quiser e quantas vezes quiser. Deste modo, é um direito que assegura o livre desenvolvimento das relações interpessoais e, ao mesmo tempo, de proteger a confiança que os indivíduos depositam nas suas comunicações privadas e no prestador de serviços das mesmas".

Como vimos, ainda que a distinção entre *dados de base e dados de tráfego* tenha relevância quase meramente teórica, o certo é que o TC faz uso da mesma para determinar que uma destas categorias – os dados de tráfego – merece proteção constitucional ao abrigo do art. 34.º da CRP e a restante categoria – dados de base – fica fora do âmbito de proteção do mesmo artigo[23].

É importante notar-se que o facto de os dados incluídos numa determinada categoria não estarem enquadrado no art. 34.º da CRP, não significa que não tenham respaldo constitucional. Efetivamente, não

---

[22] Acórdão n..º 403/2015, § 12, associado ao processo n..º 773/15, cujo relator é Conselheiro Lino Rodrigues Ribeiro, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20150403.html

[23] Esta é, de resto, jurisprudência reiterada do TC, que já havia explicado esta circunstância nos Acórdãos n..º 486/2009, 403/2015 e 463/2019. Neste contexto, nem todos os dados a que se refere o art. 4..º da Lei n..º 32/2008 estão protegidos pelo disposto nos números 1 e 4 do art. 34..º da Constituição. De acordo com a jurisprudência reiterada do TC, aquele parâmetro abrange os dados de tráfego quando pressuponham uma comunicação entre pessoas, mas já não os dados que, independentemente de qualquer comunicação, sejam atinentes à conexão de certo equipamento a uma rede de comunicações ou à mera identificação de um utilizador a quem estava atribuído um determinado número de telefone ou um endereço de protocolo IP estático; nem os dados de tráfego gerados pela comunicação entre um sujeito e uma máquina – v. g., a consulta de sítios da internet.

deixam de ter cabimento no art. 26.º da CRP, que diz respeito à reserva da intimidade privada[24], ainda que acoplado a esta circunstância venha, conforme referido pelo TC, um nível de proteção menos intenso do que aquele que o art. 34.º concede.

Na prática, esta distinção revela-se na ingerência que para a doutrina e jurisprudência é admissível num e noutro caso, que se traduz no entendimento comum de que uma determinada compressão dos direitos associados aos dados de base é aceitável, enquanto essa mesma compressão no caso dos dados de tráfego – que têm o potencial de revelar não apenas o utilizador como também a utilização da internet num determinado contexto – já não o será.

As ingerências em causa, por sua vez, e relativamente a dados de base e dados de tráfego, são a conservação (por determinado período e em determinado local) e o acesso. É relativamente a cada um destes regimes que o TC faz a sua análise.

É evidente que nos encontramos perante um caso paradigmático de ponderação e valores, e sobretudo de necessidade de compatibilização de direitos. Se, por um lado, temos este direito à reserva da intimidade privada (art. 26.º da CRP), de onde decorre também a inviolabilidade da correspondência (art. 34.º da CRP), por outro, temos o direito à segurança, também com previsão constitucional (art. 27.º da CRP).

Esta factualidade é relevante porque significa que qualquer acesso a metadados não se trata de uma ingerência sem mais, tratando-se antes de um importante processo de compatibilização de dois direitos fundamentais. E, portanto, como refere o Acórdão n.º 420/2017 do TC, a questão que se coloca é a de se aferir se a obrigatoriedade de os

[24] A este respeito, é também interessante referir que o TC, tal como melhor descreve no Acórdão n..º 403/2015, servindo-se da doutrina desenvolvida por Joaquim Sousa Ribeiro (em *A Tutela de bens da Personalidade na Constituição e na Jurisprudência constitucional portuguesas*, in Estudos de homenagem ao Prof. Doutor José Gomes Canotilho, Vol. III, Coimbra Editora, pág. 853) considera incluídos no art. 26..º da CRP outros direitos como, além da autodeterminação informacional, o direito à solidão e ao anonimato, bem como que todos estes direitos pesam na concretização da efetiva tutela constitucional a atribuir a estes dados.

fornecedores de serviços de comunicações eletrónicas conservarem este tipo de dados, constitui uma restrição destes direitos fundamentais e se tal restrição é desproporcionada nos termos do art. 18.º da constituição. Posto isto, é claro que não existem grandes dúvidas sobre a necessidade ou não de restrição dos direitos fundamentais em análise, mas antes sobre a sua proporcionalidade.

O princípio da proporcionalidade, como aliás sublinhado no Acórdão n.º 420/2017 do TC trata-se de um crivo basilar no plano das restrições de direitos fundamentais. De acordo com o n.º 2, do art. 18.º da Constituição, qualquer restrição "deve limitar-se ao necessário para salvaguardar outros direitos e interesses constitucionalmente protegidos". Por sua vez, assume três ramificações que constituem, na prática, critérios para aferir se determinada restrição passa ou não no crivo de proporcionalidade: (i) necessidade, (ii) adequação e (iii) proporcionalidade em sentido estrito.

Ora, para o TC é inequívoco que, relativamente aos dados de base, face ao interesse público prosseguido (i.e. investigação, deteção e repressão de crimes graves por parte das autoridades competentes, tal como previsto no art. 1.º, n.º 1, da Lei n.º 32/2008), tendo a "salvaguarda da legalidade democrática e a ação penal, nomeadamente contra os crimes referidos" interesse público e proteção constitucional"[25], a obrigação de os fornecedores de serviços de comunicações eletrónicas conservarem os dados de base cumpre os requisitos de necessidade[26], adequação e proporcionalidade em sentido estrito.

Em primeiro lugar porque, alega o TC, no Acórdão n.º 420/2017[27] "a conservação de dados de base é uma medida adequada para

[25] Acórdão n..º 420/2017, § 13, associado ao processo n..º 917/16, cujo relator é Conselheira Maria de Fátima Mata-Mouros, disponível em TC > Jurisprudência > Acordãos > Acórdão 420/2017. (tribunalconstitucional.pt).

[26] Aliás, como referiu o Conselho de Justiça e Assuntos Internos de 19 de dezembro de 2002, os dados relativos ao uso das comunicações eletrónicas são particularmente importantes e, portanto, uma ferramenta valiosa na prevenção de infrações e no combate à criminalidade, nomeadamente à criminalidade organizada.

[27] Acórdão n..º 420/2017, § 13, associado ao processo n..º 917/16, cujo relator é Conselheira Maria de Fátima Mata-Mouros, disponível em TC > Jurisprudência > Acordãos > Acórdão 420/2017. (tribunalconstitucional.pt).

permitir a identificação do utilizador registado, a quem o endereço do protocolo IP estava atribuído, suspeito de autoria de um dos crimes graves referidos*";* em seguida, é também uma medida necessária "na medida em que não é possível configurar um meio menos restritivo para as autoridades competentes procederem à referida identificação*"*.

Por fim, refere o TC que a proporcionalidade, no seu sentido estrito, procura vedar a adoção de medidas que se apresentem como excessivas (desproporcionadas) para atingir os fins visados. Neste juízo é necessário ponderar, de um lado, a natureza relativamente pouco invasiva da privacidade dos dados em questão (dados de base), os quais dizem respeito à identidade do utilizador, e, por outro, o período temporal de conservação (um ano) – após o qual os dados são destruídos (art. 7.º, n.º 1, alínea e), da Lei n.º 32/2008). Esta análise deve depois ser confrontada com a natureza especialmente grave dos crimes em questão e a centralidade destes dados para a condução da investigação criminal.

Aqui, o TC, no Acórdão n.º 268/22, não deteta qualquer irregularidade, tendo optado, fundamentando devidamente a sua posição, por manter a sua jurisprudência anterior. A questão central passa, neste último Acórdão, a ser outra – o da ingerência nos dados de tráfego.

E é aqui que o problema, no entender do TC, reside. Com efeito, este entende que, no caso dos dados de tráfego, gerados a propósito de uma comunicação específica, materializa-se "uma agressão mais intensa à intimidade privada dos sujeitos privados do que a preservação dos dados de base, ao permitirem identificar, a todo o tempo, a posição e os movimentos dos utilizadores"[28].

O TC defende que, ainda que a conservação seja, de facto, adequada e necessária para os fins que pretende proteger, a proporcionalidade só não poderá ser colocada em causa quando exista uma ligação direta entre os dados a conservar (e a agressão do direito fundamental que lhe subjaz) e a perseguição dos objetivos da ação penal. Ora, assim sendo,

[28] Acórdão n..º 268/22, §17.3, a respeito do processo n..º 828/2019, cujo relator é Conselheiro Afonso Patrão, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html

a conservação de todos os dados listados no art. 4.º da Lei n.º 32/2008, e de todos os indivíduos, ao ser geral e indiscriminada, é manifestamente desproporcional porque não existe esta relação direta para a conservação.

Assim, o TC entende que esta é uma solução jurídica desequilibrada face às finalidades que pretende alcançar, numa violação direta do art. 18.º, n.º 2 da CRP.

Também o TJUE já tinha entendido que a Diretiva 2006/24 implicava uma restrição desproporcionada aos direitos ao respeito pela vida privada e familiar e à proteção de dados pessoais, consagrados, respetivamente, nos arts. 7.º e 8.º da CDFUE. Em particular, entendia o TJUE que os problemas da Diretiva 2006/24, entre outros, se relacionavam com o facto de esta:

a. Não exigir relação entre os dados conservados e a ameaça à segurança pública, não se limitando a uma conservação em relação (i) a dados relativos a um período de tempo específico e/ou a uma zona geográfica específica e/ou a um círculo de pessoas específicas suscetíveis de estarem envolvidas, de alguma forma, numa criminalidade grave, ou (ii) a pessoas que poderiam contribuir, através da conservação dos seus dados, para a prevenção, deteção ou persecução de infrações graves;
b. Não conter condições substantivas e processuais relativas ao acesso das autoridades nacionais competentes aos dados e à sua subsequente utilização, não estabelecendo que estes têm que estar estritamente limitados ao propósito de prevenir, detetar ou investigar infrações graves (previamente definidas), apenas dispondo que cada Estado-Membro deveria definir os procedimentos a seguir e as condições a cumprir para obter acesso aos dados retidos de acordo com os requisitos de necessidade e proporcionalidade;
c. Exigir que esses dados fossem retidos por um período mínimo de seis meses (sem distinção entre as categorias de dados a

conservar), com base na sua utilidade possível para os fins do objetivo perseguido ou de acordo com as pessoas em questão; ao mesmo tempo, tal período era fixado entre um mínimo de seis meses e um máximo de 24 meses, sem que a determinação do período de conservação fosse baseada em critérios objetivos para garantir esta fosse limitada ao estritamente necessário;

d. Não prever garantias suficientes, no que diz respeito às regras relativas à segurança e proteção dos dados retidos pelos fornecedores de serviços de comunicações eletrónicas, conforme exigido pelo art. 8.º da CDFUE, para assegurar a proteção efetiva dos dados conservados contra o risco de abuso e contra qualquer acesso e utilização ilegal desses dados; em concreto, a diretiva não estabelecia regras específicas e adaptadas (i) à grande quantidade de dados cuja conservação é exigida por essa diretiva, (ii) à natureza sensível desses dados e (iii) ao risco de acesso ilegal a esses dados, regras que serviriam para garantir a integridade e confidencialidade dos dados, sem que sequer tenha sido estabelecida uma obrigação específica aos Estados-Membros para estabelecer tais regras;
e. Não exigir que os dados em questão fossem conservados dentro da União Europeia, não se assegurando a possibilidade de controlo por uma autoridade independente do cumprimento dos requisitos de proteção e segurança, tal explicitamente exigido pelo art. 8.º, n.º 3 da CDFUE, o qual é um componente essencial da proteção das pessoas em relação ao tratamento de dados pessoais[29].

Deste modo, ficou patente que, à luz da CDFUE, é possível a conservação destes dados, desde que exista uma ponderação sobre a

[29] Tribunal de Justiça da União Europeia, Comissão Europeia, apoiada pela Autoridade Europeia para a Proteção de Dados (AEPD), contra República da Áustria, § 37, processo C-614/10, disponível em https://curia.europa.eu/juris/document/document.jsf;jsessionid=E64E601BB3BB3FCFD0DBECA2C34F4641?text=&docid=128563&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=5154569

adequação, face à proteção de um interesse geral relevante. Contudo, e em complemento, ficou também claro que a respetiva regulamentação deve restringir a sua aplicação ao indispensável para aquele objetivo, mediante (i) definição seletiva do universo de dados e de titulares afetados, (ii) o estabelecimento de garantias no acesso das autoridades a essas informações, (iii) a estatuição de critérios objetivos de duração da conservação por atenção aos objetivos visados, e (iv) a criação de mecanismos de segurança de proteção eficazes desses dados contra abusos, utilização e acesso ilícitos.

Como muito bem refere o TC no seu Acórdão, 268/2022, o Acórdão Digital Rights Ireland permitiu delimitar o parâmetro comunitário de admissibilidade das medidas de conservação dos dados de tráfego e de localização. Assim, restavam poucas dúvidas que ponto de partida para um novo regime tinha que ser o Acórdão Digital Rights Ireland, e que todas as críticas e falhas ao regime por este feitas deveriam ser resolvidas num novo regime congruente com estas críticas.

4. O REGIME ATUAL DOS METADADOS

Após uma extensa e duradoura discussão sobre o tema[30], bem como várias tentativas, a Assembleia da República conseguiu finalmente aprovar alterações à Lei n.º 32/2008, com a publicação da Lei n.º 18/2024, de 5 de fevereiro

A nova versão do diploma determina que os dados de tráfego e de localização apenas podem ser objeto de conservação para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes, mediante autorização judicial, de caráter urgente e decidido no período máximo de 72h.

[30] Que envolveu uma nova proposta da Assembleia da República que lhe foi devolvida, perante a submissão, pelo Presidente, à fiscalização preventiva do TC, uma vez que a proposta não resolvia a questão da conservação geral e indiscriminada dos dados de tráfego.

A este respeito, surgem dúvidas sobre a efetiva utilidade deste método. Com efeito, uma das maiores críticas feitas a este procedimento – também designado por *quickfreeze*[31]- é relativamente à sua adequação, face à finalidade prosseguida com esta conservação, pelo simples facto de que, com frequência, não se demonstra totalmente eficaz tendo em vista a sua finalidade (sobretudo, e naturalmente, quando comparada com conservação generalizada), motivo pelo qual muitas vezes este método fica excluído enquanto solução única e isolada. A nível europeu, este método não é totalmente compatível com a jurisprudência do TJUE[32], que exige que a conservação desses dados seja limitada ao estritamente necessário e que esteja sujeita a garantias efetivas e a um controlo independente.

De resto, esta nova versão do diploma apenas altera o período de conservação dos dados de tráfego e localização (cujo exato período de conservação deve ser determinado na autorização judicial), mantendo o prazo de conservação de um ano, a contar da conclusão da comunicação, para os dados de base, assim como os endereços de IP.

Este regime merece, naturalmente, algumas críticas, como as que se exporão em seguida, bem como uma breve análise sobre a sua conjugação com o disposto na Lei n.º 41/2004.

A Lei n.º 41/2004 prevê que, pelo menos alguns dos dados de tráfego (desde que anonimizados) possam ser conservados pelas operadoras para efeitos de execução dos próprios contratos. Contrariamente ao que ocorria com a Lei n.º 32/2008, esta disposição estipula uma faculdade, e não uma obrigação, de os operadores conservarem tais dados.

---

[31] Que se traduz numa conservação para o futuro, desde o pedido do Ministério Público, válida apenas para o caso concreto, só podendo ser ordenada tendo como fundamento concreto a verificação de uma determinada suspeita. Em Portugal, é exemplo da utilização deste método o art. 12..º da Lei do Cibercrime.

[32] Por exemplo, Veja-se, por exemplo, o acórdão do Tribunal de Justiça da União Europeia, Tele2 Sverige AB contra Post och telestyrelsen, datado de 21 de dezembro de 2016, processo C203/15, disponível em https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=5157465.

Neste sentido, a Lei n.º 41/2004 prevê que os dados de tráfego necessários à faturação dos assinantes e ao pagamento de interligações só podem ser tratados até ao final do período durante a qual a fatura pode ser legalmente contestada ou o pagamento reclamado (que, de acordo com a Lei n.º 23/96 de 26 de julho – aplicável *ex vi* art. 6.º, n.º 3 da Lei n.º 41/2004 – é de seis meses). Tal significa que as operadoras podem conservar os dados de tráfego para efeitos de faturação e proteção comercial durante seis meses.

Não é, contudo, evidente, se a listagem de dados de tráfego que podem ser conservados ao abrigo da Lei n.º 41/2004 se justaponha totalmente ao catálogo de dados existente na Lei n.º 32/2008, sobretudo porque o grau de granularidade com que se lista os dados de tráfego a conservar é bastante distinta – ou seja, uma das listagens é muitíssimo mais concreta que a outra.

No limite, mesmo dentro da mesma categoria de dados de tráfego não é de excluir a possibilidade de se ter certos tipos de dados de tráfego que só podem ser conservados mediante a referida autorização judicial e outros tipos de dados de tráfego que podem ser conservados sem que tal seja necessário, desde que por associação à execução do contrato com o titular dos dados.

Também não é evidente se, guardando as operadoras todos os dados que legalmente *podem* guardar, com base na necessidade de faturação, se o Ministério Público se encontra legitimado, se assim entender, a requerer também esses dados.

Sem prejuízo do facto de quaisquer tratamentos efetuados pelas autoridades competentes, no âmbito da prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, se encontrarem excluídos do âmbito de aplicação material do Regulamento Geral sobre a Proteção de Dados ("RGPD"), tal como descrito no seu artigo 2.º, n.º 2, alínea d), qualquer tratamento de dados efetuado pelos prestadores de serviços de comunicações eletrónicas encontra-se, de todo o modo, sujeito ao RGPD.

Este diploma obriga a que os dados sejam tratados com um determinado fundamento de licitude que, por sua vez, se encontra ancorado na finalidade que justifica tal tratamento, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades (cfr. arts. 5.º, n.º 1, alínea b) e arts. 6.º).

Um dos fundamentos de licitude para o tratamento de dados pessoais, previstos pelo RGPD, no seu art. 6.º, é a obrigação legal. Com a Lei n.º 38/2008, existia uma obrigação legal de os operadores conservarem todos os metadados ali listados, durante o período de um ano, para finalidades de repressão de criminalidade grave, e, portanto, não se suscitavam dúvidas quanto à conformidade deste tratamento com o RGPD. Quando estes dados eram requeridos pelo Ministério Público, eram simplesmente entregues, sem que quaisquer questões se colocassem a este respeito.

Ora, atualmente, e com esta alteração de regime, esta obrigação legal de conservação inexiste relativamente a alguns dos dados de tráfego, ainda que continue a existir claramente relativamente a respeito dos dados de base.

Só que, para finalidades de execução do contrato e faturação, ao abrigo da Lei n.º 41/2004, os operadores podem continuar a conservar, pelo menos, muitos dos dados que eram conservados ao abrigo da Lei n.º 38/2008.

Quid iuris se o Ministério público solicita estes dados aos operadores? Por um lado, os dados não podem, ao abrigo do RGPD, ser tratados para outras finalidades que não aquelas para as quais são recolhidos, sem prejuízo de um eventual teste de compatibilidade; por outro, existe um dever de colaboração com as autoridades judiciárias, pelo que será difícil os operadores obviarem-se ao cumprimento desta obrigação, até porque este pedido poderá constituir, ele próprio, fundamento de licitude para o tratamento, enquanto obrigação legal.

A este respeito, e sendo difícil argumentar que os operadores se podem recusar a cumprir com tais pedidos, será também complicado não argumentar que não nos encontramos perante uma *porta lateral*

para a obtenção dos metadados, quando existe expressamente um regime muito particular a obedecer nesta matéria[33].

No demais, e por fim, de referir que não restam dúvidas que a Assembleia da República foi obrigada a tomar a decisão para assegurar que o crivo de constitucionalidade era ultrapassado e, nessa medida, foi bem-sucedida. Impõem-se, contudo, uma discussão importante sobre a ponderação e juízo de proporcionalidade feitos pelo TC.

Efetivamente, resulta das decisões aqui descritas do TC que os dois tipos de tratamentos de metadados – i.e. a conservação e o acesso – foram analisados de forma praticamente conjunta.

De referir, ainda assim, que o TC dedica parte do Acórdão n.º 268/2022 a justificar esta análise conjunta. Com efeito, apesar de admitir que a compressão nos direitos fundamentais não ocorre toda por igual nem no mesmo momento, o TC refere que "apesar de a sua simples conservação constituir, por si só, uma limitação daqueles direitos, a intensidade da restrição depende em boa medida das garantias inerentes à transmissão e acesso a esses dados"[34]. É certo que esta já havia sido a posição tomada pelo Acórdão n.º 420/2017, mas também será injusto dizer, como referiu o TC, que não se identificam motivos para alterar esta abordagem.

A Provedora de Justiça, quando apresentou o pedido de apreciação ao TC, havia argumentado em sentido diverso e a sua argumentação justifica, no mínimo, uma ponderação redobrada a este respeito. No seu entender, "perante a existência de dois momentos autónomos de

---

[33] Ver a este respeito o Acórdão da Tribunal da Relação do Porto, de 7 de dezembro de 2022, cujo n..º do processo é 5011/22.2JAPRT-A.P1, e o relator Pedro Vaz Pato, disponível em Acórdão do Tribunal da Relação do Porto (dgsi.pt), no qual o Tribunal esclarece que "tendo o acórdão do Tribunal Constitucional declarado a inconstitucionalidade, com força obrigatória geral, dos arts. 4..º, 6..º e 9..º da Lei n..º 32/2008, de 17 de julho (Lei relativa à conservação de dados gerados ou tratados no contexto de oferta de serviços de comunicações eletrónicas), não podemos tentar tornear esse acórdão, *deixando entrar pela janela* aquilo a que ele *fechou a porta*; ou seja, não podemos recorrer a outras normas para obter o mesmo efeito que resultaria da aplicação das normas declaradas inconstitucionais sem que essas outras normas contenham aquelas garantias que faltam a estas e que levaram a essa declaração de inconstitucionalidade."

[34] Acórdão n..º 286/22, § 14, a respeito do processo n..º 828/2019, cujo relator é Conselheiro Afonso Patrão, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html

agressão aos direitos, não é de todo legítimo confundi-los de acordo com uma *lógica de compensação".*

Assim, entendia a Provedora de Justiça que uma dogmática correta de direitos fundamentais exigiria que o TC analisasse*, "*autonomamente, a conformidade constitucional de cada uma das agressões aos direitos, em nada podendo o regime de acesso e de utilização dos dados interferir na análise da conformidade constitucional, designadamente e no que respeita as exigências decorrentes do princípio da proporcionalidade, da agressão aos direitos implicada na própria imposição legal de conservação de dados*".*

Acresce que, além de se tratar de dois momentos de agressão diferentes, a intensidade da sua agressão não é comparável. É inegável que, ainda que exista necessariamente uma compressão do direito fundamental à privacidade com a conservação dos dados, a gravidade da mesma não é, nem pode ser, comparável à compressão que existe no caso do acesso desses mesmos dados. Por outras palavras: se os dados forem conservados, é inegável que há um perigo de acesso indevido que lhes subjaz, do qual é difícil de fugir; contudo, também não é possível ignorar que é o próprio acesso em si que comprime em larga medida o direito à privacidade, porque, no limite, se ninguém aceder a tais dados, não há como o direito à privacidade ser violado.

O problema da análise conjunta é o perigo da atribuição de uma gravidade inconsistente com a compressão que a conservação efetivamente representa e confundir a agressão perpetuada pelo acesso com a da conservação. Ao analisar-se a conservação à luz dos perigos do acesso, a análise da proporcionalidade, na ponderação de valores na balança ficará, inevitavelmente, distorcida, pelo simples facto de que se está a atribuir uma intensidade de agressão à conservação que não lhe pertence.

Ademais, sendo os perigos do acesso manifestamente mais significativos do que o da mera conservação, mas atribuindo os primeiros à segunda, a tendência vai ser obviamente de considerar que esta é

injustificável, o que, por sua vez, poderá levar-nos a concluir que a conservação não é legítima quando, na verdade, até pode ser.

O próprio acórdão Digital Rights Irelands sublinha, precisamente, que o conteúdo essencial do direito fundamental não é afetado em face das medidas de proteção que são implementadas. Efetivamente, refere o TJUE que "conservação dos dados também não é suscetível de afetar o conteúdo essencial do direito fundamental à proteção dos dados pessoais, consagrado no artigo 8.º da CDFUE, uma vez que a Diretiva 2006/24 prevê, no seu artigo 7.º, uma regra relativa à proteção e à segurança dos dados, o que obriga a que sejam respeitados certos princípios de proteção e de segurança dos dados pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, princípios de acordo com os quais os EstadosMembros devem assegurar a adoção de medidas técnicas e organizacionais adequadas contra a destruição acidental ou ilícita, a perda ou a alteração acidental dos dados"[35].

Não foi, contudo, este o entender do TC. De resto, e pelo menos para já, a questão parece ter ficado disciplinada com este novo regime.

5. CONCLUSÕES

O presente artigo visava, por um lado, oferecer um enquadramento simples – dentro daquilo que são os limites de um tema, por natureza, complexo – sobre a temática dos metadados. Em particular, procurou-se refletir sobre as preocupações e discussões que têm tido lugar nos últimos anos a este respeito, nomeadamente nos Acórdãos do TC e do TJUE. Por outro lado, discutiu-se, de forma

[35] Tribunal de Justiça da União Europeia, Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, §40, datado de 8 de abril de 2014, processos apensos C293/12 e C594/12, disponível em https://curia.europa.eu/juris/document/document.jsf;jsessionid=3CE25888D6478AA3CC9ED7B78735A64F?text=&docid=150642&pageIndex=0&doclang=pt&mode=req&dir=&occ=first&part=1&cid=2712231

muito breve, o regime atual – também dentro dos limites do que é possível analisar nesta fase a este respeito, em que a realidade prática não é, ainda, possível de conhecer na sua totalidade.

Conforme descrito ao longo deste artigo, a discussão em torno dos metadados no contexto das comunicações eletrónicas, bem como da definição dos limites e das garantias da conservação e do acesso a esses dados tem sido particularmente longa e controversa, quer a nível europeu, quer a nível nacional.

Considerando a evolução legislativa e jurisprudencial em ambas as vertentes, antevê-se que a evolução dinâmica que se assistiu nos últimos anos relativamente ao enquadramento jurídico dos metadados ainda se mantenha futuramente, exigindo, para já, uma constante ponderação entre os diferentes valores e interesses envolvidos, nomeadamente ao nível dos tribunais, e uma adaptação com o peso e medida das novas realidades tecnológicas e sociais que vão tendo lugar.

No que respeita, em específico, ao novo regime aprovado relativamente aos metadados, através Lei n.º 18/2024, de 5 de fevereiro, e embora este seja, como ficou patente, merecedor de críticas, parece resolver, no imediato, as questões apontadas pelo TC. Sem prejuízo, só a sua aplicação prática dirá se as questões relativas a esta temática ficaram, de forma definitiva, resolvidas.

Publicidade e Transparência no âmbito do Regulamento dos Serviços Digitais (Regulamento (UE) 2022/2065 de 19 de Outubro)

Maria Madruga de Medeiros

Resumo

De forma a acompanhar a evolução da tecnologia e o consumo em linha, a Comissão Europeia propôs o novo (e já em vigor) Regulamento (UE) dos Serviços Digitais, que, de entre outras áreas, incide-se sobre a publicidade em linha.

Deste modo, este artigo tem como objectivo analisar os efeitos da publicidade direccionada e as normas do Regulamento (UE) dos Serviços Digitais referentes à transparência de informação. Para além disso, irá ser feita uma reflexão sobre os principais desafios da aplicação destas novas regras.

Palavras-chave: *Regulamento dos Serviços Digitais; Transparência; Publicidade em linha; Publicidade direccionada.*

Abstract

To keep up with the evolution of technology and online consumption, the European Commission has proposed the new (and already in force) Digital Services Regulation (EU), which, among other areas, focuses on the display of online advertising.

The aim of this article is therefore to analyze the effects of targeted advertising and the rules of the (EU) Digital Services Regulation relating to transparency of information. It will also reflect on the main challenges of applying these new rules.

Keywords*: Digital Services Act; Transparency; Online Advertising; Targeted Advertising.*

Lista de abreviaturas, siglas e acrónimos

AEPD	–	Autoridade Europeia para a Protecção de Dados
cfr.	–	confrontar
DSA	–	Regulamento dos Serviços Digitais
DMA	–	Regulamento dos Mercados Digitais
GT29	–	Grupo de Trabalho do Artigo 29.º
p.	–	Página
RGPD	–	Regulamento Geral sobre Protecção de Dados
TJUE	–	Tribunal de Justiça da União Europeia
VLOPs	–	Plataformas em linha de muito grande dimensão
VLOSEs	–	Motores de pesquisa em linha de muito grande dimensão

Introdução

Ao longo dos últimos anos, surgiram serviços digitais novos e inovadores da sociedade da informação que mudaram a vida quotidiana dos cidadãos da União Europeia. De forma a acompanhar estas mudanças, a Comissão Europeia comprometeu-se a actualizar e harmonizar as responsabilidades e as obrigações dos prestadores de serviços digitais e, em especial, das plataformas em linha[1]. Este compromisso foi materializado com o Regulamento dos Mercados Digitais (*Digital Market Act* – DMA)[2] e com o Regulamento dos Serviços Digitais (*Digital Services Act* – DSA)[3].

Em paralelo com a evolução das actividades económicas em linha, também a temática da publicidade tem vindo a renovar-se nas plataformas em linha, com anúncios mais subtis e mais direccionados para cada grupo de pessoas. A publicidade em linha poderá originar danos nocivos sobre os dados pessoais dos destinatários do serviço, nomeadamente sobre grupos de pessoas considerados mais sensíveis e sobre os dados pessoais dos destinatários, justificando deste modo a criação de novas regras aplicáveis às plataformas em linha no DSA. Estas regras e obrigações constituem o foco deste artigo.

A primeira parte é dedicada aos objectivos e ao âmbito de aplicação do DSA, sendo dada especial atenção às plataformas em linha, às plataformas em linha de muito grande dimensão (VLOPs[4]) e aos motores de pesquisa em linha de muito grande dimensão (VLOSEs[5]). De seguida, entramos na área da publicidade em linha, na qual é feita a análise das normas dos art. 26.º e 39.º do DSA. Esta última parte

---

[1] Comissão Europeia, Shaping Europe's digital future, 19.02.2020, p. 6. Disponível em https://commission.europa.eu/document/download/84c05739-547a-4b86-9564-76e834dc7a49_en?filename=communication-shaping-europes-digital-future feb2020_en.pdf&prefLang=pt

[2] Regulamento (UE) 2022/1925, de 14 de Setembro de 2022.

[3] Regulamento (UE) 2022/2065, de 19 de Outubro de 2022.

[4] *Very large online platforms* (VLOPs).

[5] *Very large online search engines* (VLOSEs).

incidirá sobre as obrigações de transparência e regras sobre a exibição de publicidade para os fornecedores das plataformas em linha e as respectivas reacções das Instituições Europeias e outras entidades. Por fim, proceder-se-á ao elenco dos principais desafios da aplicação deste Regulamento.

I – Considerações gerais sobre o Regulamento (UE) sobre os Serviços Digitais

1. Fundamentos e objectivos

A 15 de Dezembro de 2020, a Comissão Europeia, no âmbito da Estratégia Digital Europeia "Construir o futuro digital da Europa", publicou duas propostas de regulamentação relacionadas com a governação dos serviços digitais na União Europeia (UE): o DSA e o DMA[6]. De acordo com a Comissão Europeia, estas propostas legislativas teriam como objectivo "assegurar as melhores condições para a prestação de serviços digitais inovadores no mercado interno, contribuir para a segurança em linha e para a protecção dos direitos fundamentais e criar uma estrutura de governação sólida e duradoura para a supervisão eficaz dos prestadores de serviços intermediários" [7].

O DSA visa harmonizar as legislações nacionais fragmentadas sobre serviços intermediários e criar regras ao nível da UE para um ambiente em linha seguro, previsível e de confiança[8]. Este Regulamento tem também como objectivo proteger os direitos fundamentais dos consumidores e criar um quadro transparente de

[6] Comissão Europeia, Uma Europa preparada para a era digital: Comissão propõe novas regras para as plataformas digitais, 15.12.2020. Disponível em https://ec.europa.eu/commission/presscorner/detail/pt/ip_20_2347.

[7] Proposta de Regulamento do Parlamento Europeu e do Conselho Relativo a um Mercado Único de Serviços Digitais (Regulamento Serviços Digitais) e que altera a Diretiva 2000/31/CE (COM/2020/825 Final), p. 2–3.

[8] Considerando 9 do DSA.

responsabilização para os prestadores de serviços intermediários[9]. O DSA é aplicável a um vasto número de intermediários e plataformas em linha que ligam os consumidores a bens, serviços e conteúdos. Este Regulamento trata desde sítios *web* simples a grandes serviços de infraestruturas e plataformas em linha[10].

1.1 Plataformas em linha

Neste contexto, destacam-se os fornecedores de plataformas em linha por serem os destinatários das regras do DSA referentes à publicidade, que é o foco do presente artigo.

Uma plataforma em linha (alínea i) do art. 3.º do DSA) é, em termos gerais, um serviço de alojamento virtual[11], que armazena informações a pedido de um destinatário do serviço e, para além disso, difunde para o público a pedido do mesmo. Este serviço de armazenamento e difusão ao público terá de constituir a principal actividade da plataforma, excluindo assim, por exemplo, sítios *web* que tenham secções de comentários mas que sejam acessórios à finalidade do mesmo[12] e serviços de comunicações interpessoais[13], tais como serviços de correio electrónico e serviços de mensagens privadas[14].

Plataformas em linha são, assim, serviços que reúnem vendedores/anunciantes e consumidores, como por exemplo, mercados em

---

[9] Considerando 40 do DSA.

[10] Como referido no seu art. 2.º, o DSA é aplicável aos serviços intermediários (inclui serviços de "simples transporte", de "armazenagem temporária" e de "alojamento virtual") oferecidos aos destinatários do serviço cujo local de estabelecimento seja na União ou que nela estejam localizados, independentemente de onde os prestadores desses serviços têm o seu local de estabelecimento.

[11] De acordo com a subalínea iii) da alínea g) do art. 3.º do DSA, um serviço de alojamento virtual consiste na "armazenagem de informações prestadas por um destinatário do serviço e a pedido do mesmo".

[12] Por exemplo, um sítio *web* de um jornal. Considerando 13 do DSA.

[13] Tal como definido no, alínea 5) do art. 2.º da Diretiva (UE) 2018/1972, de 11 de dezembro de 2018.

[14] Considerando 14 do DSA.

linha, lojas de aplicações, plataformas de economia colaborativa e plataformas de redes sociais[15].

1.2 Plataformas e motores de pesquisa em linha de muito grande dimensão (VLOPs e VLOSEs)

No DSA estão incluídas obrigações adicionais para as plataformas de muito grande dimensão (VLOPs) e motores de pesquisa[16] de muito grande dimensão (VLOSEs).[17]

O termo "muito grande dimensão", de acordo com o n.º 1 do art. 33.º do DSA, refere-se ao número médio mensal de destinatários activos do serviço na União, que deverá reflectir todos os destinatários que, efectivamente utilizam o serviço, pelo menos uma vez, num determinado período[18] e que deve ser igual ou superior a 45 milhões. Este número deverá ser comunicado pelas próprias plataformas e motores de pesquisa na sua interface em linha (n.º 2 do art. 24.º DSA), tendo a Comissão Europeia de publicar uma lista (e mantê-la actualizada) das VLOPs e dos VLOSEs no Jornal Oficial da UE e notificar os mesmos sobre a sua decisão (n.os 4, 5 e 6 do art. 33.º DSA). Depois da notificação, as VLOPs e os VLOSEs designados terão 4 meses para cumprir as suas obrigações adicionais (n.º 6 do art. 33.º DSA). A primeira lista foi designada a 25 de

---

[15] Comissão Europeia, Regulamento dos Serviços Digitais – Garantir um ambiente em linha seguro e responsável. Disponível em https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_pt

[16] Definição de motor de pesquisa encontra-se na alínea j) do art. 3.º do DSA. Um exemplo muito conhecido será a plataforma "Google".

[17] Notemos que o DSA aplica-se a plataformas em linha de todas as dimensões (variando de acordo com as secções do Regulamento), no entanto, o mesmo não se aplica a motores de pesquisa que não são considerados VLOPs. No âmbito do DSA, a única obrigação que os motores de pesquisa que não são VLOPs parecem ter de cumprir é a de publicação de informações sobre o número médio mensal de destinatários ativos do serviço na União e a sua comunicação à Comissão e coordenador de serviços digitais (n.º 2 e 3 do art. 24.º DSA).

[18] Considerando 77 do DSA.

Abril de 2023[19], tendo as VLOPs e os VLOSEs de cumprir as obrigações fixadas na secção 5 do Capítulo III do DSA desde 25 de agosto de 2023.

Dado o impacto que as VLOPs e os VLOSEs têm no debate público, nas transacções económicas, na difusão de informação e influência do público a grande escala, existe uma maior probabilidade de originarem riscos sociais de grande dimensão[20]. Os legisladores do DSA justificam assim uma maior exigência na actuação das VLOPs e dos VLOSEs, criando obrigações adicionais para os fornecedores destas.

II – Publicidade no âmbito do Regulamento dos Serviços Digitais

1. Enquadramento

De acordo com um estudo do *International Bureau of Advertising*, na UE, o mercado da publicidade em linha tem vindo a crescer nos últimos quinze anos, em média, 4 mil milhões de euros por ano, passando de 7,6 mil milhões de euros em 2006 para 64,8 mil milhões de euros em 2019[21].

Os comerciantes em linha começaram a adoptar práticas que se centram na melhoria da compreensão do comportamento e das necessidades dos consumidores, fornecendo ofertas personalizadas e adaptadas através da utilização de dados pessoais destas[22]. Como

---

[19] A lista foi publicada a 14 de julho de 2023 em jornal oficial da UE e inclui como VLOPs as entidades *Alibaba Aliexpress; Booking.com; Facebook; LinkdIn; Instagram*, entre outros. A Comissão designou como VLOSEs o *Bing* e o *Google Search*.

[20] Considerando 75 e 76 do DSA.

[21] Estudo disponível em https://iabeurope.eu/iab-europe-adex-benchmark-2019-study-reveals-european-digital-advertising-market-exceeds-e64bn-in-2019/

[22] Comissão Europeia, Consumer Market Study on Online Market Segmentation through Personalised Pricing/Offers in the European Union, EB-04-18-559-EN-N, 25.09.2018, p. 33. Disponível em https://op.europa.eu/en/publication-detail/-/publication/ed9ce056-c2cf-11e8-9424--01aa75ed71a1/language-en

resultado das práticas de personalização, as empresas podem maximizar os lucros, uma vez que são capazes de estimar com maior exactidão o preço máximo que os consumidores estão dispostos a pagar por um produto, com base nos dados recolhidos sobre eles[23].

Esta percepção está reflectida no considerando 68 do DSA, no qual, é reconhecido que a publicidade em linha desempenha um papel importante para os serviços das plataformas em linha que, muitas vezes, são total ou parcialmente financiadas por receitas de publicidade. No entanto, é referido que podem ocorrer riscos como a divulgação de conteúdos ilegais e exibição discriminatória de anúncios. Para além disso, a personalização da publicidade torna possível uma selecção precisa e rigorosa dos receptores dos mesmos, podendo dar origem a problemas de discriminação e práticas pouco transparentes de recolha e tratamento de dados pessoais dos destinatários[24].

Deste modo, o DSA[25/26] defende uma maior transparência e controlo no visionamento de publicidade, nas interfaces em linha.

Antes de passar para os artigos do DSA referentes à publicidade em linha é de referir que a utilização de dados pessoais para a publicidade direccionada, leva inevitavelmente ao recurso ao RGPD[27]

---

[23] *Idem.*

[24] Carvalho, Jorge Morais; Lima, Francisco Arga; Farinha, Martim, "Introdution to the Digital Services Act, Content Moderation and Consumer Protection", *Revista de Direito e Tecnologia*, Volume III-1, 2021, p. 98. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3852280.

[25] De notar que, de acordo com o art. 19.º, os artigos que irão ser indicados não são aplicáveis a plataformas em linha que sejam consideradas micro ou pequenas empresas tal como definidas na Recomendação 2003/361/CE.

[26] A UE tem vindo a desenvolver legislação que afecta (directa ou indirectamente) a actividade publicitária digital como a Directiva relativa às Práticas Comerciais Desleais, a Directiva relativa aos direitos dos consumidores e o Regulamento Europeu dos Mercados Digitais. Para além disso, refere-se também o Regulamento Inteligência Artificial (entrada em vigor a 1 de agosto de 2024 e aplicável a partir de 2 de agosto de 2026) que irá influenciar a área da publicidade, nomeadamente no que toca às proibições de uso de sistemas IA com potencial significativo para manipular as pessoas ou explorar as vulnerabilidades de grupos específicos e nas obrigações de transparência.

[27] Regulamento (UE) 2016/679, de 27 de abril de 2016.

sendo este um complemento do DSA nas áreas do direito da informação e da publicidade em linha.

Para a publicidade em linha que use dados pessoais, a base de licitude mais provável é o consentimento (alínea a), do n.º 1 do art. 6.º RGPD) [28]. Nos termos do ponto 11 do art. 4.º do RGPD, o consentimento consiste numa manifestação de vontade, livre, específica, informada e inequívoca. Um recente acórdão do TJUE[29] demonstra este fundamento de licitude como a alternativa mais segura para os titulares dos dados. De forma muito sucinta, uma das questões que o acórdão revelou foi o facto de os utilizadores da rede social em linha *Facebook* terem de, no momento do seu registo, aceitar as condições gerais estabelecidas pela *Meta Platforms*, que remetem para as políticas de utilização dos dados e dos testemunhos de conexão (*cookies*) fixados pela referida sociedade, que incluiria recolha de dados pessoais dentro e fora da rede social para publicidade personalizada. Só com a aceitação destas condições é que os utilizadores conseguiriam registar-se no *Facebook*. Neste acórdão, o TJUE analisa cada um dos fundamentos de licitude geral do tratamento de dados pessoais presentes no RGPD, relativamente ao uso dos dados pessoais para publicidade em linha. O TJUE concluiu que os utilizadores da rede social em questão devem dispor da liberdade de recusar tratamento de dados pessoais não necessários à execução do contrato (como o referido *supra*) sem que, no entanto, sejam obrigados a renunciar integralmente à utilização desta rede social. Destaca-se ainda, a análise sobre o fundamento de interesse legítimo (cujo considerando 47 do RGPD refere como possível fundamento de licitude para a comercialização directa) em que o TJUE afirma que, na falta de consentimento, os interesses e os direitos fundamentais dos utilizadores prevalecem sobre o interesse do operador de uma rede social

[28] CAPELLO, M. (ed.) – "New Actors and Risks in Online Advertising", IRIS Special, European Audiovisual Observatory, 2022, p. 25. Disponível em https://rm.coe.int/iris-special-1-2022en-onlineadvertising/1680a744d7

[29] TJUE, C-252/21, Meta Platforms e o., 04.07.2023

em linha na personalização da publicidade através da qual financia a sua actividade[30].

Havendo licitude para o processamento de dados, o RGPD impõe uma série de outras obrigações relevantes para a publicidade em linha. Em primeiro lugar, as pessoas devem receber informações sobre, por exemplo, como e por quem os seus dados são processados, a duração da conservação destes dados, com quem são partilhados, entre outros (art. 12.º a 14.º)[31]. Em segundo lugar, os responsáveis pelo tratamento devem cumprir as obrigações destinadas a limitar os riscos do tratamento de dados, incluindo as relacionadas com a minimização dos dados (alínea c) do n.º 1 do art. 5.º), a confidencialidade (alínea f) do n.º 1 do art. 5.º) e a protecção de dados desde a concepção e por defeito (art. 25.º)[32]. Por último, os responsáveis pelo tratamento de dados só podem transferir dados pessoais para fora da União se existirem garantias adequadas para o efeito (art. 44.º)[33].

2. Normas relativas à publicidade no Regulamento dos Serviços digitais

2.1. Transparência sobre a publicidade nas plataformas em linha (n.º 1 do art. 26.º DSA)

Como já referido, o legislador do DSA optou pela via da transparência relativamente à publicidade nas plataformas em linha. Deste modo, o n.º 1 do art. 26.º do DSA indica que os fornecedores de plataformas em linha devem informar, nas suas interfaces[34], de forma

[30] TJUE C-252/21, cit., parágrafo 117.

[31] Capello, "New Actors…" cit., p. 25.

[32] *Idem.*, p. 25–26.

[33] *Idem*, p. 26.

[34] Interfaces são qualquer "software, nomeadamente um sítio Internet, parte de um sítio Internet ou uma aplicação, explorado por um operador económico ou em seu nome, que dá aos utilizadores finais acesso aos produtos do operador económico", como referido no art. 3.º do Regulamento (UE) 2019/1020. Como exemplo, poderemos referir o *feed* de notícias de uma rede social.

clara, concisa e inequívoca, e em tempo real, de que o que os destinatários[35] estão a ver é um anúncio, quem exibe o anúncio e porque o exibe. [36]

A alínea a) do n.º 1 do art. 26.º do DSA refere que o fornecedor de uma plataforma em linha deverá demonstrar que "as informações constituem um anúncio publicitário, nomeadamente através de sinalização bem visível, a qual pode seguir normas nos termos do artigo 44.º"[37].

A publicidade[38] tem um elemento de remuneração que envolve as plataformas, excluindo assim qualquer publicidade fora da plataforma (por exemplo, contractos entre marcas e influenciadores que não são mediados pela rede social a que o influenciador apresenta o produto)[39/40]. Nestes casos, os próprios destinatários que fizeram o contrato fora da plataforma poderão declarar que o conteúdo

---

[35] Destinatários do serviço são "qualquer pessoa, singular ou colectiva que utilize um serviço intermediário, em especial para procurar informação ou para torná-la acessível." (Alínea b) do art. 3.º do DSA).

[36] Como referido pelo considerando 68, este artigo complementa o art. 6.º da Directiva sobre o Comércio Electrónico sobre as condições das comunicações (Directiva 2000/31/CE, de 8 de junho de 2000). Permanecem assim em vigor as regras sobre identificação e informação, reflectidas no art. 21.º do Decreto-Lei n.º 7/2004, de 7 de Janeiro. Leitão, Luís Manuel Teles de Menezes, *Digital Services ACT (DSA) – O Regulamento Europeu 2022/2065 sobre os Serviços Digitais*, 1.ª. ed. Almedina, 2023, p. 68.

[37] Art. 44.º é relativo à promoção, pela Comissão Europeia, de normas facultativas estabelecidas pelos organismos de normalização europeus e internacionais.

[38] De acordo com o ponto r) do art. 3.º, um anúncio publicitário define-se por "informações concebidas para promover a mensagem de uma pessoa singular ou colectiva, independentemente de visarem objectivos comerciais ou não comerciais, e apresentadas por uma plataforma em linha na sua interface em linha mediante remuneração, especificamente paga para promover essas informações"

[39] Goanta, Catalina, "Now What: Exploring the DSA's Enforcement Futures in Relation to Social Media Platforms and Native Advertising", *Verfassungsblog*, 2022, parágrafo 16. Disponível em https://verfassungsblog.de/dsa-now-what/>. Goanta, Catalina, "Human Ads Beyond Targeted Advertising: Content Monetization as the Blind Spot of the Digital Services Act" *Verfassungsblog*, 2021, parágrafo 4. Disponível em https://doi.org/10.17176/20210905-213932-0>

[40] Isto levou a que autoridades, como o Ministério da Economia belga, pedissem aos *influencers* das redes sociais para cumprirem os deveres de informação a que os comerciantes estão normalmente sujeitos (por exemplo, revelação da identidade do comerciante, endereço físico), como resultado da aplicação da Diretiva de Direitos do Consumidor (CRD) e da Diretiva de Práticas Comerciais Desleais (UCPD). Goanta, "Now What…"cit., parágrafo 15.

publicado constitui uma comunicação comercial, de acordo com o n.º 2 do art. 26.º do DSA.

De notar que, de acordo com o considerando 68, um anúncio publicitário pode constituir ele próprio um conteúdo ilegal[41], podendo as plataformas em linha, neste caso, actuar nos termos do art. 23.º do DSA, relativa a medidas de protecção contra a utilização abusiva.

Por sua vez, de acordo com as alíneas b) e c) do art. 26.º do DSA, os fornecedores de plataformas em linha deverão indicar a pessoa singular ou colectiva em cujo nome o anúncio publicitário é apresentado e, se diferente, a pessoa singular ou colectiva que paga o anúncio publicitário.

Na proposta da Comissão sobre o DSA, no art. 24.º estava somente referido que o destinatário deveria ser informado sobre a pessoa singular ou colectiva em cujo nome o anúncio publicitário é exibido[42]. Por sua vez, a Autoridade Europeia para a Protecção de Dados (AEPD) referiu que não era claro se este preceito incluiria possíveis terceiros que entregassem o anúncio à plataforma em linha (por exemplo, uma agência publicitária)[43]. A alínea foi assim completada em conformidade, de forma a garantir que o destinatário conheça todas as entidades por detrás do anúncio.

A alínea d) refere que, os fornecedores das plataformas em linha devem informar sobre quais os principais parâmetros utilizados para determinar o destinatário da exibição do anúncio publicitário e se for caso disso, como alterá-los. Na proposta da Comissão sobre o DSA, a AEPD sugeriu que se substituísse a referência "principais parâmetros" por "parâmetros" e que, simultaneamente se

---

[41] A alínea h) do art. 3.º define conteúdos ilegais como "quaisquer informações que, por si só ou em relação a uma atividade, incluindo a venda de produtos ou a prestação de serviços, não estejam em conformidade com o direito da União ou com o direito de qualquer um dos Estados-Membros que seja conforme com o direito da União, independentemente do objeto ou da natureza precisa desse direito."

[42] COM/2020/825 Final.

[43] AEPD, Opinion 1/2021 on the Proposal for a Digital Services Act, 2021, parágrafo 64. Disponível em https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf.

esclarecesse melhor o seu sentido[44]. A versão final manteve o termo "principais parâmetros". Por sua vez, servindo de guia para a sua definição, o considerando 68 refere que as explicações sobre a lógica utilizada para exibir determinado anúncio deverão incluir informações sobre o método utilizado, como por exemplo, a publicidade direccionada e, se for o caso, os principais critérios de definição de perfis aplicados.

Ora, no contexto em linha, os utilizadores podem ser estudados com base nos dados que forneceram, bem como em informações recolhidas sobre o seu comportamento digital[45]. Isto permite que os anunciantes mostrem os seus anúncios apenas aos indivíduos do público para os quais o anúncio é relevante, aumentando assim a probabilidade de os seus anúncios resultarem numa venda[46]. Neste contexto, a publicidade direccionada é uma prática de *marketing* que utiliza dados sobre indivíduos para seleccionar e apresentar anúncios ou outras formas de conteúdo comercial[47]. Como indicado no considerando 68, a publicidade poderá ser contextual (com base no conteúdo do sítio *web* em que se encontram), comportamental (com base na observação do comportamento do utilizador em linha – sítio visitado, cliques, etc.) ou de outro tipo[48/49], como publicidade segmentada (com base nas características que o utilizador forneceu, por

---

[44] *Idem*, parágrafo 67.

[45] Parlamento Europeu, Regulating Targeted and Behavioural Advertising in Digital Services: How to Ensure Users' Informed Consent, PE 694.680, setembro 2021, p. 23–24. Disponível em https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694680/IPOL_STU(2021)694680_EN.

[46] Ranganathan, Nayanatara, "Regulating Influence, Timidly", *Putting the DSA into Practice,* Verfassungsbooks, 2023, p. 206. Disponível em https://doi.org/10.17176/20230208--093135-0; Capello, "New Actors…"cit., p. 52.

[47] Parlamento Europeu, Regulating Targeted… cit., p. 10.

[48] De notar que a versão em inglês indica somente publicidade contextual ou de outro tipo ("*whether it is contextual or other type of advertising*"). Considerando 68 do DSA.

[49] Pop, Florina; Bezemer, Jannigje; Grant, Laura, "The Digital Services Act: Creating Accountability for Online Platforms and Protecting Users' Rights?", *European Institute of Public Administration*, 2022, Parte II-Key definitions. Disponível em https://www.eipa.eu/blog/the-digital-services-act-creating-accountability-for-online-platforms-and-protecting-users--rights/

exemplo, aquando do registo em sítios Web e que pode conter dados pessoais como a idade, a localização, etc.)[50].

No entanto, a publicidade direccionada pode permitir que os anunciantes tirem partido indevido das vulnerabilidades dos consumidores individuais[51]. A falta de transparência sobre o funcionamento dos algoritmos utilizados pode também impedir que os legisladores, os indivíduos e os próprios anunciantes saibam como os anúncios são exibidos aos destinatários[52]. Deste modo, é necessário reforçar o facto de a publicidade direccionada requerer dados pessoais sobre os indivíduos visados para poder funcionar, daí a importância de informar os destinatários e dar a oportunidade aos mesmos para alterar os critérios usados pelos serviços digitais[53].

2.2 Declaração sobre comunicações comerciais (n.º 2 do art. 26.º DSA)

No n.º 2 do art. 26.º do DSA é referido que os fornecedores de plataformas em linha devem facultar aos destinatários do serviço uma funcionalidade que lhes permita declarar se os conteúdos que estão a disponibilizar constituem ou contém comunicações comerciais. Este número promove assim a transparência entre destinatários do serviço, requerendo que, no caso de o destinatário apresentar tal declaração o fornecedor da plataforma em linha assegure que os outros destinatários do serviço possam identificar de forma clara e inequívoca, e em tempo real, que o conteúdo apresentado constitui ou contém comunicações comerciais.

De acordo com o considerando 68 do DSA, este regulamento complementa a aplicação da Directiva sobre Serviços de Comunicação Social Audiovisual[54], que impõe medidas destinadas a permitir que

---

[50] A Comissão Europeia acrescenta este tipo de publicidade direccionada no seu estudo – Consumer Market Study …cit., p. 31.

[51] Capello, "New Actors …"cit., p. 52.

[52] *Idem*.

[53] *Idem*.

[54] Directiva 2010/13/UE, de 10 de março de 2010.

os utilizadores declarem a presença de comunicações comerciais audiovisuais em vídeos gerados pelos utilizadores e, complementa igualmente as obrigações dos comerciantes em matéria de divulgação de comunicações comerciais decorrentes da Directiva relativa às práticas comerciais desleais[55].

2.3 Uso de categorias especiais de dados pessoais para publicidade em linha (n.º 3 do art. 26.º do DSA)

Por sua vez, o n.º 3 do art. 26.º proíbe a exibição de anúncios publicitários com base na definição de perfis, utilizando categorias especiais de dados, nos termos do n.º 1 do art. 9.º do RGPD[56/57].

O termo "definição de perfis" não está densificado no DSA, tendo a sua definição sido remetida para o n.º 4 do art. 4.º do RGPD[58]. Em termos sucintos, a definição de perfis pode ser entendida como o processamento de dados pessoais utilizando algoritmo de forma a prever as preferências em linha do utilizador e os seus hábitos de navegação[59].

Esta técnica de direccionamento optimizada para corresponder aos interesses e apelar potencialmente às vulnerabilidades dos destinatários de serviço pode originar efeitos negativos, tais como campanhas de desinformação e discriminação de certos grupos[60].

---

[55] Directiva 2005/29/CE, de 11 de maio de 2005.

[56] Isto é, dados que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, 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.

[57] De referir que o n.º 2 do art. 28.º DSA também proíbe a exibição anúncios publicitários com base na definição de perfis utilizando dados pessoais do destinatário do serviço se tiverem conhecimento, com uma certeza razoável, de que este é um menor.

[58] "qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspectos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações"

[59] Pop, Bezemer, Grant, "The Digital Services Act…"cit., Parte II-Key definitions.

[60] Considerando 69 DSA.

O GT29 já terá referido que os efeitos da apresentação de publicidade com base na definição de perfis podem fazer-se sentir em função das características específicas de cada caso, tendo em conta a dimensão intrusiva do processo de definição de perfis, as expectativas das pessoas em causa, a forma como o anúncio é apresentado ou a utilização de vulnerabilidades conhecidas dos titulares de dados visados[61]. Para além disso, refere ainda que este tratamento, mesmo passível de ter, de modo geral, um impacto reduzido nas pessoas pode, na verdade, ter efeitos significativos em certos grupos da sociedade, designadamente em grupos minoritários ou adultos vulneráveis[62].

Adaptando esta posição para o presente DSA, o facto de o mesmo proibir a exibição de anúncios com base na definição de perfis somente quando são utilizadas categorias especiais de dados pessoais, exclui certos dados pessoais que, mesmo não integrando as categoriais especiais de dados (como dados bancários) poderão ser considerados dados sensíveis[63]/[64]. Deste modo, a definição de perfis sendo um instrumento de publicidade bastante intrusivo, deveria ter sido objecto de uma proibição com um âmbito mais abrangente.

---

[61] GT29, Orientações sobre as Decisões Individuais Automatizadas e a Definição de Perfis para efeitos do Regulamento (UE) 2016/679, wp251rev.01, 2016, p. 24. Disponível em https://ec.europa.eu/newsroom/article29/items/612053.

[62] *Idem*.

[63] Veja-se o exemplo de uma pessoa que se encontre numa situação conhecida ou provável de dificuldade financeira e que lhe seja dirigido regularmente anúncios de empréstimos com juros altos, havendo a possibilidade subscrever essas ofertas e, eventualmente, incorrer num maior endividamento. GT29, Orientações Sobre as Decisões…cit., p. 24.

[64] Griffin, Rachel, "Tackling Discrimination in Targeted Advertising: US Regulators Take Very Small Steps in the Right Direction – but Where Is the EU?" *Verfassungsblog*, 2022, parágrafo 20-21. Disponível em https://doi.org/10.17176/20220623-153440-0.and has promised new tools to ensure more representative targeting. This US lawsuit should be a wake-up call for European regulators, reminding them that taking systemic discrimination seriously requires proactive regulatory reform and enforcement. The relevant provisions of the Digital Services Act (DSA A autora defende que o DSA mostra uma compreensão muito simplista da discriminação algorítmica. É dado um exemplo hipotético em que a empresa tecnológica *Meta* não necessitaria de processar dados que mostrem que determinados indivíduos são homossexuais para discriminar com base na sexualidade. Se os seus algoritmos puderem prever que as pessoas que vão frequentemente a bares gay e gostam de ver o Queer Eye têm 25% menos probabilidades de serem candidatos desejáveis a uma certa oferta de emprego, isso seria suficiente para produzir discriminação em larga escala.

2. 4 Requisitos adicionais de transparência para as VLOPs e os VLOSEs (art. 39.º DSA)

Para além das normas de transparência referidas *supra*, o DSA apresenta, na secção 5, entre outras, regras adicionais no âmbito da publicidade em linha para os fornecedores de VLOPs e VLOSEs. Como já foi referido, dado o seu impacto e influência no mundo digital, é exigida aos VLOPSs e VLOSEs uma maior responsabilidade na sua actuação.

No art. 39.º do DSA é indicado que as VLOPs e os VLOSEs deverão disponibilizar, ao público, um repositório que contenha as informações sobre os anúncios apresentados. Os repositórios de anúncios têm como objectivo repor a transparência que se perde quando a publicidade é direccionada[65]. A publicidade direccionada nas plataformas só é visível para a pessoa que a recebe. Consequentemente, os próprios fornecedores de plataformas são (em princípio) os únicos intervenientes que têm uma visão global sobre quais os anúncios que são exibidos para cada tipo de público no seu serviço[66]. Nos repositórios de anúncios, as plataformas dão acesso a algumas informações sobre a forma como os anúncios são distribuídos e disponibilizados através de uma base de dados acessível ao público, facilitando assim a responsabilização das plataformas e dos anunciantes[67].

O n.º 2 do art. 39.º do DSA, elenca uma lista de informações que devem estar incluídas no repositório, como o conteúdo do anúncio, a pessoa (singular ou colectiva) em que cujo nome ou anúncio foi exibido e/ou que pagou o mesmo, o período de demonstração, entre outros. Ao mesmo tempo são impostas algumas limitações à informação contida nas bibliotecas de anúncios, como por exemplo, a não exposição de dados pessoais dos destinatários do anúncio nos respectivos repositórios (n.º 1 do art. 39.º DSA).

---

[65] Capello, "New Actors…" cit., p. 86.
[66] *Idem*.
[67] *Idem.*

Embora estes repositórios se revelem úteis para a consulta e controlo dos fornecedores dos VLOPs e VLOSEs, é certo que, a informação sobre transparência é frequentemente disponibilizada sob formas como interfaces gráficas, que dão a impressão de informar mas impedem a avaliação da informação em grande escala[68].

Como já referido, as VLOPs e os VLOSEs já têm de cumprir as obrigações do art. 39.º DSA, desde 25 de agosto de 2023[69/70].

2.5 Reacções das Instituições Europeias, da Autoridade Europeia para a Protecção de Dados e de outras entidades sobre as normas de transparência na publicidade

A proposta (e consequentemente a versão final) do DSA da Comissão Europeia levou a alguma discordância por parte do

---

[68] Ranganathan, "Regulating Influence, Timidly", cit., p. 203.

[69] De notar que, em julho de 2023, a *Amazon* interpôs uma acção judicial junto do TJUE, afirmando que a sua designação como VLOPs é baseada num critério discriminatório e que viola de maneira desproporcionada o princípio da igualdade de tratamento e os direitos fundamentais da recorrente. Nesta ação, foi pedido, a título subsidiário, a não aplicação da obrigação do art. 38.º DSA (de facultar aos utilizadores uma opção para cada sistema de recomendação que não se baseie na definição de perfis) e/ou a obrigação do art. 39.º DSA de compilar e disponibilizar ao público um repositório de anúncios publicitários. O TJUE decidiu suspender a decisão da Comissão na medida em que, por força dessa decisão, a *Amazon Store* seria obrigada a disponibilizar publicamente um repositório de anúncios, em conformidade com o art. 39.º do referido regulamento, sem prejuízo da exigência de o requerente compilar o repositório de anúncios. TJUE, T-367/23, Amazon Services Europe/Comissão, 5.07.2023. Por sua vez, no dia 27 de Março de 2024, o TJUE anulou a ordem de suspensão e indeferiu o pedido da *Amazon*, referindo que a não aplicação de certas obrigações previstas no DSA conduzirá ao adiamento, potencialmente por vários anos, da realização plena dos seus objectivos (nomeadamente contribuir para o bom funcionamento do mercado interno e assegurar um ambiente em linha seguro). TJUE, C-639/23 P(R), Comissão/Amazon Services Europe, 27.03.2024.

[70] Um repositório de anúncios que poderá ser apresentado, como exemplo, é a Biblioteca de Anúncios da *Meta* onde qualquer utilizador pode verificar os anúncios registados pelas suas plataformas a serem exibidos nas suas interfaces. De facto, na Biblioteca de anúncios da *Meta* poderá ser efectuada consultas multicritério e através de interfaces de programação de aplicações. Na pesquisa por multicritério, a procura poderá ser feita através de marcas e em que em cada anúncio poderá ser visto as características gerais do público do anúncio, escolhida pelo anunciante na UE, nomeadamente a localização, a idade, género, alcance. Para além disso é apresentada a identidade do anunciante e, se for o caso, da entidade que pagou o anúncio, entre outras informações.

Parlamento Europeu[71] e da AEPD[72]. Ambos sugeriram que a publicidade direccionada deveria ser regulamentada de forma mais rigorosa, a favor de formas de publicidade menos intrusivas e que não exigissem um acompanhamento exaustivo da interacção do utilizador com os conteúdos[73]. A Comissão Europeia não explica por que razão a transparência, por si só, seria a mais eficaz, sendo possível que tenha considerado que as questões relacionadas com os sistemas de publicidade em linha que recorrem à recolha intrusiva de dados pessoais, deveriam ser abordadas de forma mais adequada no âmbito do RGPD e do futuro Regulamento relativo à privacidade e às comunicações electrónicas[74]. Por outro lado, associações como a *Portugal Tech League*[75] defendem que uma das grandes vantagens da Internet tem sido tornar os benefícios da publicidade muito mais acessíveis às pequenas empresas, sendo esta, muitas vezes a única forma de as novas empresas e PMEs lançarem os seus produtos, serviços ou bens num segmento de mercado específico e chegar a novos potenciais consumidores de uma forma económica. Por conseguinte, uma proibição total da publicidade direccionada teria impedido as *startups* de competir com os concorrentes com maior presença no mercado[76].

---

[71] Resolução do Parlamento Europeu que contém Recomendações à Comissão sobre o Ato Legislativo sobre os Serviços Digitais que adapta a Regulamentação Comercial e o Direito Civil Aplicável às entidades que operem em linha, 2020/2019(INL)), 20.10.2020, parágrafo 15.

[72] AEPD, Opinion 1/2021 … cit., parágrafo 69.

[73] Tal escolha foi criticada por membros do Parlamento Europeu como Alexandra Geese que afirmou ser questionável se o problema básico é resolvido, isto é, o negócio enormemente lucrativo de exibição publicidade personalizada, que se baseia na espionagem de pessoas em todas as áreas da vida. Kayali, Laura; Larger, Thibault, "5 Challenges to the New EU Digital Rulebook", *POLITICO*, 2020. Disponível em https://www.politico.eu/article/5-challenges-to-the-new-eu-digital-rulebook/.

[74] Capello, "New Actors…" cit., p. 63.

[75] A *Portugal Tech League* é uma iniciativa que liga diversos intervenientes da economia digital portuguesa e da UE para informar e envolver a comunidade tecnológica com as políticas digitais europeias e reforçar a presença de start-ups nas discussões regulamentares. Disponível em https://portugaltechleague.eu/

[76] Portugal Tech League, Digital Services Act: A Script for Startups and SMEs to Grow in a Seamless, Open and Competitive Digital Single Market, p. 10. Disponível em https://portugaltechleague.eu/topics/the-digital-services-act

É de notar que os documentos do Conselho da União Europeia relativos às negociações do DSA revelam que a questão da introdução de restrições mais rigorosas à publicidade em linha tinha sido quase ignorada nas discussões[77]. A Alemanha foi o único Estado-Membro que levantou objecções sobre a pouca eficácia da obrigação de transparência proposta pela Comissão Europeia. Nos comentários ao art. 24.º da proposta da Comissão sobre o DSA, o Governo alemão observou que as regras da Comissão não iam suficientemente longe e que, em vez de publicidade personalizada, as plataformas poderiam gerar receitas com publicidade baseada no contexto ou com novas soluções tecnológicas, devendo os utilizadores ter o direito de utilizar plataformas em linha sem publicidade personalizada[78].

Neste ponto, é necessário ter em conta que, existem modelos de publicidade bastante intrusivos, como a publicidade comportamental, uma vez que podem fornecer aos responsáveis pelo tratamento uma imagem muito detalhada da vida pessoal dos indivíduos. A publicidade comportamental baseia-se em dados recolhidos através da observação da actividade dos utilizadores ao longo do tempo (por exemplo, a partir das páginas que visitam, do tempo que passam numa página que apresenta um determinado produto, dos gostos dados ou da sua localização) [79]. Estes dados poderão ser usados para efeitos de criação e desenvolvimento de perfis de utilizadores, para a apresentação de anúncios personalizados com base no perfil resultante e respectiva análise de interacção dos utilizadores com os anúncios apresentados[80]. Deste modo, considera-se que, tal como foi criada a norma do n.º 3 do art. 26.º do DSA (relativa à proibição de exibição de anúncios publicitários com base na definição de perfis

[77] Capello, "New Actors …"cit., p. 64.

[78] Conselho da UE, Digital Services Act: Consolidated Comments on Chapter 3 and Respective Recitals, WK 5155/2021 REV 2, 2021. Disponível em https://councildsa.reset.tech/documents/wk05155-re02/p. 276.

[79] CEPD, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, 2024, parágrafo 19-21. Disponível em https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf.

[80] *Idem*.

utilizando categorias especiais de dados pessoais) haveria oportunidade no DSA para proibir estes modelos mais intrusivos, ou pelo menos, regulamentá-los de forma mais exigente. Esta limitação não impediria a existência de outros modelos menos nocivos e igualmente úteis para as empresas. Para além disso, como será visto *infra*, a transparência só por si, não parece salvaguardar, de forma eficaz, os dados pessoais dos destinatários da publicidade em linha.

3. Principais desafios

i) Em relação às disposições sobre a publicidade no DSA

Embora no DSA se note a intenção de manter os destinatários dos serviços em linha informados e dar algum poder na decisão de como a publicidade poderá ser exibida, o Regulamento apresenta algumas fragilidades.

Em primeiro lugar, como foi visto, o DSA dá o poder ao destinatário individual para alterar os parâmetros utilizados que o seleccionam como destinatário de determinados anúncios publicitários. No entanto, esta opção poderá revelar-se ineficaz para a garantia liberdade de escolha dos destinatários. Ora, como foi referido, o fundamento de licitude do tratamento de dados pessoais para efeito de publicidade direccionada seria o consentimento, no entanto, constata-se que o mecanismo de notificação e consentimento poderá não funcionar. A maioria dos destinatários não lê as (longas) políticas de privacidade nem os seus termos e condições, ou porque não têm interesse nesta questão, ou a interface é confusa ou porque o utilizador precisa de acesso imediato aos serviços, pelo que acaba por aceitar tudo o que é apresentado[81]. Para além disso, um utilizador que esteja

[81] Galli, Federico; Lagioia, Francesca, e Sartor, Giovanni – "Consent to Targeted Advertising." *European Business Law Review,* volume XXXIII-4, 2022, p. 505. Disponível em https://cris.unibo.it/retrieve/e1dcb33a-0902-7715-e053-1705fe0a6cc9/Consent to Targeted Advertising.pdf

a navegar por várias páginas da Internet enfrenta vários *pop-ups* de consentimento e políticas de privacidade em cada sítio *web*, originando o chamado "cansaço do consentimento"[82].

Esta questão é suscitada com a Directiva relativa à Privacidade e às Comunicações Electrónicas[83] e com a utilização de testemunhos de conexão (*cookies*). A Directiva exige o consentimento dos utilizadores para os *cookies* e outros dispositivos de localização que interferem com o equipamento terminal dos utilizadores[84]/[85]. Neste âmbito, o GT29 aconselhou que, para que haja consentimento informado e válido, os fornecedores de redes de publicidade deviam criar mecanismos de aceitação prévia (isto é, o não consentimento como definição por defeito), ao invés dos mecanismos de auto-exclusão (tendo o utilizador de aceder às definições de plataformas em linha para indicar que não quer que as suas informações sejam recolhidas)[86]. Infelizmente, esta disposição não conseguiu limitar a recolha e a exploração de dados pessoais, uma vez que os utilizadores sobrecarregados com pedidos de consentimento e incapazes de avaliar as suas finalidades, não tendo as competências e o tempo necessários, e querendo aceder aos conteúdos da forma mais fácil e rápida possível, aceitam geralmente todos esses pedidos sem qualquer escrutínio[87].

O mesmo problema poderá ser transposto para o DSA, em que a falta de conhecimento dos utilizadores, as pressões indevidas por parte das plataformas em linha e os longos textos sobre a publicidade em linha invalidam as normas de transparência criadas.

Como referido, a forma como a informação é apresentada aos utilizadores pode afectar, muitas vezes, o consentimento. Neste contexto, o art. 25.º do DSA dá atenção a este problema ao proibir as

---

[82] *Idem*, p. 501.

[83] Directiva 2002/58/CE, de 12 de julho de 2002.

[84] N.º 3 do art. 5.º da Directiva relativa à privacidade e às comunicações electrónicas.

[85] Considerando 25 Directiva relativa à privacidade e às comunicações electrónicas.

[86] GT29, Parecer 2/2010 Sobre Publicidade Comportamental em Linha, 0909/10/PT [WP] 171, 2010, p. 26 e 27. Disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_pt.pdf

[87] Galli, Lagioia, Sartor, "Consent to …" cit., p. 501.

plataformas em linha de "conceber, organizar ou explorar as suas interfaces em linha de forma a enganar ou manipular os destinatários do seu serviço ou de forma a distorcer ou prejudicar substancialmente de outro modo a capacidade dos destinatários do seu serviço de tomarem decisões livres e informadas". Esta prática traduz-se nos chamados padrões obscuros, tendo estes várias formas, como definições prejudiciais para o destinatário predefinidas, a dificuldade crescente de selecção de opções que protegem a privacidade, colocação de cores mais vivas para opções de consentimento, etc.[88].

No entanto, tal como as normas sobre a publicidade no DSA, o art. 25.º aplica-se somente a plataformas em linha (como o *Facebook*, o *TikTok*, e o *YouTube*) e não a sítios *web* que incorporem, por exemplo, anúncios do *Google* (um motor de pesquisa)[89]. Acresce que, no n.º 2 deste artigo, esta proibição não se aplica a práticas abrangidas pelo RGPD e pela Directiva relativa às práticas comerciais desleais, o que irá excluir da sua aplicação os conhecidos *pop-ups* de consentimento para a recolha de dados pessoais[90]. Deste modo, o facto de esta proibição existir, demonstra um avanço no sentido de uma maior clareza para os utilizadores na entrada de uma plataforma em linha, no entanto o âmbito poderia ser mais abrangente.

Algumas sugestões poderão ser apresentadas de modo a auxiliar as plataformas em linha a respeitar as normas do DSA relativas à publicidade. Por exemplo, poderão ser criadas interfaces e

---

[88] De acordo com um estudo da Comissão Europeia, actualmente, cerca de 97% dos 75 sites e aplicações mais populares apresentam padrões obscuros. Comissão Europeia, Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation, DS-07-22-250-EN-N, 16.05.2022, p.45. Disponível em https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en; Sebastian; CASTELLARO, Sebastian e PENFRAT, Jan, "The DSA Fails to Reign in the Most Harmful Digital Platform Businesses – but It Is Still Useful", *Verfassung Blog*, 2022, parágrafo 15. Disponível em https://verfassungsblog.de/dsa-fails/; Galli, Lagioia, and Sartor, "Consent to …"cit., p. 502.

[89] O *Facebook* afirmou que a regulamentação sobre este tipo de *design* poderia afetar adversamente os seus resultados financeiros. Tanto a *Meta* quanto o *Google* juntaram-se a outras empresas de tecnologia para se opor firmemente a qualquer regulamentação sobre esta área no DSA. CASTELLARO, Sebastian e PENFRAT, Jan, "The DSA Fails…" cit., parágrafo 15 e 16.

[90] *Idem*, parágrafo 16.

predefinições favoráveis à protecção de dados, que incluem, pelo menos, a disponibilização de um botão com a opção "sem recolha de dados" de fácil acesso e que até pode ser concebido como opção pré-seleccionada[91]. Outra medida poderia ser o registo desta escolha (de não haver recolha de dados) na plataforma em linha para que os destinatários não tenham de repetir a sua selecção sempre que acedem ao mesmo sítio *web*[92], tendo em conta, no entanto que o destinatário teria de ser informado e consentir neste registo.

Em especial: O Modelo de publicidade "Consentimento ou Pagamento"

Neste ponto, destaca-se um exemplo que pode representar a insuficiência da exigência de transparência sobre publicidade nas plataformas em linha[93]. As redes sociais *Facebook* e *Instagram* oferecem a experiência "sem anúncios" em troca de 12,99 euros por mês[94], isto é, o acesso gratuito continua a ser possível, mas está condicionado ao tratamento dos dados pessoais do utilizador para fins de publicidade direccionada. Este modelo, designado por "Consentimento ou Pagamento"[95], tem vindo a ser utilizado por várias plataformas[96].

Esta exigência de pagamento em troca de um serviço sem publicidade direccionada condiciona o fundamento de licitude do consentimento, nos termos da alínea a) do n.º 1 do art. 6.º do RGPD, retirando o requisito da liberdade da manifestação de vontade do titular dos dados.

---

[91] Galli, Lagioia, and Sartor, "Consent to …" cit., p. 505.

[92] *Idem*.

[93] Embora a actuação da *Meta* que irá ser descrita, tenha sido resposta à exigência do TJUE (Processo C-252/21, Meta Platforms e o., 04.07.2023) no uso do consentimento como fundamento de licitude para o tratamento de dados pessoais para fins publicitários, e não para ultrapassar normas de transparência, este exemplo serve também para demonstrar as limitações destas normas perante determinadas actuações das plataformas em linha.

[94] Assim é o modelo oferecido pela *Meta*, na altura da elaboração deste artigo.

[95] Em inglês, *Consent or Pay.*

[96] Tech Policy Press, "Pay or Okay" – The Move to Paid Subscriptions on Social Networks, 2024. Disponível em https://www.techpolicy.press/pay-or-okay-the-move-to-paid-subscriptions-on-social-networks/

Em abril de 2024, a pedido da autoridade de controlo neerlandesa, da autoridade de controlo norueguesa e da autoridade de controlo alemã, o Comité Europeu para a Protecção de Dados (CEPD) adoptou um parecer sobre esta questão[97] (isto é, sobre o consentimento válido no contexto dos modelos "Consentimento ou Pagamento" implementados pelas grandes plataformas em linha)[98]. Em termos sucintos, o CEPD defende que, na maioria dos casos, as grandes plataformas em linha não poderão cumprir os requisitos de consentimento válido se confrontarem os utilizadores apenas com uma escolha binária entre o consentimento para o tratamento de dados pessoais para fins de publicidade comportamental e o pagamento de uma taxa[99]. É sugerido assim, pelo CEDP, que as grandes plataformas em linha, ao desenvolver a versão diferente da do serviço com publicidade comportamental, devem considerar a possibilidade de fornecer aos titulares dos dados uma "alternativa equivalente" que não implique o pagamento de uma taxa[100], por exemplo, uma versão do serviço que ofereça publicidade que envolva o tratamento de menos (ou nenhuns) dados pessoais, como publicidade contextual ou publicidade baseada em tópicos que o titular dos dados seleccionou de uma lista de tópicos de interesse[101]/[102]. No entanto, não deve ser ignorado

---

[97] De acordo com o n.º 2 do art. 64 do RGPD, as autoridades de controlo podem solicitar que o Comité analise qualquer assunto de aplicação geral ou que produza efeitos em mais do que um Estado-Membro.

[98] CEPD, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, 2024. Disponível em https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf

[99] CEPD, Opinion 08/2024…cit., parágrafo 179.

[100] *Idem*., parágrafo 74.

[101] *Idem*., parágrafo 75.

[102] Em paralelo, em julho de 2024, a Comissão Europeia informou a Meta sobre as suas conclusões preliminares, segundo as quais o seu modelo "Consentimento ou Pagamento" não cumpre o disposto no n.º 2 do art. 5.º do Regulamento dos Mercados Digitais. A justificação da Comissão baseia-se no facto de o modelo de publicidade não permitir que os utilizadores optem por um serviço equivalente ao serviço baseado em anúncios personalizados e que utilize menos dos seus dados pessoais e de não permitir que os utilizadores exerçam o seu direito de consentir livremente na combinação dos seus dados pessoais entre serviços essenciais de plataforma designados e outros serviços. Comissão Europeia, Comissão envia conclusões preliminares à Meta sobre o seu modelo «pagamento ou consentimento» por violação do Regulamento Mercados Digitais, 01.07.2024. Disponível em https://ec.europa.eu/commission/presscorner/detail/pt/IP_24_3582.

que o método mais simples e que, com mais facilidade, está em conformidade com o RGPD é o pedido de consentimento aos titulares relativamente à publicidade direccionada.

Assim, nota-se que, as normas de transparência exigidas pelo DSA (art. 26.º), com a utilização de modelos como "Consentimento ou Pagamento", tornam-se quase inúteis, pois, mesmo que os destinatários tenham conhecimento, não têm liberdade para definir os parâmetros da publicidade que recebem, de forma gratuita. Mesmo que o DSA tivesse entrado em vigor antes, as suas normas não impediriam a implementação deste modelo de publicidade. A transparência é importante, pois dá controlo aos utilizadores sobre os seus dados pessoais, no entanto, este tipo de modelos que subtraem o poder de escolha dos utilizadores esvaziam um pouco o objectivo da transparência. Para além disso, como foi referido *supra*, haveria espaço no DSA para limitar o uso, pelas plataformas em linha, de sistemas como a publicidade comportamental e, evitar, no futuro, a sujeição dos utilizadores a este tipo de estratégias e práticas de empresas que violam a protecção dos seus dados pessoais.

ii) Aplicação da legislação sobre a publicidade na UE

O ecossistema da publicidade em linha é complexo e o quadro jurídico que lhe é aplicável abrange vários domínios diferentes[103]. Na prática, isto significa que a regulamentação da publicidade em linha é da responsabilidade das várias autoridades de controlo competentes para aplicar a legislação relativa aos consumidores, à protecção de dados, à concorrência e à publicidade[104].

---

[103] Ver nota de rodapé n.º 26

[104] Reyna, Agustin, "Breaking Down Silos in Public Enforcement: Lessons from Consumer-Facing Markets", *BEUC (the European Consumer Organisation)*, 2021, p. 12. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3838697; Capello, "New Actors …" cit., p. 90.

Este cenário cria o risco de uma aplicação incoerente, que não salvaguarda adequadamente todos os diferentes valores em jogo ou que não é considerada prioritária por nenhuma das diferentes autoridades de controlo competentes[105]. Estas áreas do direito devem ser trabalhadas em conjunto pelas respectivas autoridades, tornando a sua intervenção mais direccionada e eficiente na resolução das falhas do mercado que restringem a escolha dos consumidores e prejudicam a capacidade dos consumidores de tomar decisões informadas[106]. As autoridades de controlo já estão a tentar prevenir estas lacunas, através da criação de redes de cooperação entre, por exemplo, as autoridades responsáveis pela protecção dos consumidores, dos meios de comunicação social e dos dados[107]. O DSA, no seu art. 49.º, já exige a criação de um coordenador de serviços digitais com a missão de facilitar a colaboração entre várias autoridades de controlo competentes. Esta cooperação será essencial para uma aplicação eficaz das normas referentes à publicidade em linha.

Conclusão

O objectivo deste artigo centrou-se na influência das novas disposições do DSA sobre a publicidade para os destinatários. É de notar que a publicidade em linha influencia a experiência de cada pessoa na navegação por uma determinada plataforma em linha, podendo tornar a mesma mais "agradável" e direccionada para o destinatário, utilizando, no entanto os dados pessoais e os comportamentos do mesmo. Os destinatários têm o direito serem informados sobre esta recolha de dados pessoais e como os mesmos são usados e são objecto de lucro para as mais variadas empresas.

---

[105] Capello, "New Actors…" cit., p. 90.
[106] Reyna, "Breaking Down …" cit., p. 12.
[107] Capello, "New Actors …" cit., p. 90.

No fundo, as disposições do DSA focam-se em normas de transparência sobre a exposição de publicidade nas interfaces em linha, numa maior responsabilidade por parte das VLOPs e VLOSEs e na limitação de publicidade direccionada que utiliza dados integrados nas categorias especiais de dados.

O DSA, embora com algumas limitações (por exemplo no que toca à falta de regulamentação mais rigorosa sobre a publicidade direccionada em linha, como defendido pelo Parlamento Europeu e pela AEPD), obriga as plataformas em linha a expor as suas políticas sobre a publicidade.

Para além disso, o DSA acendeu a discussão sobre os danos que poderão ser causados por modelos de publicidade baseados em recolha de dados, e que muitas das maiores empresas de tecnologia preferem manter escondidos da opinião pública.

Agora com a entrada em vigor deste novo regulamento levanta-se também a questão da aplicação das várias legislações relativas ao consumidor, protecção de dados, concorrência e publicidade, na qual será necessária a cooperação das várias autoridades de controlo competentes tanto dentro de cada Estado-Membro como entre Estados-Membros e, com a Comissão Europeia.

Synthetic data: a holy grail to healthcare research?

Marta Beleza Costa[1]
Miguel Goulão[2]

Abstract:
Healthcare research heavily relies on patient data, raising challenges due to stringent data protection legislation. Synthetic data is presented as a solution, offering privacy while facilitating research. This essay delves into the intersection of synthetic data and data protection law, analysing its regulatory implications, benefits, and disadvantages. Synthetic data shows value in various healthcare applications, from medical imaging to epidemiological studies. However, drawbacks like bias amplification and data quality assessment are still a concern. While synthetic data holds potential, regulatory frameworks need refinement to fully leverage its capability to be considered a "Holy Grail".

Keywords: Synthetic data; scientific research; healthcare; data protection law

Resumo:
A investigação cientifica no sector da saúde encontra-se fortemente dependente do tratamento dos dados de doentes. As exigências

[1] Graduated in Law from the Faculty of Law of the University of Lisbon and Master's student of Law and Tech at NOVA School of Law. Postgraduate in Digital Services Law from the Private Law Research Center of the Faculty of Law of the University of Lisbon. martabpcosta@gmail.com

[2] Data Privacy Consultant. Graduated in Law from the Faculty of Law of the University of Lisbon and Master's student of Law and Tech at NOVA School of Law. Postgraduate in Digital Services Law and in Data Protection Law, both from the Private Law Research Center of the Faculty of Law of the University of Lisbon. goulao.miguel@gmail.com

rigorosas em matéria de legislação de proteção de dados a que este tratamento está sujeito colocam vários desafios ao desenvolvimento das atividades de investigação. Assim, os dados sintéticos são apresentados como uma solução, assegurando a privacidade e, consequentemente, facilitando a investigação. Este artigo explora a relação entre os dados sintéticos e o direito da proteção de dados, analisando as implicações regulatórias, os seus benefícios e as suas desvantagens. Os dados sintéticos têm demonstrado utilidade no domínio dos cuidados de saúde, desde a imagiologia médica a estudos epidemiológicos, embora apresentando, igualmente, algumas desvantagens, como a amplificação de *bias* ou a fraca qualidade dos dados. Embora a utilização de dados sintéticos apresente potencial, é necessário introduzir reformas legislativas que possibilitem que as suas capacidades sejam plenamente aproveitadas e, consequentemente, que estes dados se tornem um verdadeiro *Holy Grail*.

Palavras-chave: Dados sintéticos; investigação científica; cuidados de saúde; direito da proteção de dados

I. Introduction

The processing of personal data for the purposes of healthcare scientific research has faced significant obstacles. Insofar as sharing knowledge and other information about health data (such as patient health records or diagnostics) is crucial for healthcare research, there is the necessity to overcome the limitations established in data protection legislation[3-4], in order to foster innovative and proper deployment of research[5]. This is especially relevant, since health data is regulated in a more stringent way by data protection legislation, having the need for assuring informed consent by the data subjects[6]. Also, given the fact that the processing of high quantities of special categories of data by new technologies is at stake, in a situation where it is possible to have indirect data collection of vulnerable data subjects, there might be the necessity to perform a Data Privacy Impact Assessment (DPIA)[7].

Nevertheless, even when complying with data protection legislation[8], researchers might face other regulatory restrictions, mostly related to ethical aspects for sharing and securing data (especially with regard to scientific research on humans). Other limitations include costly access

---

[3] It will be considered the General Data Protection Regulation par excellence: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

[4] KUO, Nicholas; PEREZ-CONCHA, Oscar; HANLY, Mark; MNATZAGANIAN, Emmanuel; HAO, Brandon; DI SIPIO, Marcus; YU, Guolin; VANJARA, Jash; VALERIE, Ivy; OLIVEIRA COSTA, Juliana; CHURCHES, Timothy; LUJIC, Sanja Lujic; HEGARTY, Jo; JORM, Louisa; BARBIERI, Sebastiano, "Enriching Data Science and Health Care Education: Application and Impact of Synthetic Data Sets Through the Health Gym Project", *JMIR Medical Education,* 10, 2024; available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10828942/

[5] GONZALES, Aldren; GURUSWAMY, Guruprabha; SMITH, Scott, "Synthetic data in health care: A narrative review", *PLOS Digit Health,* II, 1, 2023, available at: https://journals.plos.org/digitalhealth/article?id=10.1371/journal.pdig.0000082

[6] Note, for example, art. 13 and 14, GDPR.

[7] As set out in art. 35, GDPR.

[8] Note, for example art. 5(2), GDPR.

to datasets that are outside of the public domain[9] and data fragmentation that can result in gathering an incomprehensive dataset for exhaustive analysis, consequently, hindering researcher's capability to draw significant conclusions and data imbalance[10], and leading to misleading conclusions[11]. In addition, the lack of high-quality datasets has also been a significant barrier, especially to comprehend disease patterns, the identification of effective treatments and patient outcomes improvement[12].

The emergence of Artificial Intelligence (AI) – namely, Machine Learning (ML) models, such as Generative Adversarial Networks (GAN)[13] – has been proven to allow progress in the various medical fields, while maintaining efficient and dependable procedures when it comes to data access[14]. However, the biggest contribution that AI has brought for this purpose lies on the possibility of generating synthetic data – which has been presented as a game changer for solving the aforementioned limitations. In fact, data protection authorities, such as the Information Commissioner Office (ICO)[15] and the *Commission Nationale de l'Informatique et des Libertés* (CNIL)[16], have been

---

[9] GONZALES, Aldren; GURUSWAMY, Guruprabha; SMITH, Scott, "Synthetic data in health care: A narrative review", *PLOS Digit Health,* II, 1, 2023, available at: https://journals.plos.org/digitalhealth/article?id=10.1371/journal.pdig.0000082

[10] This occurs when there is misrepresentation of determined samples.

[11] ALI, Zahid, "The Dawn of a New Era: How Synthetic Data is Transforming Medical Research", 2023, available at: https://www.linkedin.com/pulse/dawn-new-era-how-synthetic-data-transforming-medical-research-ali-pmnjc/

[12] LAMBERTI, Aldo, "Lifting Data Barriers: Exploring Synthetic Data in Healthcare Research", 2023, available at: https://syntheticus.ai/blog/lifting-data-barriers-exploring-synthetic-data-in-healthcare-research

[13] "GANs work by employing two neural networks: one creates fake samples, and the other assesses how close they are to real data. These networks collaborate to refine the generated samples until they closely resemble real data", KAABACHI, Bayrem; DESPRAZ Jérémie, MEURERS Thierry; OTTE, Karen; HALILOVIC, Mehmed; PRASSER, Fabian; RAISARO, Jean Louis, "Can We Trust Synthetic Data in Medicine? A Scoping Review of Privacy and Utility Metrics", *MedRxiv,* 2023, available at: https://www.medrxiv.org/content/10.1101/2023.11.28.23299124v1.full

[14] *Ibidem*.

[15] MARSHALL, Valerie; MARKHAM, Charlie; AVRAMOVIC, Pavle; COMERFORD, Paul; MAPLE, Carsten; SZPRUCH, Lukasz, "Exploring Synthetic Data Validation – Privacy, Utility and Fidelity", *FCA Report*/*ICO Research Paper*, 2023, available at: https://www.fca.org.uk/publications/research-articles/exploring-synthetic-data-validation-privacy-utility-fidelity

[16] CNIL, "Artificial Intelligence: The CNIL Publishes a Set of Resources for Professionals", 2022, available at: https://www.cnil.fr/en/artificial-intelligence-cnil-publishes-set-resources-professionals

exploring their benefits as a privacy enhancing technology. In addition, the European Data Protection Supervisor (EDPS) led a Webinar focused on the use of synthetic data as a possible technology to mitigate data protection risks[17], where even synthetic data was presented as a "panacea" for the purposes of research[18].

Having said that, some underlying concepts will be provided, focusing on the notions of health data and scientific research. Then, the synthetic data conundrum in the light of the General Data Protection Regulation (GDPR) will be discussed, by exploring its definition and dogmatics. After discussing the regulatory state of the art in the EU, the benefits and disadvantages of the usage of synthetic data in healthcare research will be presented, while providing some potential solutions to the aforementioned challenges. Finally, one must be able to conclude if synthetic data should be considered a "Holy Grail" to healthcare research.

II. Data in the Healthcare Domain

i. Data Concerning Health

Data concerning health, notwithstanding its definition in art. 4(15), GDPR[19], must be interpreted in a broad sense, accordingly to the CJEU's understanding[20]: "the expression data concerning health

[17] IPEN; Webinar on the theme: "Synthetic data: what use cases as a privacy enhancing technology?", 2021; available at: https://www.edps.europa.eu/data-protection/our-work/ipen/ipen-webinar-2021-synthetic-data-what-use-cases-privacy-enhancing_en

[18] IPEN; "Synthetic data: what use cases as a privacy enhancing technology?" – Webinar; 2021; available at: https://www.edps.europa.eu/data-protection/our-work/ipen/ipen--webinar-2021-synthetic-data-what-use-cases-privacy-enhancing_en (remarks made by Wojciech Wiewiórowski).

[19] Art. 4(15) states: "Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".

[20] CJEU, C-101/01 Lindqvist, Bodil Lindqvist v Åklagarkammaren i Jönköping, 6/11/2003 para 50, 51

(…) must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual". Recital 35 provides some examples, such as information derived from the testing or examination of a body part or bodily substance, and information, amongst others, on a disease or medical history.

This type of data is considered sensitive data under art. 9(1), which leads to the prohibition of its processing, unless an exception provided for in paragraph 2 is applicable. Art. 9(2)(j) makes it possible to process sensitive data for scientific research purposes, in compliance with the provisions of art. 89(1) and provided that the following requirements, regarding the processing, are met: i) based on Union or Member State law; ii) proportionate to the aim pursued (the purpose of the data processing); iii) respect the essence of the right to data protection (the right to informational self-determination)[21]; iv) provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject[22]; v) that technical and organizational measures are ensured, mostly in order to comply with the data minimization principle.

ii. The Scientific Research Conundrum

a. Scientific Research in the GDPR

The concept of "scientific research" is not explicitly defined in the GDPR, although it is mentioned in several provisions[23]. However,

[21] BARRETO MENEZES CORDEIRO, António, *Direito da Proteção de Dados – À luz do RGPD e da Lei n.º 58/2019*, Almedina, 2020.

[22] Criticisms to art. 89(1) have been pointed out due to the generality and restricted scope of the safeguards stated. Regarding these considerations, PORMEISTER, Kärt, "Genetic Data and the Research Exemption. Is the GDPR Going too Far?", International Data Privacy Law, VII, 2, 2017, available at https://academic.oup.com/idpl/article-abstract/7/2/137/3798545?redirectedFrom=fulltext

[23] This is the case of art. 5(1)(b) and (e), art. 9(2)(j), art. 17(3)(d), art. 21(6) and art. 89.

recital 159[24] determines its concept in a broad sense, stating that "the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research". Recital 157 offers numerous instances of the kinds of scientific research that can be conducted. These include registry-based research, medical research into cardiovascular disease, cancer, and depression[25].

The UK data protection authority has established certain criteria in order to better understand this concept, making the following classification[26-27]: i) activities: scientific research incorporates, among others, the formulation of hypotheses, the isolation of variables and the design of experiments, the observation and measurement of data, the publication of findings, data integration and analysis, and inferential statistics; ii) standards: these include technical guidelines and approval by a committee and specific rules (e.g. animal or human research, clinical trials); iii) access: it includes the publication of results or commitment to share research findings, access to which does not have to be open (it can be in a scientific journal or other type of paid publication).

---

[24] Recital 159 states: "Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures."

[25] WIESE SVANBERG, Christian, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford Academic, 2020

[26] ICO, "GDPR Guidance and Resources, The Research Provisions", 2023, available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/the-research-provisions/

[27] CANTO MONIZ Graça, Lesson taught as part of "IV Pós Graduação Avançada em Direito da Proteção de Dados Pessoais", subordinated to the theme "O Tratamento de Dados Pessoais para Fins de Investigação Científica", 2022

The most common legal basis used for scientific research purposes are the consent of the data subject[28], as well as the legitimate and public interest. Regarding consent, recital 33 states that the requirement for specificity is somewhat mitigated. This is because in certain scientific research projects it is not always possible, at the time consent is collected, to identify the full purpose of the processing (since research projects change from time to time)[29-30]. However, the EDPB has already indicated that, when processing special categories of data, the approach provided for in recital 33 needs to "be subject to a stricter interpretation and requires a high degree of scrutiny", especially because of the limitations provided for in art. 9[31].

Processing of data for scientific research purposes needs to fulfil the requirements set out in art. 89(1). In this sense, the data processing needs to comply with appropriate safeguards for the rights and freedoms of the data subject, which need to ensure the implementation of technical and organisational measures to respect the principle of data minimisation[32]. Note that art. 89 must also be read alongside art. 9(4): insofar as art. 9(4) allows Member States do introduce national

---

[28] Consent is the most commonly used legal basis, since there is a set of ethical rules that are embodied in the Declaration of Helsinki, which state that consent to participate in scientific studies is an ethical requirement. With regard to these considerations, CANTO MONIZ Graça, Lesson taught as part of "IV Pós Graduação Avançada em Direito da Proteção de Dados Pessoais", subordinated to the theme "O Tratamento de Dados Pessoais para Fins de Investigação Científica", 2022

[29] CANTO MONIZ Graça, Lesson taught as part of "IV Pós Graduação Avançada em Direito da Proteção de Dados Pessoais", subordinated to the theme "O Tratamento de Dados Pessoais para Fins de Investigação Científica", 2022

[30] This would be the case, for example, for some research projects that involve "data-intensive longitudinal population-based research": since there is a high volume and variety of data being processed, starting of with a very detailed consent form might not be the most appropriate approach. Regarding these considerations, HO, Chih-hsing, "Challenges of the EU General Data Protection Regulation for Biobanking and Scientific Research", *Journal of Law, Information and Science*, XXV, 1, 2018, available at: https://www6.austlii.edu.au/cgi-bin/viewdoc/au/journals/JlLawInfoSci/2017/5.html

[31] EDPB, "EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research", 2021

[32] Note that, when the article mentions "public interest", this expression should only be considered when processing data for archiving purposes, which means that the provisions of art. 89 apply to public or private entities when data is processed for scientific research purposes.

legislation stating further conditions for the processing of certain types of sensitive data[33], the "safeguards" mentioned in art. 89 could be considered as such conditions[34].

Moreover, when the legislator assumes that data is processed for scientific research purposes, there is already a set of good practices, methodologies and processes that are sufficiently recognized, accepted and established in rules of ethical and professional nature, especially with regard to scientific research on humans[35]. Because of this, GDPR provides for several exceptions[36], such as the conditions of lawfulness[37], the principle of purpose limitation[38] and retention[39], as well as on the rights of data subjects[40].

Certain conditions apply to the exceptions on the rights of data subjects: i) even when said exceptions apply, the requirements of art. 89(1) still need to be verified; ii) in order to apply these derogations, exercise of these rights must be "likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes"[41]; iii) the derogations only apply to the purposes mentioned in art. 89(2) and 89(3). This means that, for example, derogations for the following use of health research data[42] for commercial purposes are not applied. Note that differentiation can be difficult between the original

[33] In particular, genetic data, biometric data or data concerning health.

[34] EDPB, "Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research", 2019

[35] For example, the Geneva Declaration of the World Medical Association states that "I will respect the secrets that are confided in me, even after the patient has died."; the International Code of Medical Ethics states that "The physician must respect the patient's privacy and confidentiality, even after the patient has died."

[36] CANTO MONIZ Graça, Lesson taught as part of "IV Pós Graduação Avançada em Direito da Proteção de Dados Pessoais", subordinated to the theme "O Tratamento de Dados Pessoais para Fins de Investigação Científica", 2022

[37] Art. 6(1) and 9.

[38] Art. 5(1)(b).

[39] Art. 5(1)(e).

[40] Art. 15, 16, 18 and 21, ex vi art. 89(2), as well as art. 14(5)(b)

[41] Arts. 89(2) and 89(3).

[42] Thus, collected for the purposes of scientific research.

scientific research purpose and subsequent purposes for the same data processing[43].

However, it must be highlighted that ethics committees play an important role in guaranteeing that the fundamental right to data protection (as well as other human rights) is integrated in scientific research, ensuring that research projects are already designed from the very beginning with data protection principles in mind. Ethical committees should, then, help in the understanding of which activities qualify as "scientific research", as well as defining the ethical standards mentioned in the GDPR[44].

b. Limitations regarding Data Processing for Scientific Research Purposes

The introduction of the GDPR was expected to harmonize the legal framework for data protection in the EU. However, this desired result has not been fully achieved, which is especially visible in the implementation of the "safeguards" provided for in art. 89(1). This is not only due to the fact that the definition of important concepts is reserved for the recitals[45], but there is also a favourable discussion on Member States being obliged to develop specific legislation regarding the aforementioned "safeguards"[46-47]. This circumstance can promote "different interpretations and forum shopping, which may erode the individuals' privacy, since the Member States do not want to fall back in the field scientific research and losing income"[48].

---

[43] WIESE SVANBERG, *Christian, The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford Academic, 2020

[44] EDPS, "A Preliminary Opinion on data protection and scientific research", 2020

[45] Note the fact that just for art. 89 there are several recitals that correspond to it, in particular, recitals 156 to 163.

[46] Others defend that art. 89 only imposes obligations for the researchers as controllers to implement safeguards. Thus, it would be enough that controllers establish the safeguards, which can include implementing guidelines or codes of conduct.

[47] EDPB, "Study on the appropriate safeguards under art. 89(1) GDPR for the processing of personal data for scientific research", 2019

[48] MESZAROS, Janos, "The Conflict Between Privacy and Scientific Research in the GDPR", *2018 Pacific Neighborhood Consortium Annual Conference and Joint Meetings (PNC)*, 2018, available at: https://ieeexplore.ieee.org/document/8579471

The GDPR also presents limitations regarding the processing of health data for the purposes of scientific research, including the necessity to specify several conditions for the publication or disclosure of said data. Also, the GDPR lies on the need to specify the nature and scope of the research, due to the fact that the data processing requires specified, explicit and legitimate purposes[49]. On one hand, this restricts the ability to repurpose personal data collected for a specific project for other uses[50]. On the other hand, it can be an obstacle to the development of the project being carried out, for example, in the cases where the dataset is used to formulate the scope of the actual research. Thus, this requires researchers to already have, from the beginning, a proper understanding and establishment of the research project's nature and purposes[51].

iii. Is Synthetic Data Relevant to all types of Scientific Research?

The use of synthetic data may be more relevant in certain types of scientific research. A study concluded that when many patients are used in comparison to the number of variables, there is higher accuracy and consistency of results between synthetic and the original data, while in respect of research that uses smaller populations, predictions were of moderate accuracy, yet clear trends were correctly observed[52]. For example, some scientific research situations in which synthetic data is mostly applied include simulation studies and predictive analytics,

---

[49] Art. 5(1)(b)

[50] WOLK DER VAN, Alex, "The (Im)Possibilities of Scientific Research Under the GDPR", *Cybersecurity Law Report*, 2017, available at: https://www.mofo.com/resources/insights/200617-scientific-research-gdpr

[51] *Ibidem.*

[52] REINER BENAIM, Anat; ALMOG, Ronit; GORELIK, Yuri; HOCKBERG, Irit; NASSAR, Laila; MASHIACH, Tanya; KHAMAISI, Mogher; LURIE, Yael; AZZAM, Zaher; KHOURY, Johad; KURNIK, Daniel; BEYAR, Rafael, "Analyzing Medical Research Results Based on Synthetic Data and Their Relation to Real Data Results: Systematic Comparison From Five Observational Studies", *JMIR Med Inform,* VIII, 2, 2020, available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7059086/

algorithms, hypothesis, and methods testing and epidemiological study/ public health research.

When it comes to simulation and prediction research, there is the necessity to use large datasets from real world sources, in order to properly anticipate certain behaviors and outcomes. Considering this, synthetic data emerge as a replacement or a supplement to real world sources, given the fact that researchers are allowed to scale the sample size or even to add variables not considered in the original data set[53]. Regarding epidemiological studies and public health research, datasets present limitations in terms of size and quality, as well as being expensive. This was especially evident in the Covid-19 pandemic, when the need of making data publicly available was felt[54]. To face these difficulties, synthetic data allows the improvement of the "timeliness of data release, support[s] researchers in doing real-time computational epidemiology, provide[s] a more convenient sample for sensitivity analyses, and build[s] a more extensive test set for improving disease detection algorithms"[55]. Finally, it has been proven that synthetic data shows higher potential for prediction, enhancing diagnostics, and comprehending risk factors.

---

[53] Note its usage, amongst others, in "disease-specific hybrid simulation and microsimulation for testing policy options and health care financing strategies evaluation. Studies also used synthetic data to validate simulation and prediction models and to improve prediction accuracy", REINER BENAIM, Anat; ALMOG, Ronit; GORELIK, Yuri; HOCHBERG, Irit; NASSAR, Laila; MASHIACH, Tanya; KHHAMAISI, Mogher; LURIE, Yael; AZZAM, Zaher: KHOURY, Johad; KURNIK, Daniel; BEYAR, Rafael, "Analyzing Medical Research Results Based on Synthetic Data and Their Relation to Real Data Results: Systematic Comparison From Five Observational Studies", *JMIR Med Inform*, VIII, 2, 2020, available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7059086/

[54] "Use of synthetic data in the area of clinical research is limited at the moment. However, users need to understand the source and the way the synthetic dataset was generated to evaluate its appropriateness for specific types of studies or specific stages of research", GONZALES, Aldren; GURUSWAMY, Guruprabha; SMITH, Scott, "Synthetic data in health care: A narrative review", *PLOS Digit Health,* II, 1, 2023, available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9931305/

[55] *Ibidem*.

III. Synthetic Data in the Light of the GDPR

i. What is Synthetic Data?

The definition of synthetic data has been the subject of some controversy in the literature[56-57]. Scholars usually make the distinction between real and not real data, insofar as synthetic data consists mostly of not real data (that are artificially manufactured with or without the original real data)[58]. However, this approach has been somewhat – and rightfully so – criticized by the EDPS[59]: if it is considered that the "real" data is "truthful" data, it's not correct to assume that synthetic data is "not real" only because the data is artificially generated. As it will be analysed[60], not only can synthetic data be categorized based on the amount of interference the original data has in the dataset, but even data that has been entirely generated by artificial intelligence can be considered partly "real", insofar as it may be possible to re-identify the data subject. Other scholars argue that "synthetic data" only refers to

---

[56] Consider, for example, the definition given by the US Census Bureau (taken from a ONS UK Working Paper): "Microdata records created by statistically modeling original data and then using those models to generate new data values that reproduce the original data's statistical properties. This definition highlights the strategic use of synthetic data because it improves data utility while preserving the privacy and confidentiality of information". Regarding this definition, UK's Office for National Statistics, "ONS methodology working paper series number 16 – Synthetic data pilot", 2021, available at: https://www.ons.gov.uk/methodology/methodologicalpublications/generalmethodology/onsworkingpaperseries/onsmethodologyworkingpaperseriesnumber16syntheticdatapilot;

[57] GONZALES, Aldren; GURUSWAMY, Guruprabha; SMITH, Scott, "Synthetic data in health care: A narrative review", *PLOS Digit Health,* 2023, available at: https://journals.plos.org/digitalhealth/article?id=10.1371/journal.pdig.0000082

[58] *Ibidem*.

[59] IPEN; "Synthetic data: what use cases as a privacy enhancing technology?" – Webinar; 2021; available at: https://www.edps.europa.eu/data-protection/our-work/ipen/ipen-webinar--2021-synthetic-data-what-use-cases-privacy-enhancing_en (remarks made by Wojciech Wiewiórowski).

[60] Section III, Item ii.

datasets incorporating merely fabricated data and without any original record[61].

Nonetheless, the classification of synthetic data has not been considered rigid[62]. Statistics field scholars divide synthetic data in fully synthetic, partially synthetic, and hybrid. A more detailed spectrum of synthetic data types is described in a working paper series by the United Kingdom's Office for National Statistics (UK's ONS). The spectrum features six levels under the synthetic and synthetically augmented dataset types[63].

That said, fully synthetic data are identified as a dataset that is completely synthetic and has a strong privacy control – given the fact that there is no correlation with the dataset generated, although having low analytic value[64]. Regarding partially synthetic data, a selection of the original dataset is replaced by synthetic data. Despite having a lower privacy control – since the dataset still contains original data –, this type of data has a higher analytic value[65]. At last, hybrid synthetic data is the result of both original and synthetic data. Despite its generation being more time and memory consuming, this type of data maintains privacy control characteristics with high effectiveness[66].

---

[61] UK's Office for National Statistics, "ONS methodology working paper series number 16 – Synthetic data pilot", 2021, available at: https://www.ons.gov.uk/methodology/methodologicalpublications/generalmethodology/onsworkingpaperseries/onsmethodologyworkingpaperseriesnumber16syntheticdatapilot; SIWICKI, Billy, "Is synthetic data the key to healthcare clinical and business intelligence?", *Healthcare IT News*, 2020, available at: https://www.healthcareitnews.com/news/synthetic-data-key-healthcare-clinical-and-business-intelligence.

[62] GIUFFRÈ, Mauro; SHUNG, Dennis, "Harnessing the Power of Synthetic Data in Healthcare: Innovation, Application, and Privacy", *npj Digital Medicine*, VI, 2023, available at: https://www.nature.com/articles/s41746-023-00927-3#citeas

[63] UK's Office for National Statistics, "ONS methodology working paper series number 16 – Synthetic data pilot", 2021, available at: https://www.ons.gov.uk/methodology/methodologicalpublications/generalmethodology/onsworkingpaperseries/onsmethodologyworkingpaperseriesnumber16syntheticdatapilot;

[64] GONZALES, Aldren; GURUSWAMY, Guruprabha; SMITH, Scott, "Synthetic data in health care: A narrative review", *PLOS Digit Health,* 2023, available at: https://journals.plos.org/digitalhealth/article?id=10.1371/journal.pdig.0000082

[65] *Ibidem*.

[66] *Ibidem*.

ii. The dogmatics of synthetic data in the light of the GDPR; (non) personal data?

Synthetic data corresponds to artificial, algorithmically generated data that, by closely mimicking the properties and relations of the source data, can be used for the same purposes[67].

The applicability of the processing of synthetic data to the GDPR depends on its dogmatic insertion in the category of "personal data", which means knowing to what extent synthetic data constitutes "information relating to an identified or identifiable natural person"[68].

Although the artificial nature of synthetic data shows that it cannot be considered data that directly identifies a natural person, it can still be information relating to an identifiable person, which makes its classification subject to the "reasonability criteria", as provided for in recital 26. If considering "all the means likely reasonably to be used", the possibility of identifying a natural person does not exist or is negligible, the information will not be considered "personal data"[69]. Having said that, one must examine the possibility of establishing a correlation between the synthetic data and the original data and, consequently, (re) identifying the data subject[70].

Despite a case-by-case basis being the key to assess whether a set of synthetic data is personal data, it is necessary to establish various factors to determine the applicability of the "reasonableness criteria", being one of them the purpose for which synthetic data is generated. Note that synthetic data is usually viewed as a form of anonymization or as a privacy-enhancing technology[10], which means that re-identification will be more difficult. It can't be said the same when synthesizing is

---

[67] MITCHELL, Colin; REDRUP HILL, Elizabeth, "Are Synthetic Health Data "Personal Data"?", *PHG Foundation Report*, 2023

[68] Art. 4(1)

[69] BARRETO MENEZES CORDEIRO, António, *Direito da Proteção de Dados – À luz do RGPD e da Lei n.º 58/2019*, Almedina, 2020

[70] MITCHELL, Colin; REDRUP HILL, Elizabeth, "Are Synthetic Health Data "Personal Data"?", *PHG Foundation Report*, 2023, available at: https://www.phgfoundation.org/publications/reports/are-synthetic-health-data-personal-data/

intended for filling gaps in essential information required to test products or software[11] but also to uncover biases in real-world data[12].

Another factor is related to the type of original data used. For example, a process that relies on statistical data to feed the algorithm has lower chances of re-identification[13], in comparison with a process that uses large sums of directly identifiable personal data.

Moreover, the higher the utility of a synthetic data set, the lower its anonymity, which means that the type of synthesizing process is also relevant to determine re-identification risks. An approach that resorts to advanced machine learning techniques has a better chance of establishing relationships between the original data and the synthetic data[14], in contrast to one that starts with source data manually manipulated[15].

We also understand that the classification of synthetic data as personal data also requires an examination of the pertinent legal definitions, especially concerning the understanding of identifiability and anonymization within the realm of data protection law[16]. In this sense, "the bar of anonymization has been set very high by the European legislator"[17], which means that "synthetic data [is] capable of being considered personal, 'pseudonymous' or anonymous depending on interpretation and context[18]."

IV. Regulatory State of the Art in the EU

The last few years have demonstrated an absence of an overall "EU data architecture, harmonization, and collaboration in data-sharing practices across countries, hindering the ability to support regulatory decision making based on RWE [Real World Evidence], and efficiently address public health challenges".[71] In order to circumvent these issues,

[71] Clara ALLOZA, Bethany KNOX, Hanaya RAAD, Mireia AGUILÀ, Ciara COAKLEY, Zuzana MOHROVA, Élodie BOIN, Marc BÉNARD, Jessica DAVIES, Emmanuelle JACQUOT, Coralie LECOMTE, Alban FABRE, Michael BATECH; "A Case for Synthetic Data in Regulatory Decision-Making in Europe", *PubMed*, CXIV, 4, 2023, 795-801; available at: https://pubmed.ncbi.nlm.nih.gov/37441734/

the establishment of the European Health Data Agency (EHDA)[72] was proposed.

Even though synthetic data have not yet been considered in any regulatory process, there have been some initiatives by the EU to implement the use of this type of data for healthcare research purposes. Some initiatives include the European Medicines Agency's joint statement calling for international collaboration to enable RWE for regulatory decision-making[73]. This collaboration would mainly be carried out by the International Coalition of Medicines Regulatory Authorities.

However, two pieces of legislation are particularly important: the Data Governance Act and the European Health Data Space Act. The latter, by determining and developing health data processing across Europe, provides a framework toward a more comprehensive (Health) Data Governance Act[74], where synthetic data are pointed to have a crucial role and seen as a solution for some of the public health sector needs. Other important initiatives include a Webinar focused on the use of synthetic data as a possible technology to mitigate data protection risk led by the EDPS[75], the Horizon Europe project[76], the Data Analysis

[72] Proposed by the Panel for the Future of Science and Technology, available at: https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2021)690009

[73] This decision is available at: https://www.ema.europa.eu/en/news/global-regulators-call-international-collaboration-integrate-real-world-evidence-regulatorydecision;

[74] Clara ALLOZA, Bethany KNOX, Hanaya RAAD, Mireia AGUILÀ, Ciara COAKLEY, Zuzana MOHROVA, Élodie BOIN, Marc BÉNARD, Jessica DAVIES, Emmanuelle JACQUOT, Coralie LECOMTE, Alban FABRE, Michael BATECH; "A Case for Synthetic Data in Regulatory Decision-Making in Europe", *PubMed*, CXIV, 4, 2023, 795-801; available at: https://pubmed.ncbi.nlm.nih.gov/37441734/

[75] IPEN; "Synthetic data: what use cases as a privacy enhancing technology?" – Webinar; 2021; available at: https://www.edps.europa.eu/data-protection/our-work/ipen/ipen-webinar-2021-synthetic-data-what-use-cases-privacy-enhancing_en

[76] This project provides new methods for the effective use of real-world data and/or synthetic data in regulatory decision-making and/or in health technology assessment. It is available at: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-hlth-2022-tool-11-02

and the Real-World Interrogation Network[77]. Moreover, data protection authorities, such as ICO[78] and CNIL, have been exploring their benefits as a privacy enhancing technology[79]. All these initiatives are particularly relevant to leverage the rapid collaboration that is taking place between government institutions, the academia, and the private sector[80].

V. Benefits of the use of Synthetic Data; Applying Synthetic Data in Healthcare Research

Synthetic data has brought a turning point to the field of scientific research in the area of healthcare, as it introduces a number of innovative applications.

Some applications include the use of synthetic data in medical imaging analysis, simulation of clinical trials regarding drug discovery and development, tailoring treatment plans for personalized medicine, improving readiness and reactive measures for public health analysis and prediction, as well as in supporting clinical decisions[81]. Synthetic data can also give rise to outputs that include images, audio files, and

---

[77] It provides real-world evidence from across Europe on diseases, populations and the uses and performance of medicines, which allows EMA and national competent authorities in the European medicines regulatory network to use these data whenever needed throughout the lifecycle of a medicinal product. It is available at: https://www.darwin-eu.org/

[78] MARSHALL, Valerie; MARKHAM, Charlie; AVRAMOVIC, Pavle; COMERFORD, Paul; MAPLE, Carsten; SZPRUCH, Lukasz, "Exploring Synthetic Data Validation – Privacy, Utility and Fidelity", *FCA Report/ICO Research Paper*, 2023, available at: https://www.fca.org.uk/publications/research-articles/exploring-synthetic-data-validation-privacy-utility-fidelity;

[79] CNIL, "Artificial Intelligence: The CNIL Publishes a Set of Resources for Professionals", 2022, available at: https://www.cnil.fr/en/artificial-intelligence-cnil-publishes-set-resources-professionals

[80] ALLOZA, Clara; KNOX, Bethany; RAAD, Hanaya; AGUILÀ, Mireia; COAKLEY, Ciara; MOHROVA, Zuzana; BOIN, Élodie; BÉNARD, Marc; DAVIES, Jessica; JACQUOT, Emmanuelle; LECOMTE, Coralie; FABRE, Alban; BATECH, Michael; "A Case for Synthetic Data in Regulatory Decision-Making in Europe", *PubMed*, CXIV, 4, 2023, 795-801; available at: https://pubmed.ncbi.nlm.nih.gov/37441734/

[81] MEHTA, Yash; "Resolving Healthcare's Prime Challenges through Synthetic Data Generation"; available at: https://datafloq.com/read/healthcare-challenges-synthetic-data-generation/

videos[82], enabling the generation of CT-like images, as well as it allows to overcome errors, inaccuracies, and bias of real-world data, by ensuring higher data quality and variety[83]. That being said, the increasing interest in utilizing synthetic data for medical purposes has prompted the development of various tools (such as Synthea[84] or MDClone's Synthetic Data Engine).

However, the main valuable aspect for the processing of synthetic data is in the fact that it "enables organizations to access concrete and representative insights from sensitive data, while minimizing the risk to patient privacy and limiting governance requirements.[85]". When it comes to patient privacy, the synthesizing process is usually employed as a privacy enhancing technique, which means that the risk of identifying the data subject is reduced – especially given that anonymous data can be generated.

Considering this, the implementation of these synthesis processes is considered to be a technical measure aimed at achieving compliance with the principle of minimisation and, consequently, being a prime example of an "appropriate safeguard", under the terms of art. 89(1). Nevertheless, it is important to take into account, according to recital 156, that these data minimization techniques must be "in pursuance of the proportionality and necessity principles". This means that, on a case-by-case basis, it is necessary to weigh up the advantages that data synthesis brings by minimizing the risk of

---

[82] GAL, Michal; "Synthetic Data: Legal Implications of the Data-Generation Revolution", *SSRN Electronic Journal*, 2023; available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4414385#

[83] LAMBERTI, Aldo, "The Benefits and Limitations of Generating Synthetic Data", 2023; available at: https://syntheticus.ai/blog/the-benefits-and-limitations-of-generating-synthetic-data

[84] WALONOSKI, Jason; KRAMER, Mark; NICHOLS, Joseph; QUINA, Andre; MOESEL, Chris; HALL, Dylan; DUFFETT, Carlton; DUBE, Kudakwashe; GALLAGHER, Thomas; MCLACHLAN, Scott; "Synthea: An approach, method, and software mechanism for generating synthetic patients and the synthetic electronic health care record"; *Journal of the American Medical Informatics Association*, XXV, 3, 2018, 230-238; available at: https://pubmed.ncbi.nlm.nih.gov/29025144/

[85] LESHIN, Jonah; JOHNS, Quinn; "The Value of Synthetic Data in Healthcare"; Available at: https://www.datavant.com/blog/synthetic-data-healthcare

identifying the data subject against other disadvantages that may arise from its application[86].

For these reasons one must consider that, within the context of a "data protection by design and by default" approach[87], the protection of the rights of data subjects is more effective. For example, research done on the usage of partially synthetic data as a proxy for original data in large-scale health surveys has shown to be successful, proving that the data, while guaranteeing patient privacy, still allowed researchers to perform analysis[88]. Moreover, facing the obstacle of limited reproducibility for clinical research findings caused by data protection legislations, synthetic data allows continuous research conduction, since the sharing of synthetic patient datasets means that clinical researchers can ensure that their results and case studies are replicable[89-90].

It could also be said that the fact that synthetic data often involves the processing of a large volume and variety of personal data makes it difficult to fulfil the various requirements for consent, particularly the fact that said consent must be "informed". However, art. 14(5)(b) already mentions a derogation from the various information duties, if "the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for (...) scientific research purposes". This derogation is "subject to the conditions and safeguards referred to in Article 89(1)" or if the information requirements are likely to render impossible or seriously impair the achievement

---

[86] Without prejudice to the disadvantages mentioned in the next section, it is necessary to consider (again, taking into account the individual circumstances of the case) any other risks that may exist for data subjects.

[87] Art. 25

[88] LOONG, Bronwyn; ZASLAVSKY; Alan M; HE, Yulei; P HARRINGTON David; "Disclosure control using partially synthetic data for large-scale health surveys, with applications to CanCORS", *Statistics in Medicine Journal*, XXXII, 24, 2013, 39-61; available at: https://pubmed.ncbi.nlm.nih.gov/23670983/

[89] DILMEGANI, Cem; "Synthetic Data for Healthcare: Benefits & Case Studies in 2024"; Available at: https://research.aimultiple.com/synthetic-data-healthcare/

[90] KAABACHI, Bayrem; DESPRAZ, Jérémie; MEURERS, Thierry; OTTE, Karen; HALILOVIC, Mehmed, PRASSER, Fabian; RAISARO Jean Louis; "Can We Trust Synthetic Data in Medicine? A Scoping Review of Privacy and Utility Metrics"; *MedRxiv*, 2023.

of the objectives of that processing. Thus, the application of this article is particularly relevant when synthetic data is processed for scientific research purposes, especially since the dataset is almost never obtained directly from the data subject.

When determining what constitutes a disproportionate effort, recital 62 refers to "the number of data subjects, the age of the data and any appropriate safeguards adopted". In other words, despite the fact that, as mentioned above, data synthesis techniques are considered an appropriate safeguard that largely reduces the risk of identifying the data subject, it is nonetheless necessary that the controller carries out a "balancing exercise to assess the effort involved to provide the information to data subjects against the impact and effects on the data subject if they are not provided with the information"[91].

Regarding governance requirements, synthetic data contributes to the data sharing between researchers and organizations, not only because it bypasses some of the current restrictions on data transfers, but also because it circumvents some of the ethical standards. For example, if a company situated in a country outside the European Economic Area (EEA) wants to access EU health data, in order to develop activities in the EU market, the sharing of patient-level data is especially hindered not only by ethical requirements but, specially, by the GDPR data transfer restrictions, imposing the need to implement, among others, appropriate safeguards[92], such as Standard Contractual Clauses (SCCs)[93]. However, if a synthetic dataset is created, the data exporter can more easily comply with the respective standards, which also allows saving resources, such as time and money[94]. In addition, concerning the saving of these two last resources, it has been pointed out that, with synthetic data, costs involved in all stages of the data lifecycle can be reduced.

[91] EDPB, "Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak", 2020

[92] Art. 46

[93] Art. 47

[94] LESHIN, Jonah; JOHNS, Quinn; "The Value of Synthetic Data in Healthcare"; Available at: https://www.datavant.com/blog/synthetic-data-healthcare

For instance, by developing a digital twin of the hospital, administrators were able to optimize staffing levels and allocate resources more efficiently[95].

Synthetic data has also shown promise in healthcare research to improve risk assessment, predictive analysis and protecting patient well-being, while maintaining ethical standards[96]. One of its uses is related to the improvement of policy implications. A study focused on demographic aging used variations regarding morbidity, disability, and doctor behavior to explore positive and negative policy outcomes on healthcare demand and resource utilization[97].

In addition, this type of data was shown to be useful in improving data scarcity and, consequently, raising data volume in imaging studies in the context of the COVID-19 pandemic[98]. Therefore, it can be applied in clinical challenges involving large populations in an epidemiological context.

VI. Disadvantages of the use of Synthetic Data

Despite the importance that synthetic data carries in terms of data processing in the healthcare domain, several concerns arise. Some disadvantages include the difficulty to generate the datasets, bias

---

[95] CHENG, Weibin; LIAN, Wanmin, TIAN, Junzhang; "Building the hospital intelligent twins for all-scenario intelligence health care"; *Digit Health*; 2022; available at: https://pubmed.ncbi.nlm.nih.gov/35720617/

[96] GIUFFRÈ, Mauro; SHUNG, Dennis, "Harnessing the Power of Synthetic Data in Healthcare: Innovation, Application, and Privacy", *npj Digital Medicine*, VI, 2023, available at: https://www.nature.com/articles/s41746-023-00927-3#citeas

[97] DAVIS, Peter; LAY-YEE, Roy; PEARSON, Janet; "Using micro-simulation to create a synthesised data set and test policy options: the case of health service effects under demographic ageing"; *Health Policy*, XCVII, 2, 2023, 267-274; available at: https://pubmed.ncbi.nlm.nih.gov/20800762/

[98] JIANG, Yifan; CHEN, Han; LOEW, Murray; KO, Hanseok; "COVID-19 CT Image Synthesis with a Conditional Generative Adversarial Network", *IEEE journal of biomedical and health informatics*, XXV, 2, 2021, 441 – 452

amplification and the complexity and lack of rigorous methods for assessing data quality[99].

First of all, complex data are difficult to generate, since the effectiveness of synthetic data generation techniques is most pronounced when the generated data is simple and can be defined by a set of rules or patterns. Generating intricate data, such as natural language text or more realistic images, poses a greater challenge and necessitates the application of more advanced techniques[100]. Furthermore, since the effectiveness of the model is tied to the source data quality, there is a risk of amplifying the bias inherent in the original dataset. This problem mostly results from the techniques used for data collection. Not only that, but one must also need to consider that the (generative) methods employed to obtain the new dataset can also lead to problems regarding automation bias[101]. Consequently, the risk inherent in (clinical) decisions made on the basis of this synthetic data can be wrongly assessed, perpetuating inequalities and contributing to the discrimination of vulnerable populations. For example, when the algorithm is trained with data that mostly considers people from a determined ethnicity, the synthetic dataset generated will end up mirroring this disequilibrium. Although this problem could be solved by oversampling the less

[99] GIUFFRÈ, Mauro; SHUNG, Dennis, "Harnessing the Power of Synthetic Data in Healthcare: Innovation, Application, and Privacy", *npj Digital Medicine*, VI, 2023, available at: https://www.nature.com/articles/s41746-023-00927-3#citeas

[100] Note the case when "the original data to be synthesized (e.g., data acquired in Living Labs) may consist of subjects' metadata (static) and a longitudinal component (set of time-dependent measurements), making it challenging to produce coherent synthetic counterparts." Regarding these considerations, ISASA, Imanol; HERNANDEZ, Mikel; EPELDE, Gorka; LONDOÑO, Francisco; BERISTAIN, Andoni; LARREA, Xabat, ALBERDI, Ane; BAMIDIS, Panagiotis; KONSTANTINIDIS Evdokimos, "Comparative assessment of synthetic time series generation approaches in healthcare: leveraging patient metadata for accurate data synthesis", *BMC Medical Informatics and Decision Making*, XXIV, 27, 2024; available at: https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-024-02427-0

[101] "There are considerable challenges associated with interpreting synthetic data generation models, including the black-box nature of generation algorithms, limitations in the evaluation metrics, and the potential for overfitting or underfitting". Regarding these considerations: GIUFFRÈ, Mauro; SHUNG, Dennis, "Harnessing the Power of Synthetic Data in Healthcare: Innovation, Application, and Privacy", *npj Digital Medicine*, VI, 2023, available at: https://www.nature.com/articles/s41746-023-00927-3#citeas

present characteristics, there is still a "risk of overgeneralization and potential creation of non-existent or incorrect correlations"[102], which can lead to the misrepresentation of the vulnerable population samples and the corresponding clinical profiles.

Another challenge associated with synthetic data is in the complexity of validating its accuracy[103]. Even if a synthetic dataset appears realistic and precise, determining whether it faithfully represents the underlying patterns of real-world data is challenging[104]. Consequently, it is not possible to assure that a model trained on synthetic data will demonstrate accuracy when deployed in the real-world context[105], since there is a lack of robust methods for assessing data quality. The main issue is related to the fact that the majority of the techniques employed for synthetic data generation do not consider the complexity and diversity of the possible different medical scenarios. Furthermore, since machine learning models have the tendency to excessively adapt the original data, leaks concerning individual records could end up being memorized, which means a higher reidentification risk[106].

Finally, another disadvantage of synthetic data results from the fact that the model used has a huge influence in the quality of the outcome

---

[102] GIUFFRÈ, Mauro; SHUNG, Dennis, "Harnessing the Power of Synthetic Data in Healthcare: Innovation, Application, and Privacy", *npj Digital Medicine*, VI, 2023, available at: https://www.nature.com/articles/s41746-023-00927-3#citeas

[103] GONZALES, Aldren; GURUSWAMY, Guruprabha; SMITH, Scott, "Synthetic data in health care: A narrative review", *PLOS Digit Health*, II, 1, 2023, available at: https://journals.plos.org/digitalhealth/article?id=10.1371/journal.pdig.0000082

[104] Not only that, but note that the black-box nature of GANs makes it harder to foresee which data utility is maintained/lost in the creation process (this is especially relevant when it comes to sensitive data). Regarding these considerations, KAABACHI, Bayrem; DESPRAZ Jérémie, MEURERS Thierry; OTTE, Karen; HALILOVIC, Mehmed; PRASSER, Fabian; RAISARO, Jean Louis, "Can We Trust Synthetic Data in Medicine? A Scoping Review of Privacy and Utility Metrics", *MedRxiv*, 2023, available at: https://www.medrxiv.org/content/10.1101/2023.11.28.23299124v1.full

[105] LAMBERTI, Aldo, "The Benefits and Limitations of Generating Synthetic Data"; available at: https://syntheticus.ai/blog/the-benefits-and-limitations-of-generating-synthetic-data

[106] KAABACHI, Bayrem; DESPRAZ Jérémie, MEURERS Thierry; OTTE, Karen; HALILOVIC, Mehmed; PRASSER, Fabian; RAISARO, Jean Louis, "Can We Trust Synthetic Data in Medicine? A Scoping Review of Privacy and Utility Metrics", *MedRxiv*, 2023, available at: https://www.medrxiv.org/content/10.1101/2023.11.28.23299124v1.full

data. Considering this, it is important to understand that it may be vulnerable to statistical noise, which can lead to incorrect classification of the data and the production of strongly unreliable outputs[107].

VII. Conclusion

As previously mentioned, processing of personal data for purposes of healthcare scientific research has faced significant obstacles, namely, the necessity to overcome limitations on data protection legislation and other regulatory restrictions, mostly related to ethical aspects for sharing and securing data. Other limitations include data fragmentation, monetary constraints on accessing data outside the public domain and the lack of high-quality datasets.

Synthetic data has been one of the solutions presented, introducing several innovative applications. This type of data (considered a "privacy enhancing technique"[108]) makes it difficult to identify the data subject since it allows the risk associated with processing activities to be mitigated to a large extent. Consequently, this can even lead to the non-application of data protection legislation when anonymous data is at stake (note that the GDPR framework does not apply to anonymous data[109]). Remember that the classification of synthetic data as personal data depends on the compliance with the "reasonableness criteria"[110]. This is particularly evident since the synthesis processes should be considered a technical measure for the purposes of achieving data minimization and, consequently, an "appropriate safeguard" in the terms of art. 89(1). That being said, compliance with data protection legislation is greatly facilitated, which will consequently make it easier to

[107] GONZALES, Aldren; GURUSWAMY, Guruprabha; SMITH, Scott, "Synthetic data in health care: A narrative review", *PLOS Digit Health*, II, 1, 2023, available at: https://journals.plos.org/digitalhealth/article?id=10.1371/journal.pdig.0000082

[108] Section V.

[109] Note recital 26

[110] Section III, Item ii

comply with ethical rules or requirements and, by that, allowing for researchers to easily share data between them, especially when dealing with international transfers.

Synthetic data carries several other benefits, such as reducing operational and data accessing costs (especially when accessing health related datasets outside of the public domain), providing medical data resources that have higher quality and variety (namely, images, audio-files, videos) – what, consequently, helps in overcoming inaccuracies, bias of real-world, as well as data fragmentation – and, lastly, improving policy implications. Thus, synthetic data allows for continuous research conduction, since, among other factors, the results and case studies are easier to replicate[111-112].

Although there is no regulatory landscape specifically aimed at the processing of synthetic data, there have been some initiatives to implement its use for healthcare research purposes. However, it is still necessary to create legal guidelines, best practices and other recommendations that ensure consistency and reliability of the synthetic data created, which would require the intervention of major stakeholders – such as the EDPS and the European Data Protection Board (EDPB) –, as well of national data protection authorities and the European Health Data Space. This means that, on a regulatory level, it is still important to establish consistency around operational, methodological, and technical matters[113].

Nevertheless, the usage of synthetic data also presents some relevant disadvantages, such as the difficulty to generate the dataset, bias

---

[111] DILMEGANI, Cem; "Synthetic Data for Healthcare: Benefits & Case Studies in 2024"; Available at: https://research.aimultiple.com/synthetic-data-healthcare/

[112] KAABACHI, Bayrem; DESPRAZ, Jérémie; MEURERS, Thierry; OTTE, Karen; HALILOVIC, Mehmed, PRASSER, Fabian; RAISARO Jean Louis; "Can We Trust Synthetic Data in Medicine? A Scoping Review of Privacy and Utility Metrics"; *MedRxiv*, 2023; available at: https://www.medrxiv.org/content/10.1101/2023.11.28.23299124v1.full

[113] ALLOZA, Clara; KNOX, Bethany; RAAD, Hanaya; AGUILÀ, Mireia; COAKLEY, Ciara; MOHROVA, Zuzana; BOIN, Élodie; BÉNARD, Marc; DAVIES, Jessica; JACQUOT, Emmanuelle; LECOMTE Coralie; FABRE, Alban; BATECH, Michael, "A Case for Synthetic Data in Regulatory Decision-Making in Europe", CXIV, 4, 2023, 795-801; available at: https://ascpt.onlinelibrary.wiley.com/doi/10.1002/cpt.3001

amplification and the complexity and lack of rigorous methods for assessing quality of the data and of the tools used. These challenges can be overcome through some mitigation measures, such as the establishment of guidelines and policies in order to properly carry out the synthetic data generation throughout the lifecycle of the research project[114]. This also involves ensuring documentation not only on the data generation process, but also on possible limitations and the existence of bias, which is useful in identifying actual and potential errors[115]. It is also important to ensure that various public and private entities join forces to collaborate, namely public and private data owners, healthcare solution developers, and synthetic data experts, guaranteeing multidisciplinary insights[116].

In particular, note the establishment of proper synthetic data generation lifecycle frameworks[117] and the analysis of clinical quality measures as ways to provide researchers a better approach to define and describe the process of validating synthetic datasets. In order to properly validate the quality of the mechanisms for synthetic data generation, the creation of domain-specific evaluation metrics and benchmarks particularly tailored for healthcare applications should be considered. On the one hand, these evaluation metrics can be created

---

[114] J. CHEN, Richard; LU, Ming Y; Y. CHEN, Tiffany; F. K. WILLIAMSON, Drew; MAHMOOD, Faisal; "Synthetic data in machine learning for medicine and healthcare"; *Nature Biomedical Engineering volume*, V, 2021, 493-497.

[115] GIUFFRÈ, Mauro; SHUNG, Dennis, "Harnessing the Power of Synthetic Data in Healthcare: Innovation, Application, and Privacy", *npj Digital Medicine*, VI, 2023, available at: https://www.nature.com/articles/s41746-023-00927-3#citeas

[116] IHI; "Maximising the potential of synthetic data generation in healthcare applications"; *A Innovative Health Initiative Call Topic*; 2023; available at: https://health.ec.europa.eu/ehealth--digital-health-and-care/european-health-data-space_en

[117] Note the case of the ATEN Framework, that is composed of other three approaches that provide for: synthetic data generation; a way to define and describe the elements of realism, and; an approach for validating synthetic data. Regarding these considerations, MCLACHLAN, Scott; DUBE, Kudakwashe; GALLAGHER, Thomas; A. WALONOSKI, Jason; "The ATEN Framework for Creating the Realistic Synthetic Electronic Health Record", *HEALTHINF, SCITEPRESS – Science and Technology Publications*, 5, 2018, 220-230. available at: https://www.researchgate.net/publication/322653777_The_ATEN_Framework_for_Creating_the_Realistic_Synthetic_Electronic_Health_Record

by the development of platforms that also provide methods for assessing utility and privacy and, consequently, streamlining the evaluation process[118]. On the other hand, a benchmark that accurately allows the representation of a wide spectrum of real-world medical scenarios, provides a way to properly compare the performance of several methods for the purposes of creating synthetic data[119]. It is also crucial that the generation of synthetic data is accompanied by consistent evaluations to minimize biases, including the implementation of auditing methods. Strategies include the implementation of anomaly detection techniques[120] and other advanced statistical methods such as distribution matching, correlation analysis, and dimensionality reduction, that allow capturing the complex correlations and patterns inherent in the original dataset, improving the data's representativeness[121].

After balancing the advantages and disadvantages of applying and using synthetic data, as well as possible solutions to overcome the latter, it is possible to conclude that the use of this type of data for the purposes of scientific healthcare research does indeed present the potential to be considered a "Holy Grail". However, there is still a long way to go, especially in regulatory terms.

---

[118] KAABACHI, Bayrem; DESPRAZ Jérémie, MEURERS Thierry; OTTE, Karen; HALILOVIC, Mehmed; PRASSER, Fabian; RAISARO, Jean Louis, "Can We Trust Synthetic Data in Medicine? A Scoping Review of Privacy and Utility Metrics", *MedRxiv,* 2023, available at: https://www.medrxiv.org/content/10.1101/2023.11.28.23299124v1.full

[119] GIUFFRÈ, Mauro; SHUNG, Dennis, "Harnessing the Power of Synthetic Data in Healthcare: Innovation, Application, and Privacy", *npj Digital Medicine*, 6, 2023, available at: https://www.nature.com/articles/s41746-023-00927-3#citeas

[120] Since overconfidence problems are common in synthetic data generation, these techniques allow to "identify instances that deviate significantly from the training data distribution helping to detect and handle out-of-distribution problems". Regarding these considerations, GIUFFRÈ, Mauro; SHUNG, Dennis, "Harnessing the Power of Synthetic Data in Healthcare: Innovation, Application, and Privacy", *npj Digital Medicine*, 6, 2023, available at: https://www.nature.com/articles/s41746-023-00927-3#citeas; MÖLLER, Felix; BOTACHE, Diego; HUSELJIC, Denis; HEIDECKER, Florian; BIESHAAR, Maarten; SICK, Bernhard; "Out-of-distribution Detection and Generation using Soft Brownian Offset Sampling and Autoencoders", *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, 2021.

[121] GIUFFRÈ, Mauro; SHUNG, Dennis, "Harnessing the Power of Synthetic Data in Healthcare: Innovation, Application, and Privacy", *npj Digital Medicine*, 6, 2023, available at: https://www.nature.com/articles/s41746-023-00927-3#citeas

A obrigação de notificar uma violação de dados pessoais à Autoridade de Controlo[1]

Luís Pinto Monteiro[2]

Resumo: O presente artigo visa analisar o dever ínsito no artigo 33.º do Regulamento Geral sobre a Proteção de Dados, mais precisamente a obrigação de notificar uma violação de dados pessoais à autoridade de controlo e a sua compatibilidade com o princípio fundamental do *nemo tenetur se ipsum accusare*, através do qual ninguém pode ser obrigado a cooperar com a sua autoincriminação.

Palavras-chave: *RGPD; data-breach; nemo tenetur; notificação à autoridade de controlo; dever de colaboração com autoridade de controlo.*

Abstract: This article aims to analyse the duty established under Article 33 of the General Data Protection Regulation, more precisely the obligation to notify a personal data breach to the supervisory authority and its compatibility with the fundamental principle *nemo tenetur se ipsum accusare*, according to which no one is bound to incriminate himself.

---

[1] O presente texto corresponde ao trabalho final realizado no âmbito da IV Pós-Graduação Avançada em Direito da Proteção de Dados, lecionado pelo Centro de Investigação de Direito Privado da Faculdade de Direito da Universidade de Lisboa. O autor aproveita o ensejo para agradecer ao ilustre causídico Gonçalo de Carvalho Azevedo pela revisão do documento para efeitos de publicação e pela frutífera troca de ideias.

[2] Advogado. Especialista em Direito Europeu e da Concorrência. Mestrado em Direito Intelectual pela Faculdade de Direito da Universidade de Lisboa, LL.M. em *Trade and Regulation* (vertente Antitrust) pela New York University (NYU), Pós-graduação em Direito da Proteção de Dados pela Universidade Católica Portuguesa e Pós-graduação Avançada em Proteção de Dados pela Faculdade de Direito da Universidade de Lisboa. CDPP – *Certified Data Protection Practitioner* pela ICS. Mais detalhes disponíveis em https://www.linkedin.com/in/luispintomonteiro/

Keywords: *GDPR; data-breach; nemo tenetur; notification to the supervisory authority; duty to cooperate with the supervisory authority.*

I. INTRODUÇÃO

Numa época vincadamente marcada por desenvolvimentos tecnológicos constantes, e num mercado em permanente mutação a um ritmo sem precedentes, são poucos aqueles que se podem dar ao luxo de viver à margem do mundo digital.

Em virtude desta realidade, a quantidade de informação recolhida relativa à vida dos internautas é absolutamente avassaladora e muitas das vezes até desconhecida da generalidade das pessoas.

As empresas detentoras de motores de pesquisa e outros tantos colossos tecnológicos a que recorremos numa base diária ou quase diária, têm acesso a uma pegada digital massificada, com a capacidade de, em conjunto ou até de forma isolada, reconstituir cada passo das nossas vidas, e inclusive gozam da aptidão de saberem mais do que cada um de nós gostaria[3]. Nesta realidade virtual, a privacidade, o segredo e o anonimato que a generalidade de nós preza, pura e simplesmente, desapareceu.

De modo que, é precisamente neste contexto de controlar e combater os perigos que advêm de um acesso indiscriminado e sem peias à informação dos particulares que a União Europeia revogou a Diretiva 95/46/CE e aprovou uma vigorosa legislação no âmbito da proteção de

[3] Neste contexto tornou-se célebre a história da cadeia de supermercados Target que soube da gravidez de uma estudante, ainda dependente dos pais, antes mesmo de esta comunicar tal notícia aos seus familiares. A descoberta ocorreu pela simples análise dos dados relativos às compras da estudante, levando a que existisse publicidade direcionada para o estádio da gravidez que havia sido detetado. Acabou por ser esta cadeia de supermercados que, de forma inadvertida, comunicou a notícia aos pais através de publicidade direcionada dirigida àquela estudante. Ver para o efeito https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

Dados Pessoais por intermédio do Regulamento (UE) 2016/679 ("RGPD")[4].

Não é obviamente nosso propósito analisar o RGPD na sua integralidade e determinar o impacto que este regime jurídico tem na vida dos particulares e das empresas. Tal aventura revelar-se-ia manifestamente inglória, atendendo aos limites impostos a trabalhos desta natureza. Ao invés, propomo-nos focar especificamente na obrigação que incide sobre o Responsável pelo Tratamento de dados de notificar uma violação de dados pessoais[5] à Autoridade de Controlo competente, sem demora injustificada e, sempre que possível, num período máximo de 72 horas após ter tido conhecimento dessa violação, a menos que esta violação não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Com efeito, tal dever encontra-se atualmente consagrado no artigo 33.º do RGPD[6].

---

[4] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27.4.2016 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.

[5] Como sucede normalmente nesta área do direito, utilizaremos a expressão anglo-saxónica "*data breach*" como sinónimo de violação de dados pessoais.

[6] O artigo 33.º do RGPD estabelece o seguinte: (1) Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo 55.º, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso. (2) O subcontratante notifica o responsável pelo tratamento sem demora injustificada após ter conhecimento de uma violação de dados pessoais. (3) A notificação referida no n.º 1 deve, pelo menos: a) Descrever a 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; (b) Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações; (c) Descrever as consequências prováveis da violação de dados pessoais; (d) Descrever as 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. (4) Caso, e na medida em que não seja possível fornecer todas as informações ao mesmo tempo, estas podem ser fornecidas por fases, sem demora injustificada. (5) 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.

II. A OBRIGAÇÃO DE NOTIFICAR A AUTORIDADE DE CONTROLO EM CASO DE VIOLAÇÃO DE DADOS PESSOAIS

a. A origem da imposição legal

Se atendermos à génese desta obrigação, constatamos tratar-se de uma inovação recente. Tal sucede porque a Diretiva 95/46/CE não previa esta incumbência ao Responsável pelo Tratamento, nem tampouco a qualquer outro sujeito que viesse a ter conhecimento de tal facto. Esta diligência surge na proposta de Regulamento de 2012, mais especificamente no seu artigo 31.º[7]. Neste artigo previu-se, em termos muito similares aos que hoje se estabelecem no RGPD, um dever de alertar a Autoridade de Controlo do sucedido e dos detalhes desse *data breach*. Daí para a frente, ao longo de toda a discussão do RGPD, o dever de transmitir as violações à Autoridade de Controlo não mais desapareceu. Simplesmente surgiram alguns matizes, sendo que o mais relevante assentou precisamente no prazo para o cumprimento deste dever de comunicação que passou das escassas 24 horas, para um prazo um pouco mais alargado de 72 horas[8].

---

[7] *Vide* Proposta de Regulamento do Parlamento e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral Sobre a Proteção de Dados), Bruxelas, 25.1.2012, COM(2012) 11 final disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52012PC0011.

[8] Para uma análise mais aprofundada sobre a evolução desta exigência legal *vide* também: i) o Parecer do Comité Económico e Social Europeu sobre a Proposta do RGPD disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52012XX0630(01); ii) o Parecer do Comité Económico e Social Europeu sobre a «Proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados» (regulamento geral sobre a proteção de dados) disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52012AE1303; iii) a Posição (UE) N.º 6/2016 do Conselho em primeira leitura com vista à adoção do Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e 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:52016AG0006(01); e a Resolução legislativa do Parlamento Europeu, de 12 de março de 2014, sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral de proteção de dados) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD) disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52014AP0212. Para uma fotografia ainda mais detalhada da evolução do processo *vide* https://eur-lex.europa.eu/procedure/PT/2012_11.

A *ratio* desta norma encontra-se certamente alicerçada num dever de colaborar com a entidade supervisora incumbida de controlar e fiscalizar o cumprimento das normas relativas à proteção de dados pessoais.

A supervisão assume aqui uma dupla dimensão: uma vertente preventiva, criando sobre o Responsável pelo Tratamento um apertado ónus, de modo a impeli-lo a implementar todos os mecanismos possíveis para garantir a segurança no tratamento de dados pessoais, e, assim, acautelar violações da Lei; bem como uma vertente repressiva, dirigida à censura e punição dessas mesmas infrações, seja mediante a instrução de processos sancionatórios de natureza contraordenacional com a correspondente e eventual aplicação de coimas, seja mediante a transmissão da compete notícia dos indícios de um crime ao Ministério Público para a abertura do respetivo inquérito de natureza penal em ordenamentos jurídicos como o português[9].

Talvez ao estabelecer este dever de avisar a Autoridade de Supervisão, o legislador terá tido em consideração o potencial número de violações que podem vir a ocorrer de diversos quadrantes, com consequências muito nefastas para os titulares dos dados pessoais e que podem passar por despercebidas em virtude dos escassos recursos de que estão dotadas as Autoridades de Controlo. Tais situações sairiam agravadas perante o silêncio do Responsável pelo Tratamento, que ao não dar "*sinal de alarme*", permitiria a circulação da informação por diversos canais sem que o lesado tivesse consciência disso. Pense-se, por exemplo, numa situação de *data breach* de uma base de dados hospitalar que contém informações sobre pessoas infetadas com o vírus da imunodeficiência humana. Perante tamanho *data breach*, um eventual silêncio do Responsável pelo Tratamento e uma subsequente apatia para evitar a publicitação e proliferação desses dados, poderia gerar consequências devastadoras para os respetivos pacientes/ titulares dos dados

[9] A censura penal não é algo que decorra diretamente do ordenamento jurídico da União Europeia, naturalmente, mas antes de uma prorrogativa dada aos Estados-membros de prever sanções mais apertadas do que aquelas que se encontram estabelecidas no RGPD.

pessoais. Sobretudo em situações em que os pacientes tenham optado pela reserva da informação enquanto lutam pela vida. Com a agravante de com o passar do tempo se tornar cada vez mais difícil identificar a origem do *data breach* que havia levado a que os dados pessoais «transpirassem» para o domínio público.

De modo que, a obrigação de comunicar uma violação de dados pessoais à Autoridade de Controlo, para além da vertente preventiva e repressiva acima mencionadas, visa também dotar a Autoridade de Controlo dos meios que lhe permitem monitorizar e tentar minimizar os impactos que tais violações podem ter nos titulares dos dados pessoais. Uma vez alertada para a situação, a Autoridade de Controlo terá outros mecanismos ao seu dispor para se articular com as autoridades nacionais e internacionais com vista a minimizar os danos.

O simples facto de existir uma obrigação de comunicar e um dever de identificar as medidas adotadas e a adotar, permite acompanhar os impactos da violação de dados pessoais junto do Responsável pelo Tratamento. Esta simples obrigação determina, bem assim, que o Responsável pelo Tratamento não fique quieto, mas antes faça tudo o que esteja ao seu alcance para controlar e mitigar os efeitos da situação.

Assim, perante a incapacidade de dotar as Autoridades de Controlo dos meios para identificar e acompanhar todas as violações de dados pessoais, exige-se à entidade melhor posicionada para detetar essa violação (*i.e.* o Responsável pelo Tratamento), a colaboração com a entidade de supervisão.

b. A omissão de notificar a violação à Autoridade de Controlo

Com efeito, como oportunamente demos nota, o artigo 33.º do RGPD exige ao Responsável pelo Tratamento, a obrigação de notificar um *data breach* à Autoridade de Controlo. Esta norma prevê igualmente um conjunto de obrigações acessórias com vista a monitorizar e controlar os impactos que tal *data breach* possa ter para os titulares dos dados pessoais.

Nesta senda, a nossa legislação nacional, nos n.ºs 1 e 2 do artigo 8.º da Lei n.º 58/2019, de 8.8 ("Lei de Execução do RGPD"), estabelece um dever genérico dirigido às entidades públicas e privadas de colaborar com a CNPD.

Importa a este propósito salientar igualmente que a alínea a) do n.º 4 do artigo 83.º do RGPD, prevê coimas até 10 000 000 de euros para pessoas singulares, ou coimas até 2% do volume de negócios a nível mundial para empresas, na eventualidade das obrigações constantes do artigo 33.º do RGPD não ser cumpridas.

Ora, o acima exposto não se confunde com as coimas potencialmente aplicadas em virtude do *data breach* em si mesmo considerado. Para estas, a previsão legal encontra-se no n.º 5 do artigo 83.º do RGPD e nos artigos 37.º e 38.º da Lei de Execução do RGPD.

Sem embargo, para o tema em análise afigura-se da maior relevância alertar para o facto de a Lei de Execução do RGPD prever que a utilização de dados de forma incompatível com a finalidade da recolha (artigo 46.º), o acesso indevido (artigo 47.º), o desvio de dados (artigo 48.º) e a viciação ou destruição de dados (artigo 49.º) – todas estas práticas consideradas como *data breaches* –, contemplam como sanção uma pena privativa da liberdade.

Sem embargo de o artigo 54.º da Lei de Execução do RGPD prever a responsabilidade penal das pessoas coletivas ou equiparadas, o que neste ponto se expressa torna-se especialmente relevante nas situações em que o Responsável pelo Tratamento é ele próprio o prevaricador, isto é, o sujeito responsável pela violação das normas acima citadas.

c. As dúvidas quanto à legalidade do dever de colaboração

Sucede, porém, que esta opção legislativa quanto à exigência de colaborar com as Autoridades de Controlo, apesar de deixar bem patente as suas virtudes no sentido de acautelar a posição do titular dos dados pessoais, suscita também inúmeras questões nos ordenamentos jurídicos que consagram princípios básicos inerentes ao Estado Direito.

Entre essas dúvidas, destaca-se a opção legislativa quanto ao dever de colaborar ínsito no RGPD no sentido de saber se não poderá ser considerado contrário ao princípio do *nemo tenetur se ipsum accusare*, já que neste dever de colaboração se poderá estar a forçar o visado a contribuir para a sua própria incriminação.

A obrigação de colaborar imposta pelo artigo 33.º do RGPD poderá porventura subverter os mais elementares princípios do processo penal e contraordenacional, na medida em que se impõe ao visado e putativo arguido – sob ameaça de sanções[10] –, contribuir com o reconhecimento de factos que podem levar à sua condenação em processo contraordenacional, tal como estabelece o n.º 5 do artigo 83.º do RGPD, ou mesmo penal, tal como prescreve a secção III da Lei de Execução do RGPD.

Quando analisamos esta questão no âmbito dos deveres de informar a Autoridade de Controlo da existência de uma violação de dados pessoais no contexto do artigo 33.º do RGPD, a realidade não se reconduz pura e simplesmente à discussão sobre a licitude ou ilicitude associada à utilização de documentos e informações recolhidas e/ou exigidas no contexto de uma investigação no exercício dos poderes de supervisão da Autoridade de Controlo.

O problema ascende a um patamar mais elevado, pois reside, ao invés, no facto de se obrigar o Responsável pelo Tratamento a, num curtíssimo espaço de tempo, sem grande margem para uma refletida ponderação da sua estratégia de defesa, e sem que haja qualquer investigação em curso por parte da Autoridade de Controlo, a espoletar uma autodenúncia quanto à existência de uma violação de dados pessoais do qual ele próprio é o responsável, e, para mais, a facultar informação detalhada sobre essa ocorrência através da partilha de factos que irremediavelmente o comprometem.

Dito de outro modo: exige-se ao prevaricador que se autodenuncie e que assista a Autoridade de Controlo a construir o discurso para a sua punição. Trata-se de uma exigência de adotar uma conduta que

[10] Tal como estabelece a alínea a) do n.º 4 do artigo 83.º do RGPD.

poderá naturalmente dar origem a um processo de natureza contraordenacional e/ou criminal, em que o visado/arguido é determinado a apresentar-se como o seu próprio delator e a auxiliar o seu algoz[11].

Nesta linha, cumpre então perguntar:

i) seria aceitável afirmar que o *nemo tenetur* atribui ao visado e potencial arguido um conjunto de direitos fundamentais, que lhe permitiriam licitamente não prestar declarações sobre os factos que lhe pudessem ser imputados e a não fornecer as provas que o pudessem incriminar, estabelecendo, deste modo, limites ao legislador europeu e nacional no momento da elaboração e aprovação do RGPD e da sua Lei de Execução? Nesta primeira visão, o legislador teria extravasado as suas competências e optado por uma solução ilegal e atentatória dos princípios fundamentais de um Estado de Direito democrático; ou
ii) haveria limites que poderiam ser impostos a este direito ao silêncio e à não cooperação com as Autoridades de Controlo por parte do visado e eventual arguido, com um propósito de salvaguardar um valor superior ligado às nefastas consequências que advêm de uma ausência de contenção dos danos decorrentes da violação de dados pessoais? Nesta segunda visão, o legislador teria andado bem face aos interesses em conflito.

A resposta a estas questões tem de passar por uma análise crítica do ordenamento jurídico atual, de modo a aferir se tal dever de colaboração, da forma como foi equacionado, se encontra em sintonia com as normas e princípios fundamentais que norteiam a nossa sociedade integrada num Estado de Direito moderno.

[11] Um procedimento deveras inédito e mais próximo do antigo processo inquisitório do que o acusatório que atualmente vigora.

III. NEMO TENETUR SE IPSUM ACCUSARE

a. A visão nacional sobre o dever de colaborar com as Autoridades e o *Nemo Tenetur Se Ipsum Accusare*

O *nemo tenetur* contém uma renúncia por parte do Estado a quaisquer formas de coação tidas como abusivas cujo propósito fosse conduzir o visado a colaborar na sua autoincriminação no âmbito de um processo sancionatório[12]. Trata-se de um princípio genericamente consagrado expressa ou implicitamente nas legislações dos Estados de Direito modernos e, bem assim, em instrumentos de direito internacional subscritos por esses Estados[13].

Como explicam Augusto Silva Dias e Vânia Costa Ramos: "*o princípio nemo tenetur goza de consagração constitucional implícita no Direito português, como vimos, e desdobra-se numa série de corolários, o mais importante dos quais é o direito ao silêncio. (...) Pode afirmar-se que este direito constitui o núcleo do nemo tenetur*".[14] E "*segundo as concepções doutrinais mais restritivas do princípio [do nemo tenetur], este confunde-se com aquele [núcleo, que equivale ao silêncio]*."[15] Sendo certo que os titulares deste direito são precisamente o arguido, suspeito ou visado[16].

Na maioria dos Estados de Direito modernos e democráticos, o arguido é tido como um autêntico e genuíno sujeito processual, a quem são reconhecidos direitos e deveres essenciais que visam evitar que este seja instrumentalizado para obter prova em seu desfavor.

---

[12] OLIVEIRA E SILVA, Sandra, *O Arguido como Meio de Prova Contra Si Mesmo – considerações em torno do princípio Nemo Tenetur Se Ipsum Accusare*, Almedina, 2019, pág. 354. *Vide* também o acórdão n.º 461/2011 do Tribunal Constitucional de 11.10.2011, processo n.º 366/11, 2.ª secção, parágrafo 10, pág. 12.

[13] FIGUEIREDO DIAS, Jorge de, COSTA ANDRADE, Manuel da e COSTA PINTO, Frederico de Lacerda da, "Supervisão, Direito ao Silêncio e Legalidade da Prova", *in Estudos sobre o Mercado de Valores Mobiliários*, Almedina, 2009, pág. 37.

[14] SILVA DIAS, Augusto e COSTA RAMOS, Vânia, *O Direito à Não Auto-Inculpação (Nemo Tenetur Se Ipsum Accusare) no Processo Penal e Contra-Ordenacional Português*, Coimbra Editora, 2009, págs. 19 e 20.

[15] *Ibidem*, pág. 21.

[16] *Ibidem*, pág. 20.

Como refere ainda a nossa jurisprudência: "*(...) considera-se que o direito à não-autoincriminação encontra o seu fundamento jurídico-constitucional imediato nas garantias processuais de defesa do arguido, destinadas a assegurar um processo equitativo, relacionando-se, de forma mediata ou reflexa, com os direitos fundamentais de matiz mais substantiva aludidos supra*"[17]. Esta mesma instância jurisdicional afirmou noutra sede inclusive: "*O princípio nemo tenetur se ipsum accusare, é uma marca irrenunciável do processo penal de estrutura acusatória, visando garantir que o arguido não seja reduzido a mero objeto da atividade estadual de repressão do crime, devendo antes ser-lhe atribuído o papel de verdadeiro sujeito processual, armado com os direitos de defesa e tratado como presumivelmente inocente. Daí que para proteção da autodeterminação do arguido, este deva ter a possibilidade de decidir, no exercício de uma plena liberdade de vontade, qual a posição a tomar perante a matéria que constitui objeto do processo.*"[18]

Para além do *supra* exposto, impõe-se acrescentar também que no ordenamento jurídico português, apesar do princípio do *nemo tenetur se ipsum accusare* não encontrar consagração expressa, tal parece decorrer claramente dos artigos 60.º e 61.º do CPP, sendo que o direito ao silêncio encontra a sua expressão na alínea d) do n.º 1 do artigo 61.º do CPP[19].

Em consonância com o que acima se expõe, não poderão ser valorados negativamente o silêncio total ou parcial, tal como estabelece,

---

[17] Acórdão n.º 461/2011 do Tribunal Constitucional de 11.10.2011, *cit.*, parágrafo 10, pág. 12.

[18] Acórdão n.º 340/2013 do Tribunal Constitucional de 17.6.2013, processo n.º 817/12, 2.ª secção, ponto 2, pág. 8.

[19] Nas palavras de SILVA DIAS, Augusto e COSTA RAMOS, Vânia: "*Ao contrário de outras Leis Fundamentais, a Constituição da República Portuguesa (CRP) não tutela expressamente o nemo tenetur. A consagração expressa do princípio surge apenas no Código de Processo Penal (CPP), na vertente do direito ao silêncio (art. 61.º, n.º 1, al. d), 132.º, n.º 2, 141.º, n.º 4, al. a), e 343.º, n.º 1, do CPP). Maugrado a ausência de previsão expressa na CRP, tanto a doutrina como a jurisprudência portuguesa são unânimes quanto à natureza constitucional implícita do nemo tenetur*", *in O Direito À Não Auto-Inculpação (Nemo Tenetur Se Ipsum Accusare) No Processo Penal e Contra-Ordenacional Português*, *cit.*, págs. 14 e 15.

aliás, respetivamente, o n.º 1 do artigo 343.º do CPP e o n.º 1 do artigo 345.º do CPP.

De modo que o *nemo tenetur* afigura-se no nosso ordenamento jurídico como princípio constitucional não escrito, mas de pleno vigor e absolutamente inquestionável[20]. Trata-se da tutela jurídico-constitucional de valores fundamentais associados à dignidade da pessoa humana que não podem ser descurados[21]. Em sintonia com esta ideia, a restrição ao presente princípio deve ser feita com as devidas cautelas.

Existe, portanto, uma íntima relação entre o direito à não-autoincriminação e o direito ao silêncio. Como refere a nossa jurisprudência: "*O princípio em causa implica o reconhecimento do direito ao silêncio e do direito do arguido à não autoincriminação enquanto elementos de um processo penal de estrutura acusatória. O primeiro daqueles direitos [i.e. o direito ao silêncio] traduz-se na faculdade reconhecida ao arguido de não se pronunciar sobre os factos que lhe são imputados, diferentemente do que sucedia nos processos regidos pelo princípio do inquisitório em que as declarações obrigatórias do arguido, maxime a confissão forçada, tendem a convertê-lo em instrumento da sua própria condenação. O direito ao silêncio tem vindo a ser reconhecido pela legislação processual penal da maioria dos ordenamentos jurídicos dos Estados de direito modernos, encontrando também consagração expressa em instrumentos jurídicos internacionais (cf. o artigo 6.º da Convenção Europeia dos Direitos do Homem e artigo 14.º do Pacto Internacional sobre Direitos Civis e Políticos). Já o segundo [i.e.* o *direito do arguido à não autoincriminação], entendido como direito a não contribuir para a sua própria incriminação, impede a transformação do arguido em meio de prova por via de uma colaboração involuntária obtida com recurso a meios coercivos ou enganosos. Existe uma ligação íntima entre os dois direitos, desde logo porque, não sendo reconhecido*

[20] Acórdão n.º 340/2013 do Tribunal Constitucional de 17.6.2013, *cit.*, ponto 2, pág. 7 e acórdão n.º 298/2019 do Tribunal Constitucional de 15.5.2019, processo n.º 1043/17, 2.ª secção, ponto 11, pág. 11.

[21] Acórdão n.º 340/2013 do Tribunal Constitucional de 17.6.2013, *cit.*, ponto 2, pág. 8.

ao arguido o direito a manter-se em silêncio, este seria obrigado a pronunciar-se e a revelar informações que poderiam contribuir para a sua condenação. Daí a correlação do nemo tenetur com a afirmação do arguido enquanto sujeito processual e, em particular, com a sua liberdade de declaração, uma vez que é nesta última que se espelha o estatuto do arguido como autêntico sujeito processual, decidindo, por força da sua liberdade e responsabilidade, sobre se e como quer pronunciar-se sobre os factos que lhe são imputados (cf. o Acórdão n.º 304/2004). De resto, a jurisprudência do Tribunal Europeu dos Direitos do Homem ("TEDH") tem reconhecido que o direito à não autoincriminação se relaciona, em primeira linha, com o respeito pela vontade do arguido em "permanecer em silêncio", em não prestar declarações (cf., por exemplo, os Acórdãos de 17 de dezembro de 1996, Sauders c. Reino Unido, Queixa n.º 19187/91, § 69; e de 21 de dezembro de 2000, Heaney and McGuiness c. Irlanda, Queixa n.º 34720/97, § 40)."[22]

Por conseguinte, atendendo ao *supra* aludido, parece acertado afirmar que, *grosso modo*, o direito à não-autoincriminação permite ao visado permanecer em silêncio para evitar agravar a sua posição num procedimento de natureza sancionatória.

Mas como se infere de tudo o que se vem dizendo até ao momento, não só do silêncio é composto o *nemo tenetur*. Trata-se de um princípio de elevada abrangência que comporta qualquer atuação do próprio visado que permita às autoridades provar uma acusação que contra si impenda, incluindo, entre outras prerrogativas, o direito a não facultar meios de prova que em última instância o prejudiquem[23].

No entanto, parece também indiscutível que o *nemo tenetur* não pode equivaler a um direito absoluto de não cooperar com as autoridades, comportando, em bom rigor, algumas limitações[24].

---

[22] Acórdão n.º 298/2019 do Tribunal Constitucional de 15.5.2019, *cit.*, ponto 10, pág. 10.

[23] Acórdão n.º 461/2011 do Tribunal Constitucional de 11.10.2011, *cit.*, parágrafo 10, pág. 12.

[24] FIGUEIREDO DIAS, Jorge de, COSTA ANDRADE, Manuel da e COSTA PINTO, Frederico de Lacerda da, "Supervisão, Direito ao Silêncio e Legalidade da Prova", *cit.*, pág. 38.

Ora, no âmbito penal pode haver limitações ao *nemo tenetur* relacionadas com a necessidade de recolha de impressões digitais, amostras de sopro, sangue e urina, bem como tecidos corporais para realizar testes de ADN que carecem da colaboração do arguido[25].

Já no âmbito contraordenacional são frequentes as limitações mais amplas ao *nemo tenetur* determinadas pelo dever de colaboração com as autoridades de supervisão, como a obrigação de prestar informações escritas ou orais, ou a cedência de documentos pré-existentes, de modo a permitir a supervisão e a fiscalização na prossecução das missões que lhes foram confiadas[26].

Como refere Figueiredo Dias e Costa Andrade: "*as restrições ao nemo tenetur situam-se (...) por excelência no âmbito do direito penal secundário e no âmbito do direito sancionatório de caráter administrativo, perante situações em que os arguidos são, na maioria das vezes pessoas coletivas. Daí que, fora deste quadro material (domínio económico) e subjetivo (pessoas coletivas), se deva seguir uma visão mais clássica do princípio nemo tenetur (...).*"[27]

Em qualquer dos casos, penal ou contraordenacional, como refere a nossa jurisprudência: *"para que a restrição seja legítima, a doutrina*

---

[25] Acórdão do TEDH *Saunders c. Reino Unido*, pedido n.º 19187/91, de 17.12.1996, pág. 19, parágrafos 68-69. No mesmo sentido, veja-se também o acórdão do TEDH *Corbet e Outros c. França*, pedidos n.º 7494/11, 7493/11 e 7989/11, de 19.3.2015, pág. 10, parágrafo 32, e, bem assim, acórdão do TEDH *Ibrahim e Outros c. Reino Unido*, processos n.º 50541/08, 50571/08, 50573/08 e 40351/09, de 13.9.2016, pág. 67, parágrafo 266.

[26] Aliás, num regime jurídico paralelo ao do RGPD – como é o caso do Regime Jurídico da Concorrência, mas com natureza exclusivamente contraordenacional –, a extensão do dever de colaboração já foi inclusivamente testado, tendo o Tribunal Constitucional concluído que: "*tal direito não [abarca], assim, a possibilidade de o arguido, em processo contra-ordenacional por práticas anticoncorrenciais, recusar a prestação de informações e a entrega de documentos, que estejam em seu poder e lhe sejam solicitados pela Autoridade da Concorrência, pressuposta a dimensão objectiva desses elementos, desprovidos de conteúdo conclusivo ou juízo valorativo, no sentido auto-incriminatório.*" Parece, por conseguinte, aceitável exigir uma colaboração em que o visado tenha de entregar documentos já previamente elaborados e guardados em arquivo físico ou digital e, bem assim, a prestar informações objetivas que lhe venham a ser solicitadas, no pressuposto, porém, de que esses documentos ou informações não tenham conteúdo conclusivo ou juízos valorativos que se possam revelar autoincriminatórios.

[27] FIGUEIREDO DIAS, Jorge de, COSTA ANDRADE, Manuel da e COSTA PINTO, Frederico de Lacerda da, "Supervisão, Direito ao Silêncio e Legalidade da Prova", *cit.*, págs. 46-47.

destaca a existência de alguns requisitos, entre eles: (i) a existência de expressa previsão legal do dever de colaboração; (ii) que a restrição vise salvaguardar outro direito ou interesse de igual ou superior peso constitucional; (iii) que seja proporcional – ou seja, necessária, adequada e proporcional em sentido estrito, nos termos do n.º 2 do art. 18.º da CRP; (iv) e que não aniquile o direito em causa atingindo o seu núcleo/conteúdo essencial, conforme preconiza o n.º 3, do art. 18.º da CRP"[28].

Ora, é quanto aos pontos associados ao princípio da proporcionalidade acima realçados que, em nosso entender, surgem as maiores dúvidas quando escalpelizado o teor do artigo 33.º do RGPD.

É que no caso concreto do artigo 33.º do RGPD, poder-se-ia eventualmente ter concebido soluções menos agressivas para gerir uma violação de dados pessoais que passariam, por exemplo, pela mera necessidade de manter um registo das situações de *data breach*, da sua extensão e das medidas implementadas e a implementar para corrigir a falha, sem que houvesse a necessidade de comunicar pró-ativamente à Autoridade de Controlo a situação de violação de dados pessoais. Se, ainda assim, se equacionasse a absoluta necessidade de reportar o *data breach* à Autoridade de Controlo para, por exemplo, prevenir a utilização ou divulgação não autorizada dos dados pessoais por terceiros, dever-se-ia, ao menos, evitar uma censura contraordenacional e sobretudo penal, dirigida ao Responsável pelo Tratamento. A comunicação obrigatória poderia assumir assim uma natureza próxima da imunidade conferida pelo regime da delação premiada[29].

De modo que a censura contraordenacional e/ou penal poderia ficar então reservada para as situações em que houvesse *data breach* e este chegasse ao conhecimento da Autoridade de Controlo em virtude de

[28] Acórdão n.º 279/2022 do Tribunal Constitucional de 15.5.2019, processo n.º 1093/2021, 1.ª secção, ponto 10, pág. 18.

[29] O regime da delação premiada está atualmente perfeitamente consolidado no nosso ordenamento jurídico por via, por exemplo, dos artigos 75.º e ss do Regime Jurídico da Concorrência, tal como previsto pela Lei n.º 19/2012, de 8 de maio, na redação dada pela Lei n.º 17/2022, de 17 de agosto.

fiscalizações ocasionais ou periódicas, como ocorre, aliás, com a Autoridade Tributária no exercício dos seus poderes de supervisão ou de inspeção no âmbito sancionatório, ou chegasse ao conhecimento da Autoridade de Controlo por via do regime geral da proteção de denunciantes de infrações[30] e, bem assim, uma censura especialmente direcionada àqueles que viessem a tratar os dados pessoais associados ao *data breach* sem que para o efeito existisse uma autorização do respetivo titular de dados.

Assim, no âmbito da presente reflexão sobre a compatibilidade do artigo 33.º do RGPD com o *nemo tenetur*, não é tanto a tutela jurídico-constitucional do *nemo tenetur* que está em causa, mas antes a sua exata extensão, conteúdo e alcance, e acima de tudo, se e quando é que tem cabimento invocar o *nemo tenetur* no âmbito de um eventual processo contraordenacional[31] que é iniciado no domínio do RGPD.

Por outras palavras, há que aferir, em primeira instância, o exato conteúdo do direito ao silêncio, do momento da sua aplicação, da subsistência parcial do dever de colaborar com as Autoridades de Controlo e da sua sujeição às diligências de prova[32].

b. O âmbito e a extensão do *nemo tenetur* no contexto do direito penal e contraordenacional

Parece ser indiscutível haver lugar para a aplicação do princípio do *nemo tenetur* no domínio do direito sancionatório, seja ele de natureza penal ou contraordenacional. O que parece variar é a intensidade com que se impõe e se afirmam as garantias asseguradas pelo *nemo tenetur* na dimensão penal por contraposição à dimensão contraordenacional.

---

[30] Tal como atualmente consagrado na Lei n.º 93/2021, de 20 de dezembro.

[31] Já que no âmbito do processo penal poucas dúvidas subsistem quanto ao cabimento alargado dos direitos associados ao *nemo tenetur*.

[32] FIGUEIREDO DIAS, Jorge de, COSTA ANDRADE, Manuel da e COSTA PINTO, Frederico de Lacerda da, "Supervisão, Direito ao Silêncio e Legalidade da Prova", *cit.*, pág. 99.

Neste sentido, refere a nossa jurisprudência: "*O direito à não auto-incriminação, nomeadamente na vertente de direito ao silêncio, tendo o seu campo de eleição no âmbito do direito criminal, estende-se a qualquer processo sancionatório de direito público. Porém, o seu conteúdo é diferenciado, consoante o domínio do direito punitivo em que se situe a sua aplicação. Ora, no âmbito contra-ordenacional – dada a diferente natureza do ilícito de mera ordenação e a sua menor ressonância ética, comparativamente com o ilícito criminal – o peso do regime garantístico é menor, conforme já defendido por este Tribunal, nomeadamente no Acórdão n.º 659/2006 (disponível no sítio da internet já referido)*" [33].

Nesta mesma linha, aliás, refere Figueiredo Dias e Costa Andrade que: "*(...) de acordo não só com a Constituição, mas também com a Convenção Europeia dos Direitos do Homem o direito ao silêncio, enquanto garantia de defesa, deve estender-se a qualquer processo onde possam ser aplicadas sanções de caráter punitivo, ainda que não criminal.*"[34]

Pode, portanto, concluir-se que o *nemo tenetur* tem inequívoca margem de aplicação nas situações censuradas pelo direito penal e contraordenacional, apesar de a sua amplitude e intensidade ser menor no direito sancionatório contraordenacional quando comparada com a sua aplicação no domínio do direito penal. De resto, como acima demos devida nota, o Estado incumbiu determinadas autoridades – entre as quais se destaca a *Comissão Nacional de Proteção de Dados* ("CNPD") –, da missão de controlar as normas relativas à proteção de dados pessoais.

Para o efeito, o legislador dotou a CNPD de uma missão de supervisão com poderes sancionatórios, com vista a detetar e censurar desvios ao padrão de comportamento coletivo tido como adequado e necessário para a sã convivência social no domínio da proteção de dados pessoais.

---

[33] Acórdão n.º 461/2011 do Tribunal Constitucional de 11.10.2011, *cit.*, parágrafo 11, pág. 12.

[34] FIGUEIREDO DIAS, Jorge de, COSTA ANDRADE, Manuel da e COSTA PINTO, Frederico de Lacerda da, "Supervisão, Direito ao Silêncio e Legalidade da Prova", *cit.*, pág. 46.

Tendo o *supra* exposto em consideração, parece de elementar bom senso que não se dotasse o visado, por exemplo, no âmbito de um procedimento contraordenacional, de um direito absoluto de não colaborar com as autoridades de supervisão, pois tal poderia equivaler à inutilidade do processo de supervisão. Isso retiraria ao supervisor os meios ao seu alcance para investigar e obter a prova que o habilitaria à tutela sancionatória. Um direito absoluto à não colaboração inibiria qualquer acesso à prova, já que tal acesso passaria a estar dependente da boa vontade do suposto infrator.

De modo que, aceitar a aplicação do princípio do *nemo tenetur* de forma absoluta, equivalente a um integral direito ao silêncio e à não cooperação total, seria dotar os visados de poderes para, com relativa facilidade, frustrar os objetivos que o legislador tinha em mente quando instituiu estas autoridades com poderes de controlo e supervisão.

Assim, como acima já aludimos, as limitações ao *nemo tenetur* têm de respeitar, entre outras coisas, o princípio da proporcionalidade. Será pela aplicação deste princípio fundamental que se encontrará, certamente, o equilíbrio entre os interesses em conflito.

c. Conteúdo e amplitude do direito ao silêncio

Para o efeito de encontrar esse equilíbrio dos interesses em confronto, afigura-se essencial atender ao conteúdo e amplitude do *nemo tenetur* no contexto europeu. E para esse propósito, há que prestar a devida atenção ao facto de o Tribunal Europeu dos Direitos do Homem ("TEDH") ter tornado claro que, embora o artigo 6.º da CEDH não mencionasse expressamente o direito ao silêncio, este constitui um direito internacionalmente reconhecido e que habita no âmago do processo equitativo. Ao proibir a coação sobre o indivíduo com o intuito de o forçar a colaborar na recolha de prova, evita-se um uso excessivo da força estatal, conduzindo a erros judiciais e por esta via, assegurando-se os propósitos ínsitos no artigo 6.º da CEDH[35].

[35] Acórdão do TJUE *DB c. Commissione Nazionale per le Società e la Borsa (Consob)*, processo C-481/19, de 2.2.2021, pág. 11, parágrafo 38.

O direito ao silêncio visa evitar, em primeira instância, que a acusação recorra a pressões abusivas para arrancar a prova contra a vontade do acusado, ou inclusive que se puna ou ameace punir o visado ou acusado por este se recusar a prestar declarações de teor autoincriminatório[36].

De salientar também que o direito ao silêncio abrange não só os factos confessados sob pressão indevida, mas também informações acessórias sobre questões de facto que possam ser posteriormente usadas pela acusação para consolidar a sua posição ou desacreditar o visado[37]. O direito ao silêncio confere, portanto, um respaldo confortável e bastante extenso à defesa a propósito da alegada conduta ilícita. Se quiséssemos transpor isto para uma escala comparativa, seriamos levados a concluir que a partilha de informação quanto aos factos incriminatórios estava mais a coberto do direito ao silêncio do que pelo dever de colaboração com as Autoridades.

Sobre o *supra* exposto importa, bem assim, recordar a jurisprudência do Tribunal de Justiça da União Europeia, quando afirma: *"Por outro lado, o órgão jurisdicional de reenvio recorda que, segundo a jurisprudência do Tribunal Europeu dos Direitos do Homem, o direito ao silêncio, que decorre do artigo 6.o da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, assinada em Roma, em 4 de novembro de 1950 (a seguir designada «CEDH»), é violado quando as pessoas são punidas pelo direito nacional por não terem respondido às perguntas das autoridades administrativas no âmbito de processos de estabelecimento de contraordenações puníveis com sanções penais (TEDH, 3 de maio de 2001, J. B. c. Suíça, CE:ECHR:2001:0503JUD003182796, §§ 63 a 71; 4 de outubro de 2005, Shannon c. Reino Unido, CE:ECHR:2005:1004JUD000656303, §§ 38 a 41, e 5 de abril de 2012, Chambaz c. Suíça, CE:ECHR:2012:0405JUD001166304, §§ 50 a 58).*[38]*"*

---

[36] Acórdão do TJUE *DB*, processo C-481/19, *cit.*, pág. 11, parágrafo 39.
[37] Acórdão do TJUE *DB*, processo C-481/19, *cit.*, pág. 11, parágrafo 40.
[38] Acórdão do TJUE *DB*, processo C-481/19, *cit.*, pág. 8, parágrafo 22.

Ora, nesta passagem salta à vista a expressão: "*processos (...) de contraordenação puníveis com sanções penais*". E este tema merece um olhar atento em momento subsequente.

Sem embargo e antes mesmo de aferir o que se entende por "processo contraordenacional com sanções penais", importa ter presente que "*Depoimentos obtidos sob coação, que no seu valor facial aparentem não ter natureza incriminatória, como declarações de exclusão da ilicitude ou mera informação relativas a matéria de facto – podem ser posteriormente utilizadas em processos de natureza criminal para suportar uma acusação, como por exemplo, para contrariar ou suscitar dúvidas sobre outras declarações do Arguido ou prova aportada por este durante um julgamento ou de outro modo abalar a sua credibilidade*"[39].

De modo que, em síntese, de acordo com o TEDH, secundado pelo TJUE, o direito à não autoincriminação encontra-se associado ao direito ao silêncio e ao direito de não contribuir para a sua acusação. Trata-se de um direito abrangente, em cuja margem de compressão é limitada, sob pena de violar o artigo 6.º da CEDH e de beliscar o conceito de processo equitativo.

Parte-se, deste modo, de um princípio geral de que a acusação deve provar a sua posição sem coagir o visado a cooperar para a sua própria incriminação.

Por outro lado, para Joana Costa, o *nemo tenetur*, à luz da jurisprudência do TEDH, é um princípio cujos contornos precisos devem ser aferidos caso a caso, e não podem nem devem ser definidos em abstrato. Como refere esta autora: "*a compreensão do princípio nemo tenetur, em especial a determinação do seu conteúdo, alcance e extensão por subordinar-se aí à ideia segundo a qual a figura do processo equitativo – e consequentemente, os vários elementos que expressa ou implicitamente a integram – não pode definir-se em abstrato, antes*

[39] Acórdão do TEDH *Saunders c. Reino Unido*, *cit.*, pág. 20, parágrafo 71. Veja-se também o acórdão do TEDH *Ibrahim e Outros c. Reino Unido*, *cit.*, pág. 68, parágrafo 268.

devendo ser verificada segundo as circunstâncias particulares do caso concreto, tomando em consideração o processo no seu conjunto"[40].

d. Conceito de "infração criminal" segundo a jurisprudência dos Tribunais Europeus, para efeitos de aplicação do *nemo tenetur*

Ora, nesta sede, com vista a escalpelizar o conceito acima mencionado de "processos de contraordenação puníveis com sanções penais", importa, antes de mais, atender ao conceito de "infração criminal", tal qual tem sido tratada pela jurisprudência do Tribunais Europeus (*i.e.* TEDH e TJUE). E a este respeito, há que referir que o conceito de "ofensa criminal" ou "infração criminal", tal como estabelecido pelo TEDH, para efeitos de aplicação do *nemo tenetur*, tem as suas especificidades.

Como o exposto acima já parecia indiciar, o conceito de "ofensa criminal" ou "infração criminal" não é necessariamente coincidente ao que existe nos ordenamentos jurídicos nacionais dos diferentes Estados-membros da União Europeia.

Com efeito, na linha do que estabelece a jurisprudência europeia: "*[o] Tribunal reitera a sua jurisprudência sedimentada quanto à determinação da existência de uma "infração criminal", onde se afigura necessário aferir três fatores: a qualificação jurídica da medida em questão de acordo com a ordenamento jurídico nacional; a própria natureza da medida; e a natureza e o grau de gravidade da "sanção" aplicada (veja-se Engel e Outros c. Países Baixos, 8 junho 1976, § 82, Series A no. 22). Para além disso, estes critérios são alternativos e não cumulativos: para efeitos de aplicação do Artigo 6 a respeito do conceito "infração criminal", basta que a ofensa em questão seja, pela sua própria natureza, "criminal" de um ponto de vista da Convenção, ou tenha feito a pessoa em causa responsável por uma sanção a qual, em*

[40] COSTA, Joana, "O princípio *nemo tenetur* na Jurisprudência do Tribunal Europeu dos Direitos do Homem", *in Revista do Ministério Público 128*, outubro – dezembro 2011, página 3.

virtude da sua natureza e o grau de gravidade, pertença em geral a uma esfera "criminal". Isto, contudo, não exclui uma abordagem cumulativa quando uma análise separada de cada critério não permite alcançar uma conclusão clara quanto à existência de uma "infração criminal" (veja-se Jussila c. Finlândia [GC], no. 73053/01, §§ 30 e 31, TEDH 2006-XIII, e Zaicevs c. Latvia, no. 65022/01, § 31, TEDH 2007-IX (extratos))"[41].

Parece decorrer desta jurisprudência que, segundo a CEDH o conceito de "ofensa criminal" ou "infração criminal" pode não estar circunscrito às situações em que existe uma sanção que estatui a privação da liberdade. Em bom rigor, para o TEDH e para o TJUE, "ofensa criminal" ou "infração criminal" parece corresponder a um conceito vago e indeterminado que deve ser concretizado com recurso a um teste com três vetores alternativos (e não necessariamente cumulativos).

E segundo a jurisprudência do TEDH, no que se refere ao primeiro critério, um procedimento de cariz administrativo no âmbito nacional também pode prever uma ofensa ou infração criminal para efeitos da CEDH[42].

Por seu turno, segundo a mesma jurisprudência: *"[n]o que se refere ao segundo critério, relativo à própria natureza da infração, este implica verificar se a sanção em causa prossegue, nomeadamente, uma finalidade repressiva (...). Daqui decorre que uma sanção com finalidade repressiva tem natureza penal na aceção do artigo 50.o da Carta e que a simples circunstância de prosseguir também uma finalidade preventiva não é suscetível de lhe retirar a sua qualificação de sanção penal. (...) Em contrapartida, uma medida que se limita a reparar o prejuízo causado pela infração em causa não tem natureza penal.*[43] *"*

---

[41] Acórdão do TEDH *Grande Stevens c. Itália*, pedido n.º 18640/10, de 4.3.2014, pág. 14, parágrafo 94 e acórdão do TJUE *Łukasz Marcin Bonda,* processo C-489/10, de 5.7.2012, pág. 9, parágrafos 37-39, e, bem assim, o acórdão do TJUE *Garlsson Real Estate SA e Outros c. Commissione Nazionale per le Società e la Borsa (Consob)*, processo C-537/16, de 20.3.2018, pág. 7, parágrafo 28.

[42] Acórdão do TJUE *Consob*, processo C-537/16, *cit.*, pág. 7, parágrafo 31.

[43] Acórdão do TJUE *Consob*, processo C-537/16, *cit.*, pág. 7, parágrafo 33.

E por fim, na linha da referida jurisprudência: *"[n]o que diz respeito ao terceiro critério, há que salientar que uma sanção administrativa pecuniária que pode atingir um montante até dez vezes o produto ou a mais valia obtida com a manipulação de mercado apresenta um nível de severidade elevado que é suscetível de reforçar a análise de que esta sanção tem natureza penal na aceção do artigo 50.o da Carta, o que cabe, contudo, ao órgão jurisdicional de reenvio verificar.*[44] *"*

Com efeito, daqui se depreende que existem três critérios para aferir se estamos efetivamente perante um procedimento que pode ser na sua face de cariz administrativo, mas que comporta, na verdade, uma sanção penal, para efeitos da aplicação do *nemo tenetur* e do correspondente direito ao silêncio.

Esses três critérios, *grosso modo*, são: i) a qualificação atribuída à natureza do procedimento no ordenamento jurídico nacional; ii) se a sanção aplicável tem natureza repressiva (ou se, ao invés, tem um mero carácter preventivo); e iii) o grau de severidade da sanção, sendo que sanções cujo intuito consiste simplesmente em compensar o dano gerado pela ilicitude não preenchem o critério da severidade, ao contrário das sanções que também comportam um certo teor punitivo em virtude da conduta.

Face ao *supra* exposto, apesar de os contornos específicos do *nemo tenetur* carecerem de uma aferição casuística, tudo aponta para que a aplicação concreta do artigo 33.º do RGPD, seja por via contraordenacional, seja por via do procedimento penal, abrirá naturalmente a porta para o preenchimento do conceito de "infração criminal", nos termos e para os efeitos da jurisprudência do TEDH e do TJUE. É que o ponto i) vê-se claramente preenchido pelos n.ºs 1 e 2 do artigo 8.º da Lei de Execução do RGPD, em articulação com os artigos 46.º a 49.º da referida Lei de Execução.

Mas para além disso, os pontos ii) e iii) *supra* também se encontram preenchidos pela alínea a) do n.º 4 do artigo 83.º do RGPD em articulação com o artigo 33.º do RGPD.

---

[44] Acórdão do TJUE *Consob*, processo C-537/16, *cit.*, pág. 7, parágrafo 35.

e. O direito ao silêncio e a natureza penal das sanções de acordo com o TEDH

Por esta altura, parece indiscutível que o direito ao silêncio se aplica com ampla abrangência e vigor aos processos de natureza criminal. A dúvida reside somente em saber se os processos de natureza administrativa de âmbito contraordenacional, em que estejam preenchidos só um, dois ou até os três fatores do conceito de "ofensa criminal" ou "infração criminal", tal como definido pelo TEDH, também podem estar abrangidos pela aplicação plena do *nemo tenetur*, em modos idênticos aos admitidos no processo penal. E quanto a esta matéria, é importante atender à jurisprudência do TJUE quando afirma: *"[q]uanto à questão de saber em que condições deve o referido direito ser igualmente respeitado no âmbito de processos de contraordenação, importa sublinhar que este mesmo direito é aplicável no contexto de procedimentos suscetíveis de conduzir à aplicação de sanções administrativas de natureza penal."* E a respeito deste ponto, o TJUE volta a reiterar o teste acima referido no acórdão *Consob*, ao afirmar: *"são pertinentes três critérios para apreciar a referida natureza. O primeiro é a qualificação jurídica da infração no direito interno, o segundo diz respeito à própria natureza da infração e o terceiro é relativo ao grau de severidade da sanção suscetível de ser aplicada ao interessado (Acórdão de 20 de março de 2018, Garlsson Real Estate e o., C537/16, EU:C:2018:193, n.o 28).*[45] *"*

E como também estabelece o TJUE no acórdão *DB*: *"[e]mbora caiba ao órgão jurisdicional de reenvio apreciar, à luz destes critérios, se as sanções administrativas em causa no processo principal têm natureza penal, esse órgão jurisdicional recorda, todavia, com razão, que, segundo a jurisprudência do Tribunal de Justiça, algumas das sanções administrativas aplicadas pela Consob parecem prosseguir uma finalidade repressiva e apresentar um grau de severidade elevado que é*

[45] Acórdão do TJUE *DB*, processo C-481/19, *cit.*, pág. 11, parágrafo 42.

suscetível de reforçar a análise de que esta sanção tem natureza penal (...). O Tribunal Europeu dos Direitos do Homem chegou, em substância, à mesma conclusão (TEDH, 4 de março de 2014, Grande Stevens e outros c. Itália, CE:ECHR:2014:0304JUD001864010, § 101). [46] *"*

Ora, o que acima já antecipávamos parece ter reflexo na jurisprudência do TJUE. Processos contraordenacionais que contemplam sanções financeiras como coimas, mas cuja finalidade é repressiva e em cujas sanções tenham um grau de severidade elevado, são suscetíveis de serem qualificados como tendo "natureza penal" para efeitos da CEDH, ao ponto de os visados se poderem socorrer do *nemo tenetur* em toda a sua amplitude e vigor, como se estivessem em causa processos de natureza penal.

Ora, o paralelo com o RGPD afigura-se evidente. Também neste quadro jurídico as coimas parecem prosseguir finalidades repressivas e um grau de severidade tal que reforça a natureza penal das sanções ali previstas à luz do TEDH[47].

Refere ainda a jurisprudência do TJUE a este respeito: *"(...) mesmo admitindo que, no processo em apreço, as sanções aplicadas a DB pela autoridade de supervisão em causa no processo principal não tinham natureza penal, a necessidade de respeitar o direito ao silêncio no âmbito de um processo de investigação levado a cabo por esta poderia igualmente resultar da circunstância, salientada pelo órgão jurisdicional de reenvio, de, em conformidade com a legislação nacional, os elementos de prova obtidos no âmbito desse processo poderem ser utilizados, no âmbito de um processo penal instaurado contra essa mesma pessoa, para demonstrar a prática de um ilícito penal.* [48] *"*

Uma vez mais, o *supra* exposto parece encaixar como uma luva no regime jurídico de proteção de dados português, já que a prova recolhida pelo *data breach* pode dar origem a sanções de natureza

---

[46] Acórdão do TJUE *DB*, processo C-481/19, *cit.*, págs. 11-12, parágrafo 43.

[47] O mesmo parece suceder com o regime jurídico da concorrência, com coimas que podem ascender aos 10% dos volumes de negócio mundial.

[48] Acórdão do TJUE *DB*, processo C-481/19, *cit.*, pág. 12, parágrafo 44.

contraordenacional e penal. De modo que, nesta sede, o *nemo tenetur* e o correspondente direito ao silêncio adquire pleno vigor.

Precisamente no contexto do acórdão acima citado, o TJUE foi levado a concluir que não podia ser imposta à empresa uma obrigação de dar respostas através das quais fosse levada a admitir a existência de uma infração[49].

Idêntico paralelo se deve estabelecer quando se olha para o RGPD e a sua respetiva Lei de Execução.

De modo que, perante todo o exposto, o dever de notificar um *data breach* às Autoridades de Controlo afigura-se incompatível com o *nemo tenetur*, precisamente devido ao carácter de natureza penal das sanções previstas tanto no RGPD, como na sua Lei de Execução. As obrigações constantes do artigo 33.º do RGPD aparentam ser ilegais e violadoras dos mais elementares princípios associados ao direito ao silêncio.

IV. CONCLUSÃO

Aqui chegados, importa, portanto, salientar, que existem direitos fundamentais típicos dos indivíduos singulares[50] e outros cuja extensão seria perfeitamente aceitável às pessoas coletivas. O *nemo tenetur*, enquanto direito fundamental, estendem-se às pessoas coletivas, nos termos e para os efeitos do n.º 2 do artigo 12.º da CRP.

Parte da doutrina defende, contudo, que o exercício dos direitos fundamentais pode sofrer alterações quando invocado por pessoas coletivas[51].

No que toca à imposição legal de notificar uma violação de dados pessoais à Autoridade de Controlo, tal como prescreve o artigo 33.º do RGPD, em nossa opinião, a obrigação representa um retrocesso nos direitos e garantias dos visados, fazendo renascer a marca outrora expurgada do nosso ordenamento jurídico e que estava associada ao processo

[49] Acórdão do TJUE *DB*, processo C-481/19, *cit.*, pág. 12, parágrafo 47.

[50] Como seria o caso da liberdade sexual.

[51] MIRANDA, Jorge e MEDEIROS, Rui, *Constituição Portuguesa Anotada*, tomo I, Coimbra Editora, 2005, pág. 113.

de natureza inquisitória. Nessa altura, existiam confissões forçadas, convertendo os visados em sujeitos da sua própria condenação. De modo que a presente obrigação configura um desrespeito pela essência do *nemo tenetur*, precisamente por ser excessiva a forma como se exige a colaboração com a entidade supervisora.

Face a tudo o que se expos, parece inquestionável que o dever que impende sobre o Responsável pelo Tratamento de alertar a Autoridade de Controlo para uma violação de dados pessoais padece irremediavelmente de uma violação do *nemo tenetur* no contexto da infração penal.

Nesta matéria, o Responsável pelo Tratamento goza de um direito ao silêncio, que lhe permite eximir-se de auxiliar a supervisão ao alertar para o *data breach* e fornecer dados que favorecem a sua autoincriminação. Tratar-se-ia de aplicar raciocínio analógico ao aplicado à testemunha quando confrontada com questões que geram a sua responsabilidade penal. Neste contexto, Augusto Silva Dias e Vânia Costa Ramos elucidam-nos do seguinte modo: "*segundo o CPP, a testemunha deve prestar juramento e deve responder com verdade às perguntas que lhe forem feitas, salvo se das respostas resultar a possibilidade da sua responsabilização penal (art. 132.º, n.º 2). Sempre que isto aconteça a testemunha pode remeter-se ao silêncio e, querendo, requerer a sua constituição como arguido. Deste modo se evita que um suspeito seja chamado a depor como testemunha e, por estar vinculado ao dever de verdade, seja obrigado a declarar contra si próprio e a auto-incriminar-se. Resulta daqui que no sistema processual penal português é titular do direito ao silêncio primeiramente o arguido e, além dele, todas as pessoas que, não o sendo, são, contudo, orientadas ou pressionadas por agentes da administração da justiça penal a declararem contra si mesmas.*"[52]

---

[52] SILVA DIAS, Augusto e COSTA RAMOS, Vânia, *O Direito À Não Auto-Inculpação (Nemo Tenetur Se Ipsum Accusare) No Processo Penal e Contra-Ordenacional Português*, *cit.*, pág. 20. Esta parece ser também a conclusão que se permite tirar quando analisadas as posições adotadas por outra doutrina autorizada. *Vide*, por exemplo, COSTA ANDRADE, Manuel da, *Sobre as Proibições de Prova*, *cit.*, pág. 121 e OLIVEIRA E SILVA, Sandra, *O Arguido como Meio de Prova Contra Si Mesmo – considerações em torno do princípio Nemo Tenetur Se Ipsum Accusare*, *cit.*, pág. 389.

Já no que diz respeito ao processo contraordenacional, ou bem que se conclui pela não aplicabilidade *tout cour* do *nemo tenetur* ao processo contraordenacional – algo que evidentemente acreditamos ser contrário à jurisprudência do TEDH e do TJUE –, ou temos de aceitar que a colaboração com a Autoridade de Controlo tem os seus limites.

Assumir uma necessidade de colaboração plena, significaria circunscrever o *nemo tenetur* a uma fase subsequente da instrução do processo sancionatório[53] e isso equivaleria a desconsiderar que o resultado dessa colaboração (forçada!) constaria para sempre dos autos. Mais tarde, tal prova constante dos autos, serviria em fase instrutória e eventualmente em fase de julgamento para prejudicar o arguido. De modo que guardar a aplicabilidade do *nemo tenetur* para momento posterior, de pouco ou nada valerá.

Assim, a nosso ver, por via do artigo 33.º do RGPD, a Autoridade Supervisora delega *ope legis* no Responsável pelo Tratamento parte do seu trabalho de investigação, coagindo o visado a dar toda a prova que dispõe da violação de dados pessoais e das consequências previsíveis que tal violação acarreta. E isto parece-nos inaceitável.

Outra seria a solução se o artigo 33.º do RGPD estabelecesse que o Responsável pelo Tratamento não sendo obrigado a dar nota da existência de uma violação de dados pessoais, o pudesse fazer, com a advertência de que esses elementos podiam ser usados contra si em processo penal ou contraordenacional, mas que tal cooperação poderia ser valorada positivamente no momento de fixar uma pena ou uma coima,

---

[53] Esta parece ser a posição adotada por COSTA PINTO, Frederico da, em "*Supervisão, Direito ao Silêncio e Legalidade da Prova*", *cit.*, pág. 102, quando afirmou, a propósito dos dever de colaboração expresso no Código dos Valores Mobiliários que: "*o problema analisado tem uma resposta linear: ou bem que estamos perante actos de supervisão e então não há que invocar o estatuto do arguido e o direito ao silêncio porque não há processo de contra-ordenação; ou, diversamente, estamos perante um processo de contra-ordenação e os actos praticados pela autoridade de supervisão traduzem-se em diligências de obtenção de provas e, em relação a estas, o arguido não tem o direito ao silêncio, mas sim o dever de se sujeitar às diligências em causa, como resulta dos artigos 60.º e 61.º, n.º 3 al. d), do CPP. A conclusão, em qualquer um dos casos, é a mesma: ou não há direito ao silêncio porque não há arguido ou não há direito ao silêncio porque o arguido tem o dever legal de se sujeitar à[s] diligências de obtenção de prova.*"

servindo esta colaboração como circunstância atenuante a seu favor. Também nesta sede, como acima demos nota, poderia funcionar o regime da delação premiada. Neste contexto, a cooperação assumiria mais a veste de um convite do que uma imposição a cooperar.

De modo que, a nosso ver, uma coisa seria exigir do visado, no âmbito da supervisão, um dever de colaboração no sentido de esclarecer factos e facultar documentos e/ou o acesso a locais onde esses documentos ou prova podem estar armazenados e que seriam do conhecimento da Autoridade de Controlo, outra coisa bem diversa é impor ao visado o anúncio da eventual existência de um ilícito passando este a ser alvo da investigação.

É preciso ter presente que uma vez avisada a Autoridade de Controlo da existência de uma violação de dados pessoais – porque o Responsável pelo Tratamento é coagido a fazê-lo, nos termos e para os efeitos do artigo 33.º do RGPD –, compete ao Responsável pelo Tratamento facultar um conjunto alargado de informações, no âmbito dos seus deveres de colaboração com a supervisão, elementos que poderão e muitas da vezes serão usados contra si como prova para instruir um procedimento sancionatório de natureza contraordenacional e/ou penal[54]. Com a solução encontrada no artigo 33.º do RGPD, o legislador instrumentalizou o Responsável pelo Tratamento para denunciar e instruir um processo sancionatório contra si mesmo. Ora, isso, em nossa opinião, atenta contra o âmago do *nemo tenetur*[55].

Se esta ideia é grave num procedimento de natureza contraordenacional[56], afigura-se totalmente inaceitável num

---

[54] Não se afigura profícuo nesta sede explorar a questão controversa de saber se pode haver uma censura penal e simultaneamente contraordenacional pelo mesmo facto, ou, se ao invés, a matéria criminal consome a possibilidade de o arguido vir a ser sujeito de um processo contraordenacional. Limitamo-nos, neste contexto, a dar nota desta relevante e interessante questão.

[55] Esta linha parece inclusive ser a posição da mais autorizada doutrina nacional, que conta com OLIVEIRA E SILVA, Sandra, *O Arguido como Meio de Prova Contra Si Mesmo – considerações em torno do princípio Nemo Tenetur Se Ipsum Accusare*, *cit.*, págs. 827-828.

[56] Onde lidamos com um direito sancionatório de natureza administrativa, axiologicamente neutro, destinado a prevenir e reprimir normas de conduta dirigidos à sã convivência económica e social da coletividade.

procedimento de natureza penal, que pode culminar com a aplicação de uma pena privativa da liberdade.

Aqui, em nosso entender, vai-se muito além do simples dever de colaboração, para uma exigência de autoinculpação.

Aceitar a solução consagrada no artigo 33.º do RGPD como lícita, seria negar por absoluto o *nemo tenetur*, colocando os visados/arguidos a substituir-se ao Estado nas suas funções de fiscalização destinadas a identificar as situações de lesão ao ordenamento jurídico, em violação do princípio da proporcionalidade constitucionalmente tutelado.

a. Nulidade da prova obtida mediante a violação do *nemo tenetur*

Uma vez que o artigo 33.º do RGPD se encontra em pleno vigor, o que sucede então nas situações em que existe prova nos autos recolhida ao abrigo desta norma?

Ora, parece ser inquestionável que a doutrina portuguesa pende para a opinião de que a violação do princípio do *nemo tenetur* tem como consequência a proibição da valoração da prova[57].

Na linha do ensinamento de Augusto Silva Dias e Vânia Costa Ramos: "*se o meio de prova, independentemente de qual seja, tiver sido obtido (...) através de coação ou de ameaça com medida legalmente inadmissível, estipulam os n.ºs 1 e 2, als. a) e d), do art. 126.º do CPP que a prova é nula e não pode ser utilizada. (...) Em qualquer dos casos, a prova não pode ser valorada e utilizada no processo, cominação que traduz a existência de uma nulidade particularmente grave e insanável. Segundo o entendimento dominante na doutrina portuguesa, tributário em certa medida da célebre teoria dos «frutos da árvore envenenada», esta consequência jurídica projeta-se à distância, estendendo-se às provas secundárias, isto é, às provas recolhidas a*

[57] COSTA ANDRADE, Manuel da, *Sobre as Proibições de Prova em Processo Penal*, Gestlegal, 2022, págs. 126 e ss e OLIVEIRA E SILVA, Sandra, *O Arguido como Meio de Prova Contra Si Mesmo – considerações em torno do princípio Nemo Tenetur Se Ipsum Accusare*, *cit.*, pág. 364.

partir das declarações, dos documentos ou dos exames sobre o corpo do suspeito ou do arguido alcançados por métodos proibidos."[58]

Como também afirmam Figueiredo Dias e Costa Andrade: "*no processo penal português vigora o regime da legalidade da prova: são admissíveis as provas que não forem proibidas por lei (artigo 125.º do CPP). A legalidade dos meios de prova, bem como as regras gerais de produção de prova e as chamadas "proibições de prova" são condições de validade processual da prova e, por isso mesmo, critérios da própria verdade material*"[59]. De modo que, para os autores, "*são nulas, não podendo ser utilizadas, as provas obtidas mediante ofensa da integridade moral das pessoas, designadamente quando obtidas mediante perturbação da liberdade de vontade*"[60]. Naturalmente que a prova nula não poderá ser tomada em consideração para condenar o visado pela putativa prática ilícita. E como afirma Frederico da Costa Pinto: "*o princípio da legalidade, que vigora em todo o Direito sancionatório público, incluindo no domínio das contra-ordenações (artigos 2.º e 43.º do RGCords), visa garantir não só os direitos dos arguidos, mas também a confiança na previsibilidade da aplicação do Direito e, em especial, procura preservar o conteúdo e a eficácia da decisão legislativa.*"[61]

O que aqui se afirma está, inclusive, em sintonia com o estabelecido na nossa jurisprudência, que prescreve: *«[O] arguido não pode ser fraudulentamente induzido ou coagido a contribuir para a sua condenação, a carrear ou oferecer meios de prova contra a sua defesa»; pelo contrário, é necessário garantir que «qualquer contributo do arguido, que resulte em desfavor da sua posição, seja uma afirmação esclarecida e livre de autorresponsabilidade» (v. idem, ibidem, p. 121). O princípio do nemo tenetur visa, pois, assegurar a autodeterminação do arguido na condução da sua defesa no processo e, nessa medida, a*

---

[58] SILVA DIAS, Augusto e COSTA RAMOS, Vânia, *O Direito À Não Auto-Inculpação (Nemo Tenetur Se Ipsum Accusare) No Processo Penal e Contra-Ordenacional Português*, *cit.*, pág. 37.

[59] FIGUEIREDO DIAS, Jorge de, COSTA ANDRADE, Manuel da e COSTA PINTO, Frederico de Lacerda da, "Supervisão, Direito ao Silêncio e Legalidade da Prova", *cit.*, pág. 29.

[60] *Ibidem*, pág. 28.

[61] *Ibidem,* pág. 100.

garantia da sua posição enquanto sujeito processual. O respetivo conteúdo material é depois assegurado mediante a imposição de deveres de esclarecimento ou de advertência e pela nulidade das provas proibidas em virtude de terem sido obtidas mediante a colaboração involuntária do arguido em consequência do uso ilegítimo de meios coercivos ou de meios enganosos. É de acordo com esta teleologia que o âmbito de proteção daquele princípio deve ser determinado, seja quanto aos modos de colaboração forçada e seus limites, seja quanto ao momento a partir do qual aquela garantia se torna operante".[62]

Face ao contexto acima exposto, tudo parece sugerir que a prova obtida ao abrigo das exigências expostas pelo artigo 33.º do RGPD, são nulas em processo penal por violação do artigo 125.º e 126.º do CPP, mas também, muito provavelmente, no âmbito contraordenacional por via da aplicação conjugada do artigo 41.º do RGCO, do artigo 126.º do CPP e dos n.ºs 8 e 10 do artigo 32.º da CRP.

[62] Acórdão n.º 298/2019 do Tribunal Constitucional de 15.5.2019, processo n.º 1043/17, 2.ª secção, ponto 10, pág. 10.

Os fundamentos de licitude aplicados nas relações laborais à luz do Regulamento Geral sobre a Proteção de Dados

Patrícia Batista Santos[1]

Resumo: A área de Recursos Humanos de entidades públicas e privadas trata um volume elevado de dados pessoais de candidatos a emprego e trabalhadores no âmbito das relações laborais. Os dados tratados ao longo do ciclo de vida do contrato de trabalho encontram-se distribuídos em duas categorias distintas – as categorias "gerais" e especiais de dados pessoais. Devido ao facto desta categorização conter dados de caracter sensível, é necessário compreender quais são os fundamentos de licitude aplicados, na prática, e analisar a aplicação cumulativa do art. 6.º e 9.º do RGPD, quando estamos perante o tratamento de categorias especiais de dados.

Palavras-chave: Regulamento Geral sobre a Proteção de Dados; Relações laborais; Dados pessoais; Categorias especiais de dados.

Abstract: The Human Resources department of public and private entities handles a high volume of personal data of job applicants and workers within the scope of work relations. The personal data processed throughout the life cycle of the employment contract falls into two

[1] Técnica de Privacidade na AdvanceCare. Investigadora do NOVA Compliance Lab e Observatório da Proteção de Dados Pessoais da NOVA School of Law. Pós-Graduada em Direito da Proteção de Dados Pessoais pelo Centro de Investigação de Direito Privado da Faculdade de Direito da Universidade de Lisboa. Mestre em Direito e Gestão na especialidade de Proteção de Dados Pessoais pela NOVA School of Law. Licenciada em Gestão de Recursos Humanos pelo Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa. O presente texto foi desenvolvido no âmbito do trabalho final de avaliação do III Curso de Pós-graduação Avançada em Direito da Proteção de Dados do Centro Investigação de Direito Privado da Faculdade de Direito da Universidade de Lisboa.

distinct categories – general and special categories of personal data. Due to that this categorization contains sensitive personal data it's necessary to understand what the legal basis are applied, in practice, and to analyze the cumulative application of Article 6 and 9 of the GDPR when are dealing with special categories of data.

Keywords: General Data Protection Regulation; Work relations; Personal data; Special categories of data.

Introdução

Quando estamos perante uma oportunidade de emprego, não compreendemos a magnitude do processo no que toca à recolha e tratamento de dados pessoais que são efetuados durante o mesmo, desde a fase inicial – a submissão do *Curriculum Vitae* (CV) para efeitos de recrutamento e seleção –, a uma fase subsequente – a execução contratual – e, posteriormente, a cessação do contrato de trabalho.

Estas fases constituem o ciclo de vida do contrato de trabalho, ciclo esse que traduz um volume considerável de dados pessoais que são alvo de tratamento por parte do responsável pelo tratamento – as empresas –, sendo a área de Recursos Humanos a responsável por tratar os dados pessoais de candidatos a emprego e trabalhadores durante todo o processo.

No entanto, com as alterações verificadas no mercado de trabalho com a introdução de novas tecnologias que conduziram a novas modalidades de recrutamento e de trabalho – recrutamento online e teletrabalho, por exemplo – também trouxeram alguns riscos para o candidato a emprego e trabalhador que não se verificavam anteriormente, sobretudo no que toca à privacidade e à proteção de dados pessoais. O Regulamento Geral sobre a Proteção de Dados (RGPD) veio devolver aos titulares o controlo sobre os seus dados (considerando 7 do RGPD), em consequência dos desafios impostos pela rápida evolução

tecnológica e da globalização que conduziram à recolha e partilha de dados pessoais, em grande escala, por parte das entidades públicas e privadas (considerando 6 do RGPD).

O RGPD também veio alterar o paradigma regulatório[2] através da atribuição de responsabilidades ao responsável pelo tratamento com a implementação de regras e procedimentos mais centrados nas atividades de tratamento que podem resultar em um elevado risco para os direitos e liberdades das pessoas singulares devido à sua natureza, âmbito, contexto e finalidades (considerando 89 do RGPD).

No âmbito das relações laborais, em que é tratado um elevado volume de dados pessoais de candidatos a emprego e trabalhadores, existe a necessidade de compreender quais são as bases legais para que o tratamento dos dados seja lícito, por envolver categorias "gerais" e especiais de dados, distribuídos por diferentes finalidades de tratamento, em cada um dos momentos do ciclo de vida do contrato de trabalho.

O presente trabalho tem por objetivo compreender quais são os fundamentos de licitude aplicados ao tratamento de dados pessoais de candidatos a emprego e trabalhadores no âmbito da relação laboral, por se tratar de duas categorias distintas de dados pessoais, que necessitam de ser discutidas por não existir um consenso quando à aplicação dos fundamentos de licitude previstos no art. 6.º e no n.º 2 do art. 9.º do RGPD, sobretudo nas situações em que está em causa o tratamento de categorias especiais de dados.

Deste modo, o presente trabalho encontra-se dividido em três partes: (i) um breve enquadramento de forma a compreender a evolução histórica do direito à proteção de dados; (ii) a proteção de dados pessoais nas relações laborais, em que iremos nos debruçar sobre a legislação laboral, e o tratamento de dados efetuado nas diferentes fases

[2] A Diretiva 95/46/CE estabelecia a obrigação geral de notificação do tratamento de dados pessoais às autoridades de controlo, por parte das empresas. Consequentemente, esta obrigação originava encargos administrativos e financeiros que, nem sempre contribuíam para a melhoria da proteção dos dados pessoais, conduzindo a esta alteração estrutural com a aplicação do RGPD (considerando 89 do RGPD).

do ciclo de vida do contrato de trabalho e, por fim; (iii) os fundamentos de licitude aplicados neste contexto, destacando o afastamento do consentimento como fundamento de licitude válido nas relações laborais, e abrir a discussão em torno da aplicação cumulativa do art. 6.º e do n.º 2 do art. 9.º do RGPD quando estamos perante o tratamento de categorias especiais de dados.

1. Evolução Histórica do Direito à Proteção de Dados

1.1 Breve enquadramento

O Direito à Proteção de Dados não é um direito novo[3], mas assumiu uma enorme relevância no panorama europeu a partir dos anos 50. A consagração dos direitos humanos através da Declaração Universal dos Direitos Humanos (DUDH) veio salvaguardar as liberdades e garantias inerentes à dignidade da pessoa humana, como o direito à privacidade e à reserva da intimidade da vida privada (art. 12.º da DUDH) [4]. O mesmo sucedeu com a aprovação da Convenção Europeia dos Direitos do Homem (CEDH) que manifestava a preocupação relativamente à intrusão do Estado na esfera privada do individuo (art. 8.º da CEDH)[5].

A partir dos anos 70, foram surgindo diversos instrumentos legislativos, a nível europeu e nacional – em diferentes Estados-Membros da União Europeia (UE) – que regulam o Direito à Proteção de Dados.

O primeiro desses instrumentos, remete para o ano 1970, em foi publicada a primeira lei de proteção de dados pessoais, no Estado de Hesse, na Alemanha, conhecida como *Hessisches Datenschutzgeset*

---

[3] CORDEIRO, A. Barreto Menezes – *Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019*. Coimbra: Edições Almedina, 2020, p. 29.

[4] ALVES, Lurdes Dias – *Proteção de Dados no Contexto Laboral*. Coimbra: Edições Almedina, 2020, p. 13.

[5] *Idem*, p. 14.

(HDSG)[6], que em 1977 foi aprovada como Lei Federal de Proteção de Dados – *Bundesdastenschutzgesetz* (BDSG)[7].

Outro instrumento legislativo publicado na mesma década, remete para a ordem jurídica portuguesa, que em 1976, com a aprovação da Constituição da República Portuguesa (CRP), consagrou o reconhecimento do direito à reserva da intimidade da vida privada e familiar (n.º 1 do art. 26.º da CRP), bem como o direito de acesso aos dados informatizados que lhe digam respeito, podendo exigir a retificação e atualização dos mesmos e o direito a conhecer a finalidade a que estes se destinam (n.º 1 do art. 35.º da CRP).

No quadro europeu, em 1981, foi conhecido o primeiro instrumento internacional juridicamente vinculativo, no âmbito da proteção de dados, que surgiu através da adoção da Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro[8].

No entanto, a necessidade de harmonizar as leis nacionais de proteção de dados, dos diferentes Estados-Membros, que já se encontravam em vigor, conduziu ao surgimento da Diretiva 95/46/CE e do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, que vinha garantir um nível de proteção equivalente em todos os Estados-Membros, relativamente ao tratamento de dados pessoais[9].

---

[6] CORDEIRO, A. Barreto Menezes – *Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019*. Coimbra: Edições Almedina, 2020, p. 64.

[7] Nos anos seguintes após a publicação do HDSG, os Estados alemães vinham a publicar diplomas semelhantes. Neste sentido, com o intuito de elaborar um diploma aplicável a todo o território alemão, foi publicado, após vários anos de negociações o BDSG, que entrou em vigor no dia 1 de janeiro de 1978 (Cfr. CORDEIRO, A. Barreto Menezes – *Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019*. Coimbra: Edições Almedina, 2020, p. 64 – 65).

[8] AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA, CONSELHO DA EUROPA – *Manual da Legislação Europeia sobre a Proteção de Dados.* Luxemburgo: Serviço das Publicações da União Europeia, 2014, p. 16.

[9] *Idem*, p. 4.

Em 2009, a entrada em vigor do Tratado de Lisboa, veio reformar o regime jurídico da proteção de dados na UE ao introduzir as suas bases legais[10], no art. 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE) e nos arts. 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE)[11].

A UE iniciou a reforma da legislação de proteção de dados, devido ao rápido avanço das tecnologias e da globalização que alteraram profundamente a nossa sociedade e trouxeram novos desafios nesta matéria[12]. A necessidade de reformar e modernizar o presente regime jurídico deveu-se, em grande medida, por não responder aos desafios impostos pelas novas tecnologias, não obstante, reconhece a validade dos princípios fundamentais da Diretiva[13] – os direitos e liberdades fundamentais das pessoas singulares e a livre circulação de dados pessoais.

Neste sentido, de forma a acautelar estes fatores e a construção de um Mercado Único Digital[14], foi publicado o 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

---

[10] ALVES, Lurdes Dias – *Proteção de Dados no Contexto Laboral*. Coimbra: Edições Almedina, 2020, p. 15.

[11] SANTOS, Patrícia Andreia Batista e – *A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*. Lisboa: Faculdade de Direito da Universidade Nova de Lisboa, 2019, p. 19. Disponível em: https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf (acedido a 31.01.2024).

[12] COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES – «*Uma abordagem global da proteção de dados pessoais na União Europeia*», de 1 de novembro de 2010, p. 2.

[13] SANTOS, Patrícia Andreia Batista e – *A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*. Lisboa: Faculdade de Direito da Universidade Nova de Lisboa, 2019, p. 23. Disponível em: https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf (acedido a 31.01.2024).

[14] Cfr. COMISSÃO EUROPEIA, COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES – *Estratégia para o Mercado Único Digital na Europa*, COM (2015) 192 final, Bruxelas, 6 de maio de 2015, p. 3. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52015DC0192&from=EN (acedido a 31.01.2024).

revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), que iniciou a sua aplicação a 25 de maio de 2018.

No panorama nacional, passado mais de um ano após o início de aplicação do RGPD em todos os Estados-Membros da UE, foi publicada a 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. Este diploma tem o objeto de reforçar as situações específicas de tratamento que o RGPD não cobre, devido às suas cláusulas abertas, atribuindo, deste modo, competências legislativas aos Estados-Membros[15].

Todavia, a Comissão Nacional de Proteção de Dados (CNPD) – autoridade de controlo nacional – emitiu a Deliberação 2019/494 que veio desaplicar algumas normas da Lei n.º 58/2019, por violarem o princípio do primado do direito da União[16] estando, entre elas, as normas relativas ao tratamento de dados pessoais nas relações laborais (art. 28.º da Lei n.º 58/2019).

2. A Proteção de Dados Pessoais nas Relações Laborais

2.1. O Ciclo de Vida do Contrato de Trabalho

2.1.1. Enquadramento

Quando nos debruçamos sobre as relações laborais, temos, em linha de conta, que o tratamento de dados pessoais neste contexto começa bem antes de se iniciar a relação entre trabalhador e empregador. Ou seja, existe tratamento de dados pessoais numa fase pré-contratual

---

[15] CORDEIRO, A. Barreto Menezes – *Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019*. Coimbra: Edições Almedina, 2020, p. 41.

[16] COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS – *Deliberação/2019/494 sobre a desaplicação, na apreciação de casos concretos, de algumas normas da Lei 58/2019*, p. 1v.

(recrutamento e seleção), na admissão do trabalhador, na execução do contrato e, por fim, na cessação da relação laboral[17].

No entanto, durante as diferentes fases do ciclo de vida do contrato de trabalho, em que os dados pessoais dos trabalhadores são tratados, temos de ter em atenção a legislação aplicável a cada um dos momentos, devido às situações específicas em que é necessário aplicar regulamentação especial[18], como acontece nas situações em que estamos perante um contrato de trabalho temporário[19], por exemplo.

O Direito à Proteção de Dados não é um direito absoluto (considerando 4 do RGPD), por isso, tem de ser conjugado com o regime jurídico aplicável neste contexto, ou seja, a legislação laboral. O Código do Trabalho (CT) apresenta um conjunto de normas que remetem para diferentes temas do âmbito laboral que se encontram previstos nos direitos de personalidade do trabalhador (arts. 14.º a 22.º do CT)[20], os quais destacamos: (i) a reserva da intimidade da vida privada (art. 16.º do CT) e a (ii) proteção de dados pessoais (art. 17.º do CT).

O direito à reserva da intimidade da vida privada[21], segundo o art. 16.º do CT, indica que as partes – empregador e trabalhador – devem respeitar os direitos de personalidade da contraparte, de forma a guardar reserva quanto à intimidade da vida privada (n.º 1) sendo que esta

---

[17] SANTOS, Patrícia Andreia Batista e – *A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*. Lisboa: Faculdade de Direito da Universidade Nova de Lisboa, 2019, p. 47. Disponível em: https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf (acedido a 01.02.2024).

[18] *Ibidem*.

[19] Regime do exercício e licenciamento da atividade da empresa de trabalho temporário e do acesso e exercício da atividade da agência privada de colocação de candidatos a emprego (Decreto-lei n.º 260/2009, republicado pela Lei n.º 5/2014 de 12 de fevereiro e alterado pela Lei n.º 146/2015).

[20] Os trabalhadores da função pública são igualmente abrangidos pelos direitos de personalidade previstos no CT, tal como estabelece o art. 4.º da Lei Geral do Trabalho em Funções Públicas (Lei n.º 35/2014, de 20 de junho).

[21] Segundo ALVES, o direito à reserva da intimidade da vida privada visa defender dois interesses. O primeiro resulta do interesse de evitar a tomada de conhecimento e a divulgação de informação pessoal; e o segundo que o direito em causa tutela um interesse na subtração à atenção dos outros (Cfr. ALVES, Lurdes Dias – *Proteção de Dados no Contexto Laboral*. Coimbra: Edições Almedina, 2020, p. 22).

abrange o acesso, divulgação de aspetos relacionados com a esfera íntima e pessoal das partes, nomeadamente no que toca à vida familiar, afetiva e sexual, bem como ao estado de saúde e com as convicções políticas e religiosas (n.º 2). Face ao artigo exposto, o art. 80.º do Código Civil, também apresenta o dever de todos guardarem reserva quanto à intimidade da vida privada dos demais (n.º 1), sendo que a sua extensão é definida consoante a natureza do caso e a condição das pessoas em causa (n.º 2)[22]. Igualmente a CRP, no seu art. 26.º, prevê a todos o reconhecimento do direito à reserva da intimidade da vida privada e familiar (n.º 1).

Relativamente ao direito à proteção de dados previsto no CT, iremos abordá-lo mais adiante, por se tratar de um artigo que remete para duas das fases do ciclo de vida do contrato de trabalho – a fase pré-contratual e de execução do contrato de trabalho.

2.1.2. O conceito de dados pessoais no âmbito das relações laborais

Antes de nos debruçarmos sobre as fases do ciclo de vida do contrato de trabalho, temos de compreender o que são dados pessoais, quer na sua definição, quer no âmbito do presente trabalho.

Segundo o n.º 1 do art. 4.º do RGPD, a definição de dados pessoais remete para toda a "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)", sendo que "é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação (…) a um ou mais

[22] De forma a delimitar o âmbito de proteção do direito à reserva da intimidade da vida privada, é utilizada a teoria das três esferas (Cfr. ALVES, Lurdes Dias – *Proteção de Dados no Contexto Laboral*. Coimbra: Edições Almedina, 2020, p. 22). Esta teoria – originária da jurisprudência e doutrina alemã – é composta pela: (i) esfera pública, na qual se insere a informação conhecida pelo público geral; (ii) esfera privada, na qual a informação apenas pertente a um grupo restrito de pessoas; e a (iii) esfera íntima, conhecida como uma esfera sagrada, devido à informação não ser do conhecimento das demais pessoas (Cfr. MARQUES, Garcia e MARTINS, Lourenço – *Direito da Informática*. Coimbra: Edições Almedina, 2000, p. 105).

elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".

Verificamos que esta definição apresenta um âmbito de aplicação muito amplo[23], o que vem confirmar que o conceito de dados pessoais abrange informações relativas à vida privada, bem como à vida profissional e social dos indivíduos[24], o que conjuga com o tratamento de dados pessoais de trabalhadores que são mencionados ao longo do RGPD, mais concretamente no n.º 2 do art. 9.º e no art. 88.º.[25]. O Acórdão *Nowak* reforça essa afirmação ao referir que o sentido amplo do conceito de dados pessoais "não está limitado às informações sensíveis ou de ordem privada, mas engloba potencialmente qualquer tipo de informações, tanto objetivas como subjetivas sob forma de opiniões ou de apreciações, na condição de «dizerem respeito» à pessoa em causa"[26].

Desta forma colocamos a seguinte questão: O que se entende por dados pessoais de trabalhadores?

Respondendo à questão, os dados pessoais dos trabalhadores são todos aqueles que envolvem o trabalhador, desde a fase pré-contratual à cessação da relação laboral[27], sendo estes compostos, em grosso modo, pelo CV que compila um vasto conjunto de informações sobre o candidato a emprego ou trabalhador – nome completo, contactos, experiência profissional, formação académica, etc. – mas também todos os dados recolhidos durante a admissão e execução do contrato de trabalho – dados bancários (IBAN), dados de contacto (morada), avaliação de desempenho, registos de tempos de trabalho, etc.

---

[23] Acórdão de 13 de maio de 2014, "*Google Spain*", C-131/12, ECLI:EU:C:2014:317, n.º 54.

[24] CORDEIRO, A. Barreto Menezes – *Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019*. Coimbra: Edições Almedina, 2020, p. 108.

[25] *Ibidem*.

[26] Acórdão de 20 de dezembro de 2017, "*Nowak"*, C-434/16, ECLI:EU:C:2017:994, n.º 34, cit.

[27] SANTOS, Patrícia Andreia Batista e – *A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*. Lisboa: Faculdade de Direito da Universidade Nova de Lisboa, 2019, p. 49. Disponível em: https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf (acedido a 02.02.2024).

Entretanto, são igualmente recolhidos e tratados dados pessoais com uma categorização especial – categorias especiais de dados ou "dados sensíveis" –, pelo facto, de serem proibidos de tratar, à partida, como prevê o n.º 1 do art. 9.º do RGPD.

O n.º 1 do art. 9.º do RGPD refere que os dados que revelem a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, bem como os dados genéticos, biométricos, de saúde ou relativos à vida sexual ou orientação sexual não podem ser alvo de tratamento, a menos que se enquadrem nas situações previstas no n.º 2 do presente artigo. No entanto, dentro do leque de situações em que estes dados podem ser tratados, encontramos duas situações que se aplicam no contexto laboral: (i) quando o tratamento for necessário para efeitos do cumprimento de uma obrigação legal e do exercício de direitos específicos do responsável pelo tratamento ou do titular de dados no âmbito da legislação laboral, segurança social e de proteção social (alínea b) do n.º 2 do art. 9.º); e (ii) para efeitos de medicina preventiva ou do trabalho, avaliação da capacidade de trabalho do empregado, diagnóstico médico, prestação de cuidados de saúde ou de ação social ou gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros (alínea h) do n.º 2 do art. 9.º). Ou seja, estas duas situações apresentam um contexto específico da realidade laboral, identificando assim, o (i) cumprimento de obrigações legais e o exercício de direitos específicos em matéria de legislação laboral e a (ii) segurança e saúde no trabalho[28].

Nesse sentido, colocamos a questão: Quais são as categorias especiais de dados que podem ser tratados neste âmbito?

Como foi referido *supra*, as categorias especiais de dados não podem ser objeto de tratamento a menos que se verifique uma das exceções previstas no n.º 2 do art. 9.º do RGPD. Neste contexto, os dados pessoais que podem ser tratados são referentes à filiação sindical, dados relativos à saúde e dados biométricos para o controlo de assiduidade e acessos[29].

---

[28] *Idem*, p. 51.
[29] *Ibidem*.

Como podemos verificar, a tipologia de dados apresentada é muito específica do âmbito laboral, sendo que estes dados são recolhidos e tratados, sobretudo, nas fases de admissão e execução do contrato de trabalho, como veremos mais adiante.

Esta diferente categorização, entre dados pessoais e categorias especiais de dados, será relevante quando abordarmos os fundamentos de licitude aplicados no decorrer do presente trabalho.

2.2. As Fases do Ciclo de Vida do Contrato de Trabalho

2.2.1. O artigo 88.º do RGPD

O RGPD apresenta uma norma específica, relativamente ao tratamento de dados pessoais no contexto laboral, através do seu art. 88.º. Esta norma resulta da consciencialização das várias possibilidades de controlo do empregador sobre o trabalhador, através da utilização das novas tecnologias, bem como das diferenças em proteção laboral dos diferentes Estados-Membros relativamente ao tratamento de dados pessoais de trabalhadores[30]. Neste sentido, determina que os Estados-Membros podem estabelecer na sua ordem jurídica ou em convenções coletivas de trabalho, normas mais específicas que garantam a defesa dos direitos e liberdades relativamente ao tratamento de dados pessoais de trabalhadores no contexto laboral (primeira parte do n.º 1 do art. 88.º do RGPD).

Quando nos debruçamos sobre os tratamentos de dados pessoais efetuados neste âmbito, verificamos que os mesmos se encontram inseridos nas diferentes fases do ciclo de vida do contrato de trabalho e, por sua vez, em algumas das finalidades de tratamento realizadas em contexto laboral, nomeadamente: (i) o recrutamento; (ii) a execução do contrato; (iii) o cumprimento das obrigações previstas na ordem jurídica ou em convenções coletivas de trabalho relativas à gestão e

[30] MOREIRA, Teresa Coelho – *Direito do Trabalho na Era Digital. Coimbra*: Edições Almedina, 2021, p. 196.

organização do trabalho, à saúde e segurança no trabalho, à proteção dos bens do empregador, aos direitos e benefícios do trabalhador; (iv) e a cessação da relação laboral (segunda parte n.º 1 do art. 88.º do RGPD).

Pelo facto do art. 88.º do RGPD ser uma cláusula aberta, deu oportunidade ao legislador nacional de estabelecer normas relativas a esta situação específica através do art. 28.º da Lei n.º 58/2019[31]. Esta norma reforça que os dados pessoais dos trabalhadores podem ser alvo de tratamento por parte do empregador, para as finalidades e com os limites definidos no Código do Trabalho, bem como na respetiva legislação complementar ou em outros regimes setoriais (n.º 1 do presente artigo).

No entanto, temos de ter em consideração que o tratamento de dados pessoais no contexto laboral deve incluir medidas adequadas e específicas, de forma a salvaguardar os interesses legítimos e os direitos fundamentais do titular de dados, neste caso, o candidato a emprego e do trabalhador (n.º 2 do art. 88.º do RGPD).

2.2.2. A Pré-Contratação

O primeiro contacto entre as partes – candidato a emprego e empregador –, dá-se quando um indivíduo demonstra interesse em candidatar-se a (i) uma vaga de emprego ou (ii) espontaneamente, através dos diferentes canais para esse efeito; seja através do site institucional de uma empresa e redes sociais profissionais – como o *LinkedIn* –, mas também em sites de emprego ou de trabalho temporário.

O leque de canais para que um candidato a emprego possa submeter o seu CV é vasto, resultado da evolução tecnológica que conduziu à

[31] 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.

alteração das modalidades de recrutamento[32] que, ao longo dos anos, transitaram do CV em papel para o digital, sendo esta a modalidade mais comum nos dias de hoje.

Independentemente do canal de submissão[33], deve ser transmitido, quando os dados pessoais são recolhidos, um conjunto de informações relativas ao seu tratamento. Ou seja, as empresas, neste caso, o responsável pelo tratamento[34], tem o direito de informar o candidato a emprego quanto aos (i) elementos relacionados com o responsável pelo tratamento e Encarregado de Proteção de Dados – identidade e contactos –, os (ii) requisitos legais para proceder ao tratamento dos dados – as finalidades de tratamento; os interesses legítimos do responsável pelo tratamento ou de um terceiro, quando aplicado o n.º 1 do art. 6.º do RGPD; os prazos de conservação[35] e os direitos que o titular dos dados pode exercer, incluindo o direito a reclamar e a retirada de consentimento, quando aplicável – e (iii) os destinatários dos dados pessoais – nas situações em que se verifique transferências de dados pessoais

---

[32] SANTOS, Patrícia Andreia Batista e – *A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*. Lisboa: Faculdade de Direito da Universidade Nova de Lisboa, 2019, p. 54. Disponível em: https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf (acedido a 03.02.2024).

[33] Os candidatos podem submeter o seu CV através de formulários *online* que se encontram disponíveis no site institucional da empresa que publicou a vaga, ou através da criação de uma conta, em que é replicado o CV para que a empresa possa aceder aos seus dados pessoais, bem como visualizar o histórico de candidaturas efetuadas.

[34] O responsável pelo tratamento é a pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que individualmente ou em conjunto, determina as finalidades e os meios de tratamento de dados pessoais (n.º 7 do art. 4.ºdo RGPD).

[35] Apesar de não se encontrar definido um prazo de conservação para os dados recolhidos durante o processo de recrutamento e seleção, neste caso o CV, a CNPD defende que os dados pessoais relativos aos candidatos a emprego desatualizam no prazo de um ano a contar desde a data em que os mesmos foram recolhidos. Disponível em: <https://rhmagazine.pt/os-dados-dos--seus-colaboradores-respeitam-rgpd/> (acedido a 03.02.24). No entanto, as empresas devem manter o registo dos processos de recrutamento por um período de cinco anos, sendo que esse registo deve conter, com desagregação por sexo, os (i) convites para o preenchimento de lugares; os (ii) anúncios de oferta de emprego; os números de (iii) candidaturas para apreciação curricular, (iv) candidatos presentes nas entrevistas de pré-seleção e os (v) que aguardam ingresso; os (vi) resultados de testes ou provas de admissão ou seleção; e (viii) balanços sociais (n.º 1 do art. 32.º do CT).

para países terceiros ou uma organização internacional[36] – que se encontram previstos no art. 13.º e no n.º 1 e 2 do art. 14.º do RGPD[37].

Com base nas informações referidas *supra*, colocamos duas questões fundamentais:

I. Quais são as categorias de dados pessoais tratadas para este efeito?
II. Quais são as finalidades de tratamento identificadas neste âmbito?

Respondendo à primeira questão, o CV é o elemento que contem a maioria dos dados pessoais utilizados durante o processo de recrutamento e seleção. Neste sentido, as principais categorias de dados pessoais que se encontram no CV são: os dados de identificação e de contacto; dados curriculares/académicos[38] e dados relativos à experiência profissional[39].

No entanto, podem ser recolhidas outras categorias de dados que, à partida, não podem ser exigidas ao candidato a emprego. O n.º 1 do art. 17.º do CT refere que o empregador não pode obrigar o candidato a emprego, bem como ao trabalhador, a prestar informações relativas à sua vida privada, saúde ou estado de gravidez. Todavia, estes dados são tratados exclusivamente, nas situações em que sejam estritamente

---

[36] PINHEIRO, Alexandre Sousa *et al*. – *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Edições Almedina, 2018, p. 348.

[37] Apesar dos arts. 13.º e 14.º do RGPD apresentarem conteúdo idêntico com ligeiras exceções, o legislador europeu decidiu distingui-los por demonstrarem dois meios de recolha diferentes: os (i) dados pessoais recolhidos junto do titular – art. 13.º – e os (ii) dados pessoais que não foram recolhidos junto do titular – art. 14.º. (Cfr. CORDEIRO, A. Barreto Menezes – *Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019*. Coimbra: Edições Almedina, 2020, p. 340).

[38] No decorrer do processo de recrutamento e seleção, o empregador poderá solicitar documentação que comprove os títulos escolares/académicos relevantes para a vaga que o candidato concorreu, sendo, desta forma realizado o *pre-employment background checks* do mesmo (Cfr. SANT'ANA, Simão e GOUVEIA, Vitorino – *Guia Prático para a conformidade com o RGPD nos Recursos Humanos*. Coimbra: Edições Almedina, 2021, p. 112).

[39] SANT'ANA, Simão e GOUVEIA, Vitorino – *Guia Prático para a conformidade com o RGPD nos Recursos Humanos*. Coimbra: Edições Almedina, 2021, p. 119.

necessários e relevantes para avaliar a aptidão do candidato a emprego/trabalhador (alínea a) do n.º 1 do art. 17.º do CT); ou quando particulares exigências inerentes à natureza da atividade profissional o justifiquem (alínea b) do n.º 1 do art. 17.º do CT)[40], sendo que, em ambos os casos, é necessário que seja fornecida por escrito, a fundamentação para esse tratamento.

Além disso, nas situações em que são exigidos dados relativos à saúde e estado de gravidez[41], os mesmos são prestados ao médico, que apenas pode comunicar ao empregador se o candidato a emprego/trabalhador se encontra apto, ou não, para desempenhar a função (n.º 3 do art. 17.º do CT).

Relativamente à segunda questão colocada, a finalidade de tratamento identificada neste âmbito, pelo responsável pelo tratamento, é o recrutamento e seleção[42]. Ou seja, os dados pessoais do candidato a emprego somente são tratados para esta finalidade, que deve seguir os princípios impostos pelo RGPD, mais concretamente, o princípio da limitação das finalidades previsto na alínea b) do n.º 1 do art. 5.º do RGPD[43].

Apesar dos deveres de informação levantarem diversas questões, nomeadamente, quais os fundamentos de licitude aplicados neste contexto, esse ponto será abordado no próximo capítulo.

---

[40] Só em casos muito excecionais relacionados com o tipo de atividade e posto de trabalho, é que podem ser exigidos ao trabalhador, informações relativas ao seu estado de saúde ou gravidez (Cfr. MARTINEZ, Pedro Romano *et al*. – *Código do Trabalho Anotado*. Coimbra: Edições Almedina, 12.ª Ed, 2020, p. 104).

[41] Pelo facto dos dados relativos à saúde e estado de gravidez se encontrarem inseridos nas categorias especiais de dados, o empregador só pode ter acesso à declaração médica que indique se o candidato a emprego ou trabalhador se encontra apto/inapto, sendo a mesma emitida pelo médico da medicina do trabalho (Cfr. SANT'ANA, Simão e GOUVEIA, Vitorino – *Guia Prático para a conformidade com o RGPD nos Recursos Humanos*. Coimbra: Edições Almedina, 2021, p. 111).

[42] SANT'ANA, Simão e GOUVEIA, Vitorino – *Guia Prático para a conformidade com o RGPD nos Recursos Humanos*. Coimbra: Edições Almedina, 2021, p. 118.

[43] O princípio da limitação das finalidades indica que os dados pessoais são recolhidos para finalidades determinadas, explícitas e legitimas e não podem ser tratados posteriormente de forma incompatível com essas finalidades (alínea b) do n.º 1 do art. 5.º, n.º 1 do RGPD).

2.2.3 Admissão do trabalhador e execução do contrato de trabalho

Quando o candidato a emprego é selecionado para preencher a vaga para qual concorreu, o empregador inicia ao seu processo de admissão que vai resultar, no exercício das funções do, agora, trabalhador.

Durante estas duas fases, será realizada uma recolha adicional de dados pessoais de forma a poder ser elaborado o contrato de trabalho[44], que resultará no início da relação laboral entre trabalhador e empregador.

É importante referir que ao iniciar a relação laboral, o RGPD e a Lei n.º 58/2019 devem ser conjugadas com o CT e legislação específica para esse efeito, tal como determina o n.º 1 do art. 28.º da Lei n.º 58/2019.

A admissão e o exercício de funções representam duas fases distintas do ciclo de vida do contrato de trabalho. Porventura, os dados pessoais recolhidos e tratados durante estas duas fases, além de apresentarem diferentes categorias de dados, também constituem distintas finalidades de tratamento como veremos de seguida.

Os exemplos de categorias de dados pessoais tratados neste âmbito são diversos. Neste sentido, iremo-nos debruçar nas mais relevantes. Dentro das categorias de dados apresentadas nas duas fases em análise, destacamos:

I. Fase de admissão do trabalhador: Dados de identificação e contacto; relativos à situação familiar (número de dependentes); categoria profissional e antiguidade na empresa (caso se verifique, sobretudo nas situações de mobilidade interna); retributivos e benefícios associados[45].

---

[44] SANT'ANA, Simão e GOUVEIA, Vitorino – *Guia Prático para a conformidade com o RGPD nos Recursos Humanos*. Coimbra: Edições Almedina, 2021, p. 127.

[45] *Idem*, p. 136.

II. Fase do exercício de funções/execução do contrato de trabalho: Dados de identificação e contacto; financeiros e fiscais; relativos à formação escolar/académica e experiência profissional; ações de formação profissional; categoria profissional e antiguidade na empresa; assiduidade e absentismo; desempenho profissional; saúde; acidentes de trabalho; processos disciplinares; penhora (caso se verifique); quotas sindicais e de recolha de imagem[46].

Como verificamos, o volume de categorias de dados pessoais tratados, sobretudo, na fase do exercício de funções/execução do contrato de trabalho é relativamente maior, do que em outras fases do ciclo do contrato de trabalho. Isto deve-se ao facto desta fase coincidir com os dados pessoais que são tratados no âmbito da gestão dos recursos humanos.

Em relação às finalidades de tratamento atribuídas em ambas as fases, podemos agrupá-las, verificando-se assim a: celebração e execução do contrato de trabalho; gestão de recursos humanos; avaliação de desempenho; gestão administrativa; controlo de assiduidade; processamento salarial; formação; medicina do trabalho; gestão de acidentes de trabalho; gestão de benefícios; gestão de processos disciplinares; gestão de penhoras e pagamento de quotas sindicais e videovigilância[47].

Subsequentemente, iremos verificar que os fundamentos de licitude aplicados apresentam uma maior diversidade, relativamente aos atribuídos na fase anterior, como iremos analisar no próximo capítulo.

É importante frisar que, independentemente da fase do ciclo em que se encontram os dados pessoais dos trabalhadores, os mesmos devem ser salvaguardados pelos direitos de personalidade previstos nos arts. 16.º e seguintes do CT.

---

[46] *Idem*, p. 136 – 138.
[47] *Idem*, p. 135 – 136.

2.2.4. Cessação do Contrato de Trabalho

Ao contrário do que verificámos até agora, quando o contrato de trabalho cessa[48], questiona-se o que fazer em relação aos dados pessoais recolhidos durante as fases anteriores a esta[49], dado que estamos perante a última fase do ciclo de vida do contrato de trabalho.

No entanto, apesar de podermos hesitar entre o apagamento dos dados pessoais do, agora, ex-trabalhador e a sua conservação, temos de ter em linha de conta que o apagamento dos dados não ocorre apenas quando se verifica a cessação do contrato de trabalho[50]. Isto deve-se ao facto de existirem prazos estipulados por lei que permitem a monitorização dos dados e o apagamento dos mesmos ainda durante a execução do contrato de trabalho[51]. Ou seja, o apagamento de dados pessoais de trabalhadores não é imediato por existirem prazos de conservação aplicados a esses dados que podem ocorrer em qualquer uma das fases do ciclo de vida do contrato de trabalho.

A título de exemplo, quando um contrato de trabalho cessa, os dados relativos a declarações contributivas para efeitos de aposentação ou reforma podem ser conservados por tempo indeterminado com o objeto de auxiliar o trabalhador na reconstituição da carreira contributiva[52] (n.º 6 do art. 21.º da Lei n.º 58/2019). Todavia, o mesmo não se verifica quando, durante a vigência do contrato, são realizadas operações de tratamento de dados biométricos para controlo de assiduidade e acessos às instalações do empregador, sendo que esses dados devem ser destruídos quando o contrato de trabalho cessa (n.º 3 do art. 18.º do CT).

---

[48] O art. 340.º do CT define as modalidades de cessação do contrato de trabalho, sendo estas compostas pela (i) caducidade; (ii) revogação; (iii) despedimento por facto imputável ao trabalhador; (iv) despedimento coletivo; (v) despedimento por extinção do posto de trabalho; (vi) despedimento por inadaptação; (vii) resolução pelo trabalhador; e (viii) denúncia pelo trabalhador.

[49] SANT'ANA, Simão e GOUVEIA, Vitorino – *Guia Prático para a conformidade com o RGPD nos Recursos Humanos*. Coimbra: Edições Almedina, 2021, p. 288.

[50] *Ibidem*.

[51] *Ibidem*.

[52] Em regra geral, os dados pessoais do trabalhador devem ser eliminados quando o contrato de trabalho cessa, a menos que recaia sobre o empregador, uma obrigação jurídica de conservação (Cfr. PINHEIRO, Alexandre Sousa *et al*. – *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Edições Almedina, 2018, p. 674).

É importante ressalvar que, independentemente da fase em que se encontra o ciclo de vida do contrato de trabalho, devem ser respeitados os princípios relativos ao tratamento de dados pessoais previsto pelo RGPD, nomeadamente o princípio da minimização[53] e da limitação da finalidade[54].

3. Os Fundamentos de Licitude aplicados nas Relações Laborais

3.1. Os fundamentos de licitude

O princípio da licitude, lealdade e transparência define que os dados pessoais são objeto de um tratamento lícito, leal e transparente relativamente ao titular dos dados (alínea a) do n.º 1 do art. 5.º do RGPD). A licitude – a qual nos debruçamos no presente trabalho – encontra-se associada ao cumprimento da legitimidade na prossecução do tratamento de dados pessoais. Isto é, os dados são tratados de forma lícita quando cumprem com as disposições que regem os direitos e a legitimidade no tratamento, bem como as exigências previstas na CDFUE[55].

Neste sentido, o princípio da licitude, lealdade e transparência vai nos remeter para os fundamentos de licitude previstos no RGPD, mais concretamente o art. 6.º. Não obstante, o RGPD não apresenta de uma forma clara, quais os fundamentos de licitude aplicados nas relações laborais, encontrando-se assim, dispersos ao longo do RGPD, nomeadamente nos arts. 6.º e 9.º[56].

---

[53] O princípio da minimização refere que os dados devem ser adequados, pertinentes e limitados ao que é necessário em relação às finalidades para as quais são tratados (alínea c) do n.º 1 do art. 5.º do RGPD).

[54] O princípio da limitação da finalidade indica que os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades (alínea b) do n.º 1 do art. 5.º do RGPD).

[55] PINHEIRO, Alexandre Sousa *et al*. – *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Edições Almedina, 2018, p. 207.

[56] SANTOS, Patrícia Andreia Batista e – *A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*. Lisboa: Faculdade de Direito da Universidade Nova de Lisboa, 2019, p. 49. Disponível em: https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf (acedido a 05.02.2024).

Como referimos anteriormente, verifica-se uma distinção entre categorias "gerais" de dados pessoais (n.º 1 do art. 4.º do RGPD) e categorias especiais de dados (n.º 1 do art. 9.º do RGPD). Consequentemente, essa categorização vai-se replicar nos fundamentos de licitude aplicados ao tratamento dos dados. Ou seja, as categorias "gerais" de dados vão remeter para os fundamentos de licitude previstos no art. 6.º do RGPD e as categorias especiais de dados para as exceções previstas no n.º 2 do art. 9.º do RGPD.

Fazendo a distinção entre estas duas categorias, observamos diferentes fundamentos de licitude e exceções que são aplicadas no tratamento de dados de candidatos a emprego e trabalhadores. Nas categorias "gerais" de dados verificamos: (i) a execução do contrato ou diligências pré-contratuais a pedido do titular (alínea b) do n.º 1 do art. 6.º do RGPD); (ii) a obrigação jurídica (alínea c) do n.º 1 do art. 6.º do RGPD); e os interesses legítimos do responsável pelo tratamento (alínea f) do n.º 1 do art. 6.º do RGPD)[57].

I. Execução do contrato ou diligências pré-contratuais

A execução do contrato é caracterizada como o principal fundamento de licitude aplicado ao tratamento de dados pessoais de trabalhadores, por ser o mais utilizado pelo empregador[58]. Por sua vez, as diligências pré-contratuais a pedido do titular também abrangem o tratamento que precede à celebração do contrato de trabalho entre as partes[59]. Não obstante, este fundamento não equivale a uma promessa de celebração de contrato, como ocorre durante o processo de

[57] *Idem*, p. 50.

[58] HENRIQUES, Sérgio Coimbra e LUÍS, João Vares – "Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral" *In*: *Anuário da Proteção de Dados 2019*. Lisboa: CEDIS, 2019, p. 30 – 31.

[59] PINHEIRO, Alexandre Sousa *et al*. – *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Edições Almedina, 2018, p. 216.

recrutamento e seleção de um candidato a emprego[60] – sendo um fundamento de licitude aplicado a uma situação particular[61].

II. Obrigação Jurídica

Recai sobre este fundamento as obrigações previstas na legislação laboral que têm impacto no tratamento de dados pessoais de trabalhadores no âmbito da gestão de recursos humanos, nomeadamente as obrigações em matéria da segurança e saúde no trabalho, por exemplo[62].

III. Interesses Legítimos do Responsável pelo Tratamento

Quando o empregador aplica o interesse legítimo, como fundamento de licitude, tem de verificar se a finalidade de tratamento em causa é legítima. Neste sentido, o tratamento sobre os dados pessoais de trabalhadores, deve ser realizado através de métodos ou tecnologias específicas que sejam consideradas estritamente necessárias, adequadas e proporcionais, de forma a serem aplicadas com o menor grau de intrusão possível para a privacidade e respeito dos direitos e liberdades da pessoa singular[63] – ou seja, do trabalhador.

Nas categorias especiais de dados, ao contrário do que verificamos *supra*, os fundamentos de licitude encontram-se previstos nas exceções do art. 9.º do RGPD: (i) o cumprimento de obrigações jurídicas e do

---

[60] *Idem*, p. 671.

[61] Existem empresas a recorrer ao tratamento de dados pessoais com base no consentimento do candidato a emprego, por atribuírem à declaração de consentimento a garantia de licitude para o tratamento dos dados. Por sua vez, o consentimento acaba por não ser o fundamento de licitude adequado, nestas circunstâncias, dando assim lugar às diligências pré-contratuais devido ao candidato a emprego estar a proceder a uma diligência pré-contratual quando envia um CV para uma empresa (Cfr. PINHEIRO, Alexandre Sousa *et al*. – *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Edições Almedina, 2018, p. 671).

[62] HENRIQUES, Sérgio Coimbra e LUÍS, João Vares – "Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral*" In*: *Anuário da Proteção de Dados 2019*. Lisboa: CEDIS, 2019, p. 29.

[63] *Idem*, p. 31.

exercício de direitos específicos associados à relação laboral (alínea b) do n.º 2 do art. 9.º do RGPD); e (ii) testes e exames médicos (alínea h) do n.º 2 do art. 9.º).

Posto isto, colocamos a seguinte questão: Como é que os fundamentos de licitude no tratamento de dados pessoais de candidatos a emprego e trabalhadores são aplicados na prática?

Para responder à questão, recolhemos dois exemplos para demonstrar as atividades e finalidades de tratamento aplicadas no âmbito das relações laborais e os respetivos fundamentos de licitude.

Tabela 1 – Exemplos dos fundamentos de licitude aplicados nas relações laborais[64]

Finalidade de Tratamento	Fundamento de Licitude
Celebração e Execução do Contrato de Trabalho	Execução do contrato; Obrigação jurídica
Gestão de Recursos Humanos (RH)	Execução do contrato; Obrigação jurídica
Processo de Avaliação de Desempenho	Execução do contrato
Gestão Administrativa e de Contactos	Execução do contrato
Controlo de Assiduidade/Absentismo	Execução do contrato; Obrigação jurídica
Processamento Salarial	Execução do contrato; Obrigação jurídica
Formação Profissional	Execução do contrato; Obrigação jurídica

[64] SANT'ANA, Simão e GOUVEIA, Vitorino – *Guia Prático para a conformidade com o RGPD nos Recursos Humanos*. Coimbra: Edições Almedina, 2021, p. 135.

Finalidade de Tratamento	Fundamento de Licitude
Medicina do Trabalho	Obrigação jurídica
Gestão de Acidentes de Trabalho	Obrigação jurídica
Gestão de Benefícios Retributivos	Execução do contrato
Gestão de Processos Disciplinares	Execução do contrato
Gestão de Penhoras e Pagamento de Quotas Sindicais	Obrigação jurídica
Finalidades Estatísticas	Obrigação jurídica
Videovigilância	Interesse legítimo do responsável

Tabela 2 – Aplicação dos fundamentos de licitude no tratamento de dados pessoais no âmbito da gestão de recursos humanos[65]

Atividade de Tratamento	Finalidade de Tratamento	Fundamento de Licitude
Recrutamento	Tratamento de candidaturas e gestão de entrevistas	Diligências pré-contratuais
	Criação de uma base de dados com os CV's dos candidatos	Interesse legítimo do responsável

[65] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS – *Référentiel relatif aux traitements de données à caractère personnel mis en oeuvre aux fins de gestion du personnel*. Disponível em: <https://www.cnil.fr/sites/default/files/atoms/files/referentiel_grh_novembre_2019_0.pdf> (acedido a 07.02.2024).

Atividade de Tratamento	**Finalidade de Tratamento**	**Fundamento de Licitude**
Gestão Administrativa de Pessoal	Gestão de processos dos trabalhadores	Execução do contrato
	Realização de relatórios estatísticos	Interesse legítimo do responsável
	Gestão da estrutura interna organizacional	Interesse legítimo do responsável
	Gestão de *fringe benefits*	Interesse legítimo do responsável
	Gestão de eleições no seio organizacional	Obrigação jurídica
	Gestão de reuniões de órgãos representativos de trabalhadores	Obrigação jurídica
Gestão de Remunerações e Cumprimento de Formalidades Administrativas	Estabelecimento de remunerações e fornecimento da declaração de vencimento	Execução do contrato
	Declaração social nominativa	Obrigação jurídica

Atividade de Tratamento	Finalidade de Tratamento	Fundamento de Licitude
Fornecimento de Equipamento Informático aos Trabalhadores	Manutenção e monitorização da rede informática	Interesse legítimo do responsável
	Gestão da rede informática permitindo a definição de acessos a aplicações e outras redes	Interesse legítimo do responsável
	Implementação de dispositivos destinados a garantir a segurança e o bom funcionamento das redes e aplicações	Interesse legítimo do responsável
	Gestão do *e-mail* profissional	Interesse legítimo do responsável
	Utilização da *intranet* para divulgar ou recolher dados da gestão administrativa	Interesse legítimo do responsável
Organização do Trabalho	Gestão de agenda de projetos profissionais	Interesse legítimo do responsável
Gestão de Carreira e de Mobilidade	Avaliação de desempenho dos trabalhadores	Interesse legítimo do responsável
	Gestão de competências profissionais internas	Interesse legítimo do responsável
	Validação do certificado de competências profissionais	Interesse legítimo do responsável
	Gestão da mobilidade profissional	Execução do contrato

Atividade de Tratamento	Finalidade de Tratamento	Fundamento de Licitude
Formação	Acompanhamento de pedidos e de períodos de formação	Execução do contrato
	Organização de ações de formação e a avaliação das competências adquiridas	Interesse legítimo do responsável
Gestão da Ação Social	Gestão da ação social e cultural implementada pelo empregador, excluindo a saúde ocupacional, atividades de serviço social ou suporte psicológico	Interesse legítimo do responsável

As tabelas 1 e 2 apresentam as várias atividades de tratamento que são efetuadas no âmbito da gestão de recursos humanos, que se baseiam na execução do contrato ou diligências pré-contratuais a pedido do titular (alínea b) do n.º 1 do art. 6.º do RGPD), obrigação jurídica (alínea c) do n.º 1 do art. 6.º do RGPD) e no interesse legítimo do responsável (alínea f) do n.º 1 do art. 9.º do RGPD).

Ao verificarmos as duas tabelas, entendemos que, na prática, são aplicados os fundamentos previstos no art. 6.º do RGPD, por este cobrir as situações em que são tratados os dados pessoais de trabalhadores. Entretanto, constatamos que em ambos os exemplos não eram aplicados as exceções do art. 9.º do RGPD.

Será que estes dois fundamentos das categorias especiais de dados não são necessários para que os dados pessoais de trabalhadores, sobretudo os de caráter sensível, não tenham um maior reforço quando são tratados? E o consentimento, não é um fundamento de licitude válido para o tratamento de dados pessoais de trabalhadores?

Veremos, de seguida, a resposta a ambas as questões.

3.2. O afastamento do consentimento como fundamento de licitude válido no âmbito das relações laborais

O consentimento é um dos fundamentos de licitude previstos no art. 6.º do RGPD[66]. Porém, a sua definição apresenta várias particularidades que demonstram como este fundamento não é válido no âmbito das relações laborais.

A alínea 11) do n.º 1 do art. 4.º do RGPD, refere que o consentimento é uma manifestação de vontade, livre, específica, informada e inequívoca pela qual o titular aceita através de uma declaração ou ato positivo inequívoco, que os seus dados sejam objeto de tratamento.

Por sua vez, o consentimento só pode ser considerado válido, quando é oferecido ao titular uma verdadeira opção de aceitar ou recusar, sem que este saia prejudicado caso não aceite consentir o tratamento em questão[67]. O n.º 3 do art. 7.º do RGPD faz enfase a essa opção ao referir que o titular tem o direito de retirar o seu consentimento a qualquer momento, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado, estabelecendo que o mesmo deve ser tão fácil de retirar quanto de dar.

Ao debruçarmo-nos sobre as relações laborais, temos em linha de conta o vínculo existente entre o trabalhador e empregador. O art. 11.º do CT estabelece que o contrato de trabalho é aquele em que uma pessoa singular – trabalhador – se obriga, mediante uma retribuição, a prestar a sua atividade sob a autoridade de outrem – empregador. Ou seja, estamos perante uma relação em que se verifica a dependência económica do trabalhador face ao empregador, sendo esta marcada pela subordinação jurídica que resulta da relação entre as partes, demonstrando que estamos perante um desequilíbrio de poderes[68].

---

[66] Segundo a alínea a) do n.º 1 do art. 6.º do RGPD, o tratamento de dados pessoais só é lícito quando o titular dos dados tiver dado o seu consentimento para tal.

[67] GRUPO DE TRABALHO DO ARTIGO 29.º – *Orientações relativas ao consentimento na aceção do Regulamento 2016/679*, adotadas em 28 de novembro de 2017, última redação revista e adotada em 10 de abril de 2018. p. 3.

[68] SANTOS, Patrícia Andreia Batista e – *A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*. Lisboa: Faculdade de Direito da Universidade Nova de Lisboa, 2019, p. 61. Disponível em: https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf (acedido a 08.02.2024).

No entanto, o considerando 43 do RGPD refere que nas situações em que exista um desequilíbrio manifesto entre o titular e o responsável pelo tratamento, o consentimento não constitui um fundamento de licitude válido[69]. Além disso, o Parecer 2/2017 sobre o tratamento de dados pessoais no local de trabalho, reforça a invalidade do consentimento como fundamento de licitude ao referir que a base jurídica não pode e nem deve ser o consentimento do trabalhador, devido à natureza da relação entre as partes[70].

Na ordem jurídica nacional, o art. 28.º da Lei n.º 58/2019 estabelece que o consentimento do trabalhador não constitui um fundamento de licitude válido se o tratamento de dados pessoais estiver abrangido pela alínea b) do n.º 1 do art. 6.º do RGPD – ou seja, a execução do contrato de trabalho (alínea b) do n.º 3 do art. 28.º do presente diploma)[71].

Face à imposição prevista na legislação europeia e nacional no que toca ao âmbito de aplicação do consentimento, concluímos que este fundamento não pode ser aplicado no contexto em causa, por traduzir uma dependência e subordinação do trabalhador, que não se encontra em posição de conceder o seu consentimento nos termos exigidos pelo RGPD e pela Lei n.º 58/2019, sem que este não lhe cause qualquer tipo

---

[69] O RGPD retirou o acento tónico do consentimento como um fundamento de licitude válido para o tratamento de dados pessoais nas situações previstas no considerando 43, como o caso da relação entre trabalhador e empregador. O considerando 43 do RGPD torna-se relevante por demonstrar que o tratamento de dados pessoais de trabalhadores deve assentar em outros princípios que não o consentimento, para que o tratamento seja considerado válido (Cfr. MOREIRA, Teresa Coelho – *Direito do Trabalho na Era Digital*. Coimbra: Edições Almedina, 2021, p. 201).

[70] GRUPO DE TRABALHO DO ARTIGO 29.º – *Parecer 2/2017 sobre o tratamento de dados pessoais no local de trabalho*, adotado em 8 de junho de 2017, p. 7.

[71] A alínea a) do n.º 3 do art. 28.º foi uma das normas a ser desaplicada pela CNPD, por esta restringir excessivamente a relevância do consentimento do trabalhador, eliminando, deste modo, qualquer margem de livre-arbítrio dos trabalhadores mesmo nas situações em que a sua manifestação não apresenta nenhum risco para os seus direitos e interesses. Devido à restrição injustificada e desproporcionada da norma, a CNPD entendeu que a mesma não corresponde a uma medida legislativa nacional que salvaguarde a dignidade, os direitos fundamentais e o interesse legítimo do trabalhador, não cumprindo com os requisitos exigidos na alínea b) do n.º 2 do art. 9.º e do n.º 2 do art. 88.º do RGPD (Cfr. COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS – *Deliberação/2019/494 sobre a desaplicação, na apreciação de casos concretos, de algumas normas da Lei 58/2019* – N.º 4, p. 5).

de consequência[72] devido à desigualdade presente na relação entre as partes – trabalhador e empregador. Essa consequência pode verificar-se através da necessidade de o trabalhador obter o seu posto de trabalho, nos casos de candidatos a emprego, bem como na manutenção do seu atual posto[73], caso este impossibilite o empregador de tratar os seus dados pessoais.

Não obstante, podem existir situações em que o consentimento é considerado válido para o tratamento de dados pessoais de trabalhadores, sobretudo se o tratamento em causa for do interesse do próprio trabalhador[74], como é o caso do tratamento de imagem e voz do trabalhador no âmbito da divulgação interna e/ou externa da empresa.

3.3. A possível aplicação cumulativa do artigo 6.º e do n.º 2 do artigo 9.º do RGPD

Na prática, os fundamentos de licitude aplicados no contexto laboral são os que se encontram previstos no art. 6.º do RGPD – execução do contrato ou diligências pré-contratuais a pedido do titular; obrigação jurídica; e interesse legítimo do responsável pelo tratamento –, ficando de parte as exceções previstas no art. 9.º do RGPD, quando envolvem o tratamento de categorias especiais de dados. O que vem realçar o "peso" do art. 6.º do RGPD, nomeadamente, da execução do contrato como fundamento de licitude, por ser aquele que abrange a maioria das finalidades de tratamento previstas no âmbito laboral. Não obstante, não podemos excluir a aplicação das exceções do art. 9.º do RGPD.

Reintroduzindo a questão colocada anteriormente sobre a (possível) necessidade de aplicar o n.º 2 do art. 9.º do RGPD, quando se

---

[72] ALVES, Lurdes Dias – *Proteção de Dados no Contexto Laboral*. Coimbra: Edições Almedina, 2020, p. 58.

[73] MOREIRA, Teresa Coelho – *Direito do Trabalho na Era Digital*. Coimbra: Edições Almedina, 2021, p. 202.

[74] ALVES, Lurdes Dias – *Proteção de Dados no Contexto Laboral*. Coimbra: Edições Almedina, 2020, p, p. 60.

verifica o tratamento de categorias especiais de dados de trabalhadores, com o intuito de ter um maior reforço quando são alvo de tratamento, temos de ter em atenção duas situações: (i) o art. 6.º do RGPD abranger o tratamento de categorias "gerais" de dados e categorias especiais de dados, afastando a aplicação das exceções do art. 9.º do RGPD; e (ii) a possível aplicação cumulativa do art. 6.º e do n.º 2 do 9.º do RGPD.

Observando a primeira situação, reparamos que a maioria das autoridades de controlo europeias consideram que os fundamentos de licitude aplicados ao tratamento de dados pessoais de candidatos a emprego e trabalhadores se baseiam exclusivamente no art. 6.º do RGPD, nomeadamente na execução do contrato, obrigação jurídica e interesse legítimo do responsável, como é o caso da *Commision Nationale de L'informatique et des Libertés* (CNIL)[75] e da *Agencia Espanõla de Protección de Datos* (AEPD)[76]. A CNPD também segue a mesma lógica, dando um maior destaque à execução do contrato e obrigação jurídica[77].

Não obstante, analisando a segunda situação, encontramos outras autoridades de controlo, mais concretamente, a autoridade de controlo do Reino Unido – *Information Commissioner's Office* (ICO) –, que defende a aplicação cumulativa do art 6.º e do n.º 2 do 9.º do RGPD, nos casos em que ocorre o tratamento de categorias especiais de dados, sendo necessário identificar a condição de licitude prevista no art. 6.º do RGPD e a exceção do art. 9.º do RGPD[78].

---

[75] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS – *Référentiel relatif aux traitements de données à caractère personnel mis en oeuvre aux fins de gestion du personnel*, p. 5 – 6. Disponível em: <https://www.cnil.fr/sites/default/files/atoms/files/referentiel_grh_novembre_2019_0.pdf> (acedido a 10.02.2024).

[76] AGENCIA ESPANÕLA DE PROTECCIÓN DE DATOS – *La protección de datos en las relaciones laborales,* p. 8 – 9. Disponível em: <https://www.aepd.es/es/documento/la-proteccion-de-datos-en-las-relaciones-laborales.pdf> (acedido a 10.02.2024).

[77] Segundo a CNPD, o tratamento de dados pessoais de trabalhadores encontra-se previsto, na maior parte dos casos, através da legislação laboral e/ou da necessidade para a execução do contrato de trabalho entre as partes. Disponível em: <https://www.cnpd.pt/organizacoes/areas-tematicas/consentimento/> (acedido a 10.02.2024).

[78] Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> (acedido a 11.02.2024).

Face às duas situações apresentadas *supra*, constatamos que não existe um consenso entre as diferentes autoridades de controlo sobre o tema[79], deixando ao critério do responsável pelo tratamento – as empresas –, quais os fundamentos de licitude aplicados neste contexto, sendo o mais comum, a aplicação dos fundamentos de licitude previstos no art. 6.º do RGPD. Todavia, segundo as orientações do Grupo de Trabalho do Artigo 29.º, "os responsáveis pelo tratamento apenas podem tratar dados pessoais de categorias especiais se puderem satisfazer uma das condições estabelecidas no n.º 2 do art. 9.º, bem como uma das condições definidas no art. 6.º"[80]; ou seja, apesar das empresas aplicarem as condições previstas no art. 6.º do RGPD, podem igualmente aplicar as exceções do art. 9.º do RGPD, por estar em causa o tratamento de categorias especiais de dados.

Neste sentido, as categorias especiais de dados devem apresentar um maior reforço relativamente às categorias "gerais" de dados, por essa tipologia de dados, não poder, à partida, ser alvo de tratamento (n.º 1 do art. 9.º do RGPD).

Assim, verifica-se a necessidade de aplicar cumulativamente o art. 6.º e o n.º 2 do 9.º do RGPD quando estamos perante uma situação em que ocorra o tratamento de uma categoria especial de dados[81]. Por exemplo, durante a execução do contrato de trabalho, o trabalhador realiza exames de saúde no âmbito da medicina do trabalho, que resultam de uma obrigação legal prevista no Regime Jurídico da Promoção da Segurança e Saúde no Trabalho[82]. Apesar de o art. 6.º do RGPD

---

[79] SANTOS, Patrícia Andreia Batista e – *A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*. Lisboa: Faculdade de Direito da Universidade Nova de Lisboa, 2019, p. 52. Disponível em: https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf (acedido a 11.02.2024).

[80] GRUPO DE TRABALHO DO ARTIGO 29.º – *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679*, adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018, p. 16, *cit*.

[81] *Ibidem*.

[82] Segundo o n.º 1 do art. 108.º da Lei n.º 102/2009 (Regime Jurídico da Promoção da Segurança e Saúde no Trabalho), o empregador deve promover a realização de exames de saúde, de forma a comprovar e avaliar a aptidão física e psíquica do trabalhador para o exercício da sua atividade.

salvaguardar este tratamento, por se tratar de uma obrigação jurídica (alínea c) do n.º 1 do presente artigo), deve igualmente ser aplicado a alínea b) do n.º 2 do art. 9.º do RGPD por se tratar do cumprimento de uma obrigação jurídica e do exercício de um direito específico associado à relação laboral.

Conclusão

As diferentes fases do ciclo de vida do contrato de trabalho – pré-contratação; admissão do trabalhador; execução e cessação do contrato de trabalho –, demonstram um volume considerável de dados pessoais de candidatos a emprego e trabalhadores que são alvo de tratamento, estando estes distribuídos por diferentes finalidades e categorias de dados. A categorização dos dados pessoais – categorias "gerais" e especiais de dados – levantam algumas questões relativamente aos fundamentos de legitimidade no tratamento aplicados nas relações laborais. Isto deve-se ao facto de as categorias "gerais" de dados remeterem para o art. 6.º do RGPD e as categorias especiais de dados para o n.º 2 do art. 9.º do RGPD.

Esta distinção, como verificámos no presente trabalho, não é refletida na prática, por os fundamentos de licitude previstos no art. 6.º do RGPD – execução do contrato ou diligências pré-contratuais a pedido do titular; obrigação jurídica e interesse legítimo do responsável – cobrirem, de igual modo, as categorias especiais de dados. Não obstante, apesar de o consentimento constituir um dos fundamentos previstos no art. 6.º do RGPD, este não é considerado válido no âmbito das relações laborais devido ao desequilíbrio de poderes associado à relação entre trabalhador e empregador.

Neste sentido, existem diferentes autoridades de controlo a defenderem apenas a aplicação do art. 6.º do RGPD, mas também as que se opõem, por considerarem que as categorias especiais de dados

necessitam de um maior reforço face às restantes[83], defendendo a aplicação cumulativa do art. 6.º e do n.º 2 do art. 9.º do RGPD, nestas situações em concreto.

Devido ao facto de não existir consenso quanto à aplicação dos fundamentos de licitude neste âmbito, por parte das autoridades de controlo, o responsável pelo tratamento – neste caso as empresas – toma uma decisão justificando o tratamento com base na (i) execução do contrato; numa (ii) obrigação jurídica; e no (iii) interesse legitimo do responsável (alíneas b), c) e f) do n.º 1 do art. 6.º do RGPD).

Posto isto, constatamos que existe a necessidade de discutir a possibilidade de aplicar cumulativamente o art. 6.º e o n.º 2 do art. 9.º do RGPD, sobretudo, entre as várias autoridades de controlo, por o tema em questão, retratar duas categorias distintas de dados pessoais, em que uma delas – categorias especiais de dados – necessita de uma maior proteção de forma salvaguardar os direitos e liberdades dos candidatos a emprego e trabalhadores.

[83] Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> (acedido a 16.02.2024).

O Anuário da Proteção de Dados é uma revista jurídica de livre acesso, disponível em linha no sítio https://protecaodedadosue.cedis.fd.unl.pt, que pretende divulgar estudos doutrinários sobre o direito da proteção de dados pessoais. O Anuário é editado desde 2018 pelo Observatório da Proteção de Dados Pessoais, um grupo de investigação criado em 2016 no CEDIS – Centro de I&D sobre Direito e Sociedade da NOVA School of Law. Aberto a qualquer interessado, o Observatório integra atualmente catorze investigadores (quatro doutorados) oriundos de faculdades de direito (professores e doutorandos), de empresas e do setor público.

JURIS NOVA
DataporEU
SRS ADVOGADOS FOCUS MATTERS.
FUTURA