ANUÁRIO
DA PROTEÇÃO DE DADOS
2025

COORDENAÇÃO
FRANCISCO PEREIRA COUTINHO
GRAÇA CANTO MONIZ

CEDIS
CENTRO DE I&D SOBRE DIREITO E SOCIEDADE

ANUÁRIO
DA PROTEÇÃO DE DADOS
2025

ANUÁRIO
DA PROTEÇÃO DE DADOS
2025

COORDENAÇÃO
FRANCISCO PEREIRA COUTINHO
GRAÇA CANTO MONIZ

CEDIS
CENTRO DE I&D SOBRE DIREITO E SOCIEDADE

ANUÁRIO DA PROTEÇÃO DE DADOS 2025
Ano 8 – 2025

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: 75 exemplares

Outubro, 2025
ISSN 2184-5468

Catalogação na Publicação
Pereira Coutinho, Francisco e Canto Moniz, Graça (coord.). Anuário da Proteção de Dados 2025. Lisboa: CEDIS, 2025.

Índice

I – ARTIGOS

II – COMENTÁRIOS DE JURISPRUDÊNCIA/NOTAS DE INVESTIGAÇÃO

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 oito artigos publicados na edição de 2025 do Anuário resultam de uma chamada lançada em setembro de 2024 no sítio da internet do Observatório da Proteção de Dados Pessoais. Os textos foram depois sujeitos a um processo de *blind peer review* e posteriormente revistos pelos coordenadores do Anuário. Aos autores foi permitido escreverem de acordo com a nova ou a antiga grafia.

O Anuário inicia-se com um texto da autoria do André Feiteiro sobre o consentimento no tratamento de neurodados, seguindo-se um artigo da Camila Zanatta que trata o tema dos algoritmos e da transparência numa perspetiva de direito comparado. A tutela jurisdicional das ações propostas para reagir às decisões sancionatórias da CNPD é tratada pela Diana Camões. De seguida, a Elodie Beco debruça-se o interesse legítimo enquanto fundamento de licitude dos tratamentos de dados pessoais. O Jacob Bourgault apresenta o tema da vigilância em larga escala comparando os regimes vigentes nos Estados Unidos da América, no Reino Unido e em França e, por fim, a Maria Miguel Rios escreve sobre as decisões do Tribunal de Justiça da União Europeia e o seu impacto no regime das transferências de dados pessoais. Pela

primeira vez, este número do Anuário inclui uma secção dedicada a comentários de jurisprudência que conta com os contributos do Francisco Arga e Lima e da Moa Hedlund.

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, Domingos Farinho, Giovan Saavedra, Inês Oliveira, Joel Alves, Samo Bardutzki, Sebastião Barros Vale, Tiago Branco da Costa e Vinicius Mozetic. Por fim, agradecemos à Elodie Beco o auxílio prestado na edição do Anuário, bem como a todos os autores que nela participam.

Lisboa, 27 de agosto de 2025

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

I – ARTIGOS

A hipótese de limitar a prestação de consentimento para o tratamento de neurodados

André Feiteiro [1]

Sumário: Coloca-se a hipótese, neste estudo, de que viabilização tecnológica dos meios de recolha e tratamento de neurodados fora do contexto de diagnóstico e tratamento médico permitirá recolher e tratar dados pessoais identificáveis com o pensamento e consciência humana. Neste estudo, exploram-se fundamentos contra a possibilidade de afastar a proibição do art.º 9.º, n.º 1, do RGPD, mediante a prestação de consentimento pelo titular dos dados como fundamento legítimo para o tratamento daquele tipo de neurodados, por lhes aproveitarem normas que previnem a limitação voluntária de direitos de personalidade.

Abstract: In this paper, it is proposed that innovation in the collection and processing of neurodata outside of the medical diagnosis and treatment will enable the collection and processing of data related to human thought and consciousness. In this paper, reasons are explored to reject the possibility to provide consent as legitimate grounds to process that type of neurodata and as a means to overcome the prohibition of Article 9(1), GDPR, considering that limitations on waiver of personal rights should also apply in the context of the collection and processing of this type of neurodata.

Palavras-chave: neurodados; categorias especiais de dados; consentimento; direitos de personalidade; limitação voluntária

---

[1] Advogado. LL.M. International Business Law pela Tilburg University, 2018. Lic. pela Faculdade de Direito da Universidade de Lisboa, 2016. ORCID: 0000-0003-4412-2977.

Keywords: neurodata; special categories of data; consent; personal rights; voluntary waiver

1 Introdução

A economia do presente estudo aconselha-nos a sinalizar imediatamente o problema: o regime de proteção reforçada aplicável à recolha e tratamento de categorias especiais de dados pode não tutelar suficientemente a recolha e tratamento de dados pessoais que dizem respeito a processos da consciência humana. Isto é assim, uma vez que o regime das categorias especiais de dados do art. 9.º do RGPD[2] parece (em potência) revelar-se incapaz de acompanhar o desenvolvimento dos meios de captura de informação sobre o pensamento e consciência, comprometendo, assim, elementos essenciais do sujeito titular dos dados, desde logo a liberdade psicológica e liberdade e reserva de pensamento[3-4]. Esta conclusão preliminar não ignora o entendimento de que os neurodados encontram, hoje, correspondência nos dados pessoais relativos à saúde e dados biométricos[5]. Esta é, contudo, uma reflexão

---

[2] Regulamento (UE) n.º 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) (doravante, neste estudo, RGPD).

[3] Não se pretende, aqui, tomar posição sobre se a dignidade da pessoa humana está condicionada à aquisição e manutenção de consciência, tema que merece desenvolvimento próprio. Pretende-se, apenas, sinalizar que a liberdade psicológica e reserva de pensamento são elementos indissociáveis do (e imprescindíveis ao) sujeito titular de direitos.

[4] O Tribunal Europeu dos Direitos Humanos (TEDH) considerou a liberdade de pensamento, consciência e religiosa prevista no art. 9.º da Convenção Europeia dos Direitos do Homem como uma das fundações de uma sociedade democrática. *Nolan and K. v. Russia*, n.º 2512/04, 12 de fevereiro de 2009.

[5] Autoridade Europeia para a Proteção de Dados (EPDS), *TechDispatch #1/2024 – Neurodata*, https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2024-06-03-techdispatch-12024-neurodata_en, consultado a 6 de agosto de 2025. Ainda, Global Privacy Assembly, 46th Closed Session of the Global Privacy Assembly – Resolution on principles regarding the processing of personal information in neuroscience and neurotechnology, https://globalprivacyassembly.org/wp-content/uploads/2024/11/Resolution-on-Neurotechnologies.pdf, consultado a 6 de agosto de 2025.

sobre potenciais implicações futuras caso o desenvolvimento tecnológico venha a traduzir-se num suficiente aprofundamento da técnica de captura e leitura da atividade cerebral do ser humano.

A *pessoa* é objeto de estudo em disciplinas muito variadas. Dos avanços nas ciências naturais, em particular nas neurociências, brotam, em medida semelhante, novas implicações na pessoa sujeito-agente do Direito. Resultado desses avanços, a par do desenvolvimento técnico que permite aceder a espaços mais profundamente interiores, também a tutela jurídica passa a incluir realidades menos tangíveis aos sentidos e mais próximas ao *ser*.

Os direitos subjetivos, que são uma construção viva, sensíveis ao tempo e ao espaço[6], justificam o deslocamento dos limites do Direito para proteção de bens jurídicos cujas fronteiras estão, também elas, em movimento. Não se trata de uma mudança no conceito de justiça, mas antes de um alargamento do que é concebido como *direito*. O que entendemos como *sujeito* justifica, hoje, contornos distintos daqueles que inicialmente justificavam a configuração de um direito subjetivo: o tempo e o espaço que nos são contemporâneos são determinantes; os fundamentos alteram-se à medida que evoluem os meios técnicos. No que diz respeito aos direitos de personalidade, a reconfiguração do seu conteúdo e funções é resultado de alterações profundas no contexto histórico, social e cultural[7]. A título de exemplo, na Itália e Alemanha da primeira metade do século XX, os direitos de personalidade não eram entendidos como atribuições intangíveis da pessoa

---

[6] Ascensão, José de Oliveira, *Direito Civil Teoria Geral*, I, 2.ª edição, Coimbra, Coimbra Editora, 2000, p. 73. O autor sublinha isto mesmo sob a epígrafe "O nosso tempo", num tempo ainda longe de conhecer o tempo tão particular que é o nosso contemporâneo.

[7] Sobre o Direito como "realidade existencial", que é produto, muitas vezes, de frágeis contingências históricas e culturais, e, em particular, os direitos de personalidade como realidades condicionadas histórica, cultural e cientificamente, *vide* Messinetti, Davide / Di Ciommo, Francesco, "Diritti della personalità" em *Diritto Civile*, coord. Martuccelli, Silvio / Pescatore, Valerio, Milano, Giuffré Editore, 2011, pp. 601 e 602, e, também, Menezes Cordeiro, António, *Tratado de Direito Civil Português*, I, Tomo III, 2.ª edição, Coimbra, Almedina, 2007, p. 44.

humana, mas como posições jurídicas funcionais ao serviço do supremo interesse do Estado[8].

O redimensionamento da tutela jurídica não é necessariamente uma dinâmica extroversa, ou seja, partindo do indivíduo para elementos que lhe são exteriores. Do direito de propriedade, permissão específica de aproveitamento de um bem[9] exterior ao indivíduo e que com ele não se confunde, partimos, no passado, para a proteção de outros bens jurídicos, mais próximos e até confundíveis com o próprio titular, como o bom nome, a reserva da intimidade privada, ou a liberdade de criação artística, por exemplo. A dinâmica, nestes casos, é introversa[10]. Também os dados pessoais, e, em particular, os neurodados[11], são parte desta trajetória de rearranjo das fronteiras da tutela jurídica[12].

A descodificação de processos cognitivos conscientes e inconscientes é, ainda, um desafio técnico por ultrapassar[13]. A este desafio

---

[8] Messinetti, Davide / Di Ciommo, Francesco, *op. cit.*, p. 601. Ajuda à construção da ideia de tutela jurídica viva, a sugestão dos autores de que a inclusão dos direitos de personalidade no *Codice Civile* italiano de 1942 de forma exígua se explica pelo facto de, naquele momento histórico, o indivíduo não sentir ameaçadas, por exemplo, a sua intimidade e reserva privada, nem temer o tratamento ilícito de dados pessoais ou agressões à identidade pessoal. A afirmação dos direitos de personalidade como os conhecemos hoje, adiantam os autores, tem causa na afirmação das sociedades industrial e pós-industrial, em particular a difusão dos meios técnicos próprios dos tempos atuais.

[9] Menezes Cordeiro, António, *Tratado de Direito Civil*, vol. I, 4.ª edição, Coimbra, Almedina, 2016, p. 896.

[10] Menezes Cordeiro, António, *Tratado de Direito Civil*, vol. XIII, 1.ª edição, Coimbra, Almedina, 2022, p. 344. A construção do direito subjetivo deve, nas palavras do autor, "a sua ontologia histórico-dogmática à figura da propriedade". Para uma resenha breve do caminho dogmático entre a construção do direito de propriedade e as propostas de direitos subjetivos de personalidade decalcados daquele direito de propriedade, em especial a explicação de que os direitos de personalidade assentam na construção de "direitos sobre si próprio", vide Menezes Cordeiro, António, *Tratado de Direito Civil Português*, vol. I, tomo III, 2.ª edição, Coimbra, Almedina, 2007, pp. 50 a 54.

[11] Sobre o que entendemos por neurodados, na tentativa de os definir para efeitos do presente estudo, remetemos para a secção 2 deste estudo.

[12] Bublitz, Jan Christoph, "Freedom of Thought in the Age of Neuroscience: A Plea and a Proposal for the Renaissance of a Forgotten Fundamental Right", *Archiv für Rechts- und Sozialphilosophie*, vol. 100, 1, 2014. A este respeito, o autor bem aponta que a importância da liberdade de pensamento, que é muita, contrasta com a sua relevância prática, que, até muito recentemente, era pouca, na medida em que não se equacionavam meios que pudessem constranger efetivamente essa liberdade de pensamento.

[13] Naddaf, Miryam, *Brain-reading device is best yet at decoding 'internal speech'*, https://www.nature.com/articles/d41586-024-01424-7, consultado a 13 de dezembro de 2024. O texto

seguir-se-á um dilema ético, que, dependendo da viabilidade técnica, não é menos importante. As neurotecnologias atualmente disponíveis, em particular as tecnologias não-invasivas, estão, ainda, aquém do que se pode vir a ter como autêntica leitura do pensamento, permitindo apenas inferir processos cognitivos, através de padrões de ativação da atividade cerebral[14]. Por isto, é nosso dever descartar apelos éticos exagerados relacionados com os avanços nas neurotecnologias[15]. Não se pretende hiperbolizar riscos que só podemos conceber, hoje, como hipóteses de futuro não confirmadas, ainda que tenhamos já sugestões concretas de que esses riscos existem. Mantemos, sem prejuízo, que a reflexão sobre limites à intromissão (ainda que futura) é relevante, ainda que pareça distante ou irrealizável uma tecnologia que permita capturar com suficiente fiabilidade o pensamento humano.

A descodificação daqueles processos pressupõe que seja possível estabelecer correlação entre atividade cerebral e o mundo objetiva e cientificamente observável. As neurotecnologias[16] procuram reconhecer

---

remete para o estudo "Representation of internal speech by single neurons in human supramarginal gyrus" da autoria de Sarah K. Wandelt, David A. Bjånes, Kelsie Pejsa, Brian Lee, Charles Liu e Richard A. Andersen, publicado em 2024. Nele, os autores referem que "[e]mbora se tenham registado avanços importantes na decodificação de discurso vocalizado, tentado ou mimetizado, resultados relativos à descodificação de discurso interno são escassos e ainda não atingiram funcionalidade elevada" (tradução nossa). Wandelt, Sarah K. / Bjånes, David A. / Pejsa, Kelsie et al., "Representation of internal speech by single neurons in human supramarginal gyrus", *Nature Human Behaviour*, 8, 2024, pp. 1136-1149.

[14] Ienca, Marcello / Fins, Joseph J. / Kellmeyer, Phillip et al., "Towards a Governance Framework for Brain Data", *Neuroethics*, vol. 15, 20, 2022.

[15] Gilbert, Frederic / Russo, Ingrid, "Neurorights: The Land of Speculative Ethics and Alarming Claims?", *AJOB Neuroscience*, vol. 15, 2, 2007, pp. 113-115.

[16] Definidas como o tipo de tecnologia que "permite observar ou modificar funções cerebrais" (tradução livre). Eaton, M. L. / Illes, J., "Commercialising cognitive neurotechnology – the ethical terrain", *Nature Biotechnology*, vol. 25, 4, 2007, pp. 393-397. Definidas, ainda, pela OCDE, como "os dispositivos e procedimentos usados para aceder, investigar, estudar, manipular ou emular a estrutura e funções dos sistemas neuronais", definição utilizada, também, pela UNESCO num relatório relevante sobre a utilização ética das neurotecnologias. OCDE, *Recommendation of the Council on Responsible Innovation in Neurotechnology*, https://legalinstruments.oecd.org/en/instruments/oecd-legal-0457, consultado a 1 de março de 2025. UNESCO, *Report of the International Bioethics Committee of UNESCO (IBC) on the ethical issues of neurotechnology*, https://unesdoc.unesco.org/ark:/48223/pf0000378724, consultado a 1 de março de 2025.

padrões de atividade cerebral para, daí, inferir conclusões, e à questão sobre se é possível descodificar o pensamento humano, a resposta é gradual e crescentemente afirmativa à luz de desenvolvimentos recentes[17-18].

---

[17] A título de exemplo, Wandelt, Sarah K. / Bjånes, David A. / Pejsa, Kelsie et al., *op. cit.*, pp. 1138-1145. Os autores alegam ter descodificado palavras pensadas (mas não verbalizadas) pelos sujeitos objetos de teste, apenas com recurso a monitorização da atividade cerebral através de implantação de microelétrodos. Os autores treinaram um BMI (*brain-machine interface*) na interpretação das palavras "battlefield", "cowboy", "python", "spoon", "swimming", "telephone", "nifzig" e "bindip". A cada participante foi pedido que pensasse as palavras apresentadas num ecrã. Num dos participantes foi possível descodificar com 79% de precisão, noutro apenas 23%, o que, de acordo com os autores, pode estar relacionado com a forma como diferentes pessoas processam o seu discurso interno. Também relevante, pelo potencial catalisador que tem a utilização de neurodados recolhidos relativos a um sujeito objeto de teste na descodificação da atividade cerebral de um outro sujeito, *vide* Ferrante, Matteo / Boccato, Tommaso / Ozcelik, Furkan et al., "Through their eyes: Multi-subject brain decoding with simple alignment techniques", *Imaging Neuroscience*, vol. 2, 2024, pp. 1-21. Como maior evidência de que a novas técnicas tem correspondido um aprofundamento da precisão e alcance, outros autores demonstram, recentemente, em 2024, que a aplicação de novas técnicas à descodificação da fala através da leitura da atividade cerebral permitiu um melhoramento de resultados na ordem dos 15-27% quando comparados com resultados da aplicação de técnicas anteriores. Jayalath, Dulhan / landau, Gilad / Shillingford, Brendan et al., "The Brain's Bitter Lesson: Scaling Speech Decoding With Self-Supevised Learning", *Proceedings of the 42nd International Conference on Machine Learning*, Vancouver, Canadá, p. 5. Já este ano, em 2025, a Meta anunciou resultados de pesquisa relativa à descodificação da fala através da atividade cerebral com precisão de até 80% dos caracteres. O anúncio está disponível em https://ai.meta.com/blog/brain-ai-research-human-communication/ e resume um estudo publicado pela equipa de pesquisa, que citamos, e que está disponível em https://ai.meta.com/research/publications/brain-to-text-decoding-a-non-invasive-approach-via-typing/ Lévy, Jarod / Zhang, Mingfang (Lucy) / Pinet, Svetlana et al., "Brain-to-Text Decoding: A Non-invasive Approach via typing", 10.48550/arXiv.2502.17480.

[18] A investigação relativa à descodificação da atividade cerebral não é nova. Em 2006, já se demonstrava ser possível reconstruir uma imagem visualizada pelo sujeito objeto de teste através da monitorização e interpretação da atividade cerebral, sem prejuízo da precisão e resolução dessa reconstrução serem, ainda, baixas. Thirion, Bertrand / Duchesnay, Edouard / Hubbard, Edward et al., "Inverse retinotopy: Inferring the visual content of images from brain activation patterns", *NeuroImage*, vol. 33, 4, 2006, pp. 1104-1116. Também relevante, em particular porque demonstra ser possível reconstruir imagens sem recurso a categorias ou classificações prévias, Miyawaki, Yoichi / Uchida, Hajime / Yamashita, Okito et al., "Visual Image Reconstruction from Human Brain Activity using a Combination of Multiscale Local Image Decoders", *Neuron*, vol. 60, 5, 2008, pp. 915-929. Como os autores referem, "[na] experiência da percepção cabe um vasto número de estados possíveis". O sucesso de investigação anterior à dos autores na tentativa de descodificação da atividade cerebral deve-se a métodos de previsão dos estados de perceção dos sujeitos objetos de teste, mediante a classificação da sua atividade cerebral em categorias pré-especificadas. Como indicam os autores, "[a] reconstrução de imagens visuais sem restrições [(sem recurso às tais categorias pré-especificadas)] é mais difícil, uma vez que não é prático especificar a atividade cerebral de entre todas as imagens possíveis". De forma mais genérica, para uma resenha do estado da arte em 2009, *vide* Kay, Kendrick N. / Gallant, Jack L., "I can see what you see", *Nature Neuroscience*, 12, 2009, pp. 245-246.

Na medida em que avançam os meios, crescem os riscos associados à sua utilização.

A noção de risco é muito relevante em matéria de proteção de dados. O risco de dano a bens jurídicos de maior importância justifica, por exemplo, um regime de proteção reforçada de dados pessoais enquadráveis nas categorias especiais de dados elencadas no n.º 1 do art. 9.º do RGPD[19]. Os avanços nos meios de recolha e tratamento de neurodados e das técnicas de previsão da cognição e comportamento humanos encontram os habituais riscos do tratamento de dados pessoais, mas, para lá dos riscos comuns ao tratamento de dados pessoais fora do âmbito do art. 9.º do RGPD[20], têm uma influência potencial na razoável expectativa de conservação da liberdade psicológica, reserva de pensamento e, indiretamente, no livre desenvolvimento da identidade dos titulares dos dados. Admitimos que a reserva interior é necessária ao desenvolvimento livre. Por isto, a viabilização dos meios técnicos exige um movimento equivalente da tutela jurídica que assegure um núcleo de proteção híper-reforçado, verdadeira garantia de um núcleo individual indisponível à semelhança do que acontece com outros direitos subjetivos, em particular, direitos de personalidade.

Hoje, os neurodados são dados pessoais relativos à saúde e estão protegidos através do regime aplicável às categorias especiais de dados do art. 9.º do RGPD. Isto resulta da interpretação ampla dada pelo TJUE a dados relativos à saúde, que inclui dados sobre estado físico e mental do titular dos dados[21_22]. Estuda-se a hipótese, no presente estudo, da

---

[19] Considerando 51) do RGPD, no qual se lê que "[m]erecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais".

[20] São riscos e vulnerabilidades partilhados entre todos os dados pessoais o risco de re-identificação, roubo, uso não autorizado, a vigilância, entre outros. Ienca, Marcello / Fins, Joseph J. / Kellmeyer, Phillip et al., "Towards…, *op. cit*.

[21] Tribunal de Justiça da União Europeia (TJUE), C-184/20, OT v Vyriausioji Tarnybines Etikos Komisija, 1 de agosto de 2022, parágrafo 124.

[22] A Information Commissioner's Office (ICO), autoridade competente no Reino Unido em

recolha e tratamento de neurodados em contextos que atribua aos neurodados uma significação que informa muito além dos dados relativos à saúde, ou outras categoriais especiais de dados, como a origem racial ou étnica, orientação sexual, genética, biometria, ou a saúde do titular dos dados. Coloca-se a hipótese de que a viabilização tecnológica de instrumentos e técnicas permita recolher e tratar dados pessoais identificáveis com o pensamento e consciência humana[23]. Sendo já evidente a vulnerabilidade do pensamento e consciência individuais ao dia de hoje, apenas por formas mediatas de influência, designadamente através da exploração, prospeção e análise preditiva de dados em áreas

matéria de proteção de dados, publicou um relatório sobre o impacto das neurotecnologias no campo da recolha e tratamento de dados pessoais. A secção "Regulatory Issues" é particularmente relevante ao identificar os riscos e inoperâncias concretas entre a recolha e tratamento de neurodados fora do contexto das categorias especiais de dados (designadamente o contexto clínico) e a lei aplicável em matéria de proteção de dados no Reino Unido. Information Commissioner's Office (ICO), *ICO tech futures: neurotechnology*, https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/ico-tech-futures-neurotechnology/, consultado a 1 de março de 2025.

[23] Wandelt, Sarah K. / Bjånes, David A. / Pejsa, Kelsie et al., *op. cit.*, pp. 1136-1149. Miyawaki, Yoichi / Uchida, Hajime / Yamashita, Okito et al., *op. cit.*, pp. 915-929. Para além daqueles estudos já citados, para uma compreensão geral do estado da arte e preocupações associadas ao desenvolvimento tecnológico aplicado à extração de informação relacionada com o pensamento e consciência humana, designadamente as preocupações em matéria de direitos fundamentais, *vide* Reveley, Fletcher, *Advances in Mind-Decoding Technologies Raise Hopes (and Worries)*, https://undark.org/2024/01/03/brain-computer-neurorights/?utm_source=join1440&utm_medium=emai, consultado a 16 de dezembro de 2024. Ainda, na mesma esteira, *vide* Powers, Benjamin, *Technology Melds Minds With Machines, and Raises Concerns*, https://undark.org/2020/04/22/brain-technology-interface/, consultado a 16 de dezembro de 2024. Amplamente citado, estabelecendo quatro prioridades éticas para o desenvolvimento e aplicação das neurotecnologias, *vide* Yuste, Rafael / Goering, Sara / Agüera y Arcas, Blaise et al., "Four ethical priorities for neurotechnologies and AI", *Nature*, vol. 551, 2017, pp. 159-163. Os autores explicam que a afirmação de prioridades éticas das neurotecnologias é condição para a sua introdução no mercado de consumo. Estas são a privacidade e o consentimento, a agência e identidade, capacitação (*augmentation*) e enviesamento (*bias*). Os autores entendem que a relação privacidade-consentimento é assegurada através de um mecanismo *opt out* que deve ser a escolha por defeito. Esta solução pressupõe, contudo, a possibilidade dos sujeitos titulares dos dados consentirem na recolha e tratamento (portanto, *opt in*). A Autoridade Europeia para a Proteção de Dados (*European Data Protection Supervisor*, EDPS) publicou um relatório relevante no qual se analisam os riscos inerentes à recolha e tratamento de neurodados em novos contextos. Neste relatório afirma-se, de início, que certos usos de neurodados compreendem riscos inaceitáveis para os direitos fundamentais. Autoridade Europeia para a Proteção de Dados (EPDS), *TechDispatch op. cit*.

como o comércio e a política[24], o titular dos dados dificilmente se concebe como associal, mas como permeável em toda a linha[25]. Inserido num contexto em que as escolhas informadas são, tendencialmente, escolhas decisivamente influenciadas, o reforço da proteção da informação sobre o que cada um sente ou pensa, assume o papel de salvaguarda da identidade do titular dos dados.

Este estudo coloca a hipótese de que aproveitam aos dados pessoais relativos à experiência subjetiva da consciência e aos processos objetivos conscientes ou inconscientes as normas que previnem a limitação voluntária de certos direitos de personalidade, e que, por isso, deve ser de afastar a possibilidade de levantar o regime de proibição do art. 9.º, n.º 1, do RGPD. Para tanto, será necessário, em primeiro lugar, definir neurodados e enquadrá-los nas diferentes categorias especiais de dados do art. 9.º do RGPD.

2 Os neurodados

A noção de identidade é relevante no contexto da proteção de dados pessoais. A noção de *privacy* não é adivinhada, mas construída ao longo

---

[24] Leal, Ana Alves, "Aspetos jurídicos da análise de dados na Internet (*big data analytics*) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação", *FinTech: Desafios da Tecnologia Financeira*, 2.ª edição, Almedina, 2019, pp. 89-220.

[25] Por um lado, sobre a má reputação da *privacy*, e sobre uma incapacidade generalizada de expor com suficiência a sua importância que resulta na derrota da *privacy* face a temas como a segurança nacional e a inovação tecnológica, e, por outro, sobre como central à *privacy* está não o sujeito por si só, mas o sujeito social, cultural e relacionado com os outros, *vide* Cohen, Julien E., "What privacy is for", *Harvard Law Review*, vol. 126, 2013, pp. 1904-1907. As incursões do autor nos méritos da disciplina da *privacy* são relevantes: a *privacy* é um escudo que protege a subjetividade de esforços alheios, sejam comerciais ou governamentais, de "fixar, prever e ver através" do conjunto das subjetividades, protegendo assim a autodeterminação individual. Nas palavras do autor, o sujeito que beneficia da *privacy* não é o sujeito autónomo, a ilha pré-cultural que o modelo liberal presume ser. Ainda, sobre como as novas tecnologias que se alimentam de dados colocam uma séria ameaça à autonomia do pensamento e à liberdade interior, e, no âmbito de outros campos de estudo, sobre como essa reserva interior e a capacidade de pensar livremente são fundamentais à democracia e à dignidade e identidades individuais, *vide* Alegre, Susie, *Freedom to Think – Protecting a Fundamental Human Right in the Digital Age*, Londres, Atlantic Books, 2023.

do tempo até à definição funcional de privacidade como controlo sobre a informação, nos termos da qual a *privacy* "é o direito dos indivíduos, grupos, ou instituições, de determinarem quando, como e em que medida a informação sobre os próprios é comunicada aos outros"[26-27]. Esta definição é especialmente funcional na sociedade da informação, mas o desenvolvimento técnico dos meios pelos quais se obtêm dados pessoais, designadamente a obtenção de dados pessoais através de neurotecnologias, sugere-nos que recuperemos uma outra definição possível de *privacy*, economicamente menos funcional, mas mais identitária: "a liberdade de construção de uma identidade individual sem constrangimentos irrazoáveis"[28]. Reconhecemos, em potência, estes constrangimentos na recolha e tratamento de neurodados, importando defini-los como objeto do presente estudo.

Os neurodados podem definir-se como os dados pessoais relativos à atividade cerebral de um indivíduo obtidos por qualquer meio que permita registar diretamente a atividade fisiológica do cérebro. Esta definição não passa de uma definição funcional: é uma definição interessada, sobretudo, nos meios mediante os quais os dados pessoais são recolhidos[29], muito à semelhança, aliás, do que fez o legislador europeu

---

[26] Westin, Alan F., *Privacy and Freedom*, IG Publishing, 2018, p. 24. A obra é publicada pela primeira vez em 1967.

[27] A tríade *privacy*, privacidade e proteção de dados não são conceitos equivalentes. Para efeitos do presente estudo, referimo-nos a *privacy* como conceito dialogante com a dogmática da proteção de dados pessoais. Sobre as diferenças entre os conceitos, bem como a evolução histórica da *privacy* norte-americana, *vide* Pinheiro, Alexandre Sousa, *Privacy e Proteção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, AAFDL, Lisboa, 2015, pp. 267 e seguintes. Para uma comparação entre os conceitos *privacy* e proteção de dados, anterior ao RGPD, da autoria da, à data, Advogada-Geral do Tribunal de Justiça da União Europeia (TJUE) Juliane Kokott, *vide* Kokkot, Juliane / Sobotta, Christoph, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", *International Data Privacy Law*, vol. 3, n.º 4, 2013, pp. 222-228.

[28] Agre, Philip E. / Rotenberg, Marc, *Technology and Privacy: The New Landscape*, The MIT Press, Cambridge, Massachussetts, 1997, p. 7.

[29] Estão disponíveis outras definições. A título de exemplo, a Autoridade Europeia para a Proteção de Dados (EDPS) define neurodados como "informação recolhida do cérebro e/ou do sistema nervoso" (tradução livre). Esta definição parece-nos ter, contudo, pouca profundidade. Autoridade Europeia para a Proteção de Dados (EDPS), *TechDispatch* …, *op. cit.* Ainda, a definição de neurodados oferecida pela Global Privacy Assembly como "dados relativos ao

com a definição de dados biométricos.

Em primeiro lugar, os neurodados são *dados pessoais*, na medida em que correspondem a informação relativa a uma pessoa singular identificada ou identificável nos termos do art. 4.º, parágrafo 1) do RGPD. O Considerando 26) ajuda neste exercício: uma pessoa singular é identificável, se considerarmos o universo dos meios suscetíveis de serem utilizados pelo responsável pelo tratamento ou por outra pessoa, para identificar a pessoa singular, e, para além disso, se há uma probabilidade razoável de os meios utilizados identificarem a pessoa singular, considerados fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados.

Em segundo lugar, os neurodados são *dados pessoais relativos à atividade cerebral de um indivíduo*, na medida em que, por um lado, a atividade fisiológica do cérebro pode ser medida, de entre outras formas, através do registo das oscilações da atividade elétrica e do nível de oxigenação da corrente sanguínea nas diferentes regiões do cérebro – através da eletroencefalografia[30] e magnetoencefalografia[31], respetivamente, a título de exemplo.

Em terceiro lugar, são neurodados aqueles que, sendo relativos à atividade cerebral de um indivíduo, são *obtidos por qualquer meio que permita registar diretamente a atividade fisiológica do cérebro*. A noção de apreensão direta é relevante: não serão, para este efeito, neurodados as informações obtidas mediante observação indireta daquela atividade,

---

funcionamento, atividade ou estrutura do cérebro humano de um indivíduo que inclua informação única sobre a sua fisiologia, saúde, ou estados mentais que permitam a sua identificação ou o torne identificável" (tradução nossa). Global Privacy Assembly, 46th Closed Session … *op. cit*.

[30] Nuñez, Paul L. / Srinivasan, Ramesh, *Electrical Fields of the Brain: The Neurophysics of EEG*, Oxford University Press, Nova Iorque, 2006, p. 3. Os autores definem a eletroencefalografia como o registo das oscilações dos potenciais elétricos no escalpe humano.

[31] Baillet, Sylvain, "Magnetoencephalography for brain electrophysiology and imaging", *Nature Neuroscience*, vol. 20, n.º 3, 2017, p. 327. As correntes eletroquímicas que circulam nos e entre os neurónios produzem indução magnética, que é captada numa MEG. Em maior detalhe, *vide* Hämäläinen, Matti / Hari, Riitta / Ilmoniemi, Risto et al., "Magnetoencephalography: theory, instrumentation and applications to the noninvasive study of human brain function", *Review of Modern Physics*, vol. 65, n.º 2, 1993, 416.

de que são observáveis o comportamento, capacidades motoras, ou externalizações do arbítrio de um indivíduo, mas sim, e apenas, os dados obtidos através de neurotecnologias disponíveis. Destacam-se, hoje, e entre outras, a eletroencefalografia, a magnetoencefalografia, e a ressonância magnética funcional[32], que permitem apreender atividade cerebral independentemente da sua expressão exterior, como o comportamento, as capacidades motoras, ou externalizações do arbítrio de um indivíduo.

Muito relevante é, também, a ideia de que os dados têm correspondência com a atividade cerebral: aqui excluímos técnicas de radiografia, porque a informação extraída, nestes casos, é estática e limita-se à densidade dos tecidos; não diz respeito, portanto, à atividade cerebral com um mínimo de continuidade.

A fatalidade de que o comportamento humano tem por referência processos conscientes e inconscientes que têm lugar no cérebro é partilhada entre todos nós. Sujeitas ao meio envolvente, as ações e omissões de um sujeito estão intimamente ligadas à sua atividade cerebral. É sabido, hoje, que este fenómeno é observável através dos instrumentos e técnicas certas[33]. Interessam-nos aquelas capazes de registar os fenómenos constantes (o registo do filme, por oposição à fotografia), designadamente a eletroencefalografia e a magnetoencefalografia (doravante EEG e MEG, respetivamente), a ressonância magnética funcional (em língua inglesa, e mais comummente conhecida por fMRI, doravante RMf).

---

[32] Hallinan, Dara / Schütz, Philip / Friedewald, Michael et al., "Neurodata and Neuroprivacy: Data Protection Outdated?", Surveillance & Society, vol. 12, n.º 1, 2014, pp. 55-72. Os autores definem neurodados como um conjunto de dados que descrevem *diretamente* o funcionamento do cérebro humano. Ainda que publicado durante a vigência da Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, que antecedeu o RGPD, aborda temas relevantes ao presente estudo, designadamente a proximidade dos neurodados e a identidade, a diferença entre dados que resultam de externalizações e dados recolhidos sem mediação ou filtro, o caso dos neurodados, e a aparente desadequação do regime jurídico aplicável à tutela da recolha e tratamento de neurodados.

[33] Cfr. notas de rodapé 16, 17 e 22.

A física e análise associadas à neuroimagiologia são complexos. O objetivo deste estudo não é oferecer uma visão detalhada sobre conceitos estudados pelas ciências naturais, mas apenas introduzir esses conceitos de forma que a problemática (que exige multidisciplinariedade) possa ser suficientemente compreendida pelo leitor. As técnicas de neuroimagiologia estão amplamente (e são permanentemente) estudadas em grande profundidade, de que daremos nota por meio de citação, não exaustiva, mas na medida do que entendamos relevante para a compreensão jurídica do problema.

3 As principais técnicas de recolha de neurodados

O EEG e o MEG procuram extrair uma imagem da atividade cerebral através do registo e medição dos potenciais elétricos e dos campos magnéticos no cérebro durante um determinado período, respetivamente. Estas técnicas são utilizadas, sobretudo, em pré-cirurgia, diagnóstico de epilepsia, patologias funcionais, trauma, lesões vasculares cerebrais, perturbações do sono, entre outras[34]. A análise clínica traduz a informação recolhida em padrões clínicos, uma vez que as imagens não valem por si e requerem interpretação contextualizada, a interpretação clínica.

A MEG realiza-se com recurso a *scanners* de grande dimensão, que lhe conferem menor agilidade e viabilidade como meio de seguimento contínuo da atividade cerebral[35]. Evidência da maior

---

[34] Teplan, Michal, "Fundamentals of EEG measurement", Measurement Science Review, vol. 2, n.º 2, 2002. Fred, A.L. / Kumar, S.N. / Kumar Haridhas, A. et al., "A Brief Introduction to Magnetoencephalography (MEG) and Its Clinical Applications", Brain Sciences, vol. 12, n.º 6, 2022, p. 788.

[35] De entre as várias limitações logísticas características da MEG, há que considerar que a MEG deve ser realizada numa sala com isolamento próprio, de modo que o magnetismo de outros aparelhos não interfira na recolha de imagem cerebral, e que os equipamentos tradicionais têm componentes que requerem refrigeração, o que ajuda a explicar o tamanho destes aparelhos de medição. Boto, Elena / Meyer, Sofie S. / Shah, Vishal, et al. "A new generation of magnetoencephalography: Room temperature measurements using optically-pumped magnetometers", Neu-

agilidade do EEG são as eletroencefalografias ambulatórias, no âmbito das quais a atividade cerebral é monitorizada durante um período prolongado no decurso da sua rotina habitual. Dedicar-nos-emos, ainda neste estudo, e ainda que brevemente, às limitações das técnicas de neuroimagiologia – de cuja categoria fazem parte o EEG, a MEG, e a RMf –, pois o risco associado à recolha e tratamento de neurodados depende, primeiramente, de soluções para essas limitações.

A RMf é hemodinâmica: é a oxigenação da corrente sanguínea na proximidade das células nervosas no cérebro que permite detetar que regiões do cérebro estão especialmente ativas, e durante quanto tempo, durante a realização de uma determinada tarefa[36]. A obtenção de dados clínicos através de uma RMf é um processo delicado. As imagens de RMf são obtidas de forma contínua, alternando entre períodos de ativação e repouso, em número e duração suficientes que permitam um contraste esclarecedor entre a imagem neuronal em atividade e em repouso[37].

A tomografia computadorizada (vulgo, TAC) é uma técnica de diagnóstico que recorre a raios X para capturar uma imagem de cortes do cérebro, tipicamente utilizada em contexto clínico para avaliar a presença de tumores e outras lesões, hemorragias intracranianas, hidrocefalia, acidentes vasculares cerebrais, infeções, inflamações e

---

roImage, vol. 149, 2017, pp. 404-414.

[36] Jezzard, Peter / Toosy, Ahmed T., "Functional MRI", *MR Imaging in White Matter Diseases of the Brain and Spinal Cord*, Springer, Berlin, 2005, p. 93. Belliveau, John W. / Kennedy Jr., D. N. / McKinstry, R.C. et al., "Functional mapping of the human visual cortex by magnetic resonance imaging", *Science*, vol. 254, n.º 5032, 1991, p. 254. Ogawa, Seiji / Tank, David W. / Menon, Ravi et al. "Intrinsic signal changes accompanying sensory stimulation: Functional brain mapping with magnetic resonance imaging", *Proceedings of the National Academy of Sciences*, vol. 89, 1992, p. 5951. Kwong, Kenneth K. / Belliveau, John W. / Chesler, David A. et al. "Dynamic magnetic resonance imaging of human brain activity during primary sensory stimulation", *Proceedings of the National Academy of Sciences*, vol. 89, 1992, p. 5675.

[37] Belliveau, John W. / Kennedy Jr., D. N. / McKinstry, R.C. et al., *op. cit.*, p. 254. Em maior detalhe, mas explicado de forma compreensível ao leitor dedicado a temas fora das ciências naturais, vide Jones, Owen D / Buckholtz, Joshua W. / Schali, Jeffrey D. et al, "Brain Imaging for Legal Thinkers: A Guide for the Perplexed", *Stanford Technology Law Review*, vol. 5, 2009.

outros[38]. A tomografia por emissão de positrões (ou PET), por sua vez, é uma técnica de imagiologia que requer que ao sujeito em exame sejam administrados radionuclídeos, que são moléculas com um componente radioativo, sendo assim possível observar as concentrações daqueles radionuclídeos e as alterações nos processos metabólicos no cérebro que são, depois, interpretados clinicamente[39].

Constam como técnicas de neurimagiologia, ainda, a cintilografia (ou SPECT) e a ecografia transfontanelar, entre outros. Estas técnicas registam a anatomia do cérebro, mas, também, a sua atividade, dados de que se inferem diagnósticos e para os quais se procuram soluções médicas, mas cujos limites não são, necessariamente, os clínicos[40].

4 A significação dos neurodados

Da utilização destas técnicas de neuroimagiologia, extrai-se informação em bruto que se enquadra no conceito de neurodados que adiantámos anteriormente. Os dados recolhidos correspondem a informação relativa à atividade cerebral de um indivíduo identificado ou identificável obtida por um meio que permitiu registar diretamente a atividade fisiológica do cérebro humano. Ainda que sejam dados pessoais, estes dados são, contudo, dados pessoais em bruto. A distinção entre dados em bruto e outro tipo de dados é de extrema importância: os dados não são, por si só, informação com significado; nem todas as

---

[38] Das, Manasmita, *Neuroimaging Techiniques and What a Brain Image Can Tell Us*, https://www.technologynetworks.com/neuroscience/articles/neuroimaging-techniques-and-what-a--brain-image-can-tell-us-363422, consultado a 18 de janeiro de 2025.

[39] Das, Manasmita, *Neuroimaging*, *op. cit*.

[40] Chekroud, Adam M. / Everett, Jim A. C. / Bridge, Holly et al., "A review of neuroimaging studies of race-related prejudice: does amygdala response reflect threat?", *Front. Hum. Neurosci.*, vol. 8, n.º 179. Os autores concluem que é possível estabelecer uma correlação entre grupos de pessoas e atividade da amígdala, no sentido de o sujeito a exame conceber preconceituosamente determinados grupos de pessoas, na medida em que esses grupos sejam concebidos por esse sujeito como uma ameaça potencial.

fontes de dados são fontes de informação ou conhecimento sobre um titular dos dados pessoais[41].

Melhor se entende a noção de dados em bruto quando é contraposta à de informação, isto é, dados que, uma vez tratados, ganham significado. Senão vejamos: as medições a que aludimos são fontes de dados com uma dimensão puramente fisiológica. Estes dados não passam de indicadores de variações elétricas ou magnéticas no cérebro, ou fluxos sanguíneos nesta parte do corpo humano, e correspondem, no caso do EEG, por exemplo, a indicadores de frequência elétrica da atividade cerebral em diferentes estados do indivíduo, como o sono, o relaxamento ou o estado de alerta em diferentes faixas de frequência[42]. Estes dados em bruto correspondem a uma representação neutra de um facto[43].

Uma vez interpretados os dados em bruto, depreende-se a natureza multinível dos neurodados: da interpretação de um ou mais indicadores em bruto podem extrair-se informações sobre o estado ou condição física ou psicológica do titular dos dados. A este nível, os neurodados ganham significado: a medição de determinada frequência nada diz sobre o indivíduo, por si só, mas a interpretação dos potenciais elétricos na frequência *theta* medida através de um EEG pode sugerir depressão e ansiedade, ou relaxamento e intuição[44].

Aos dados carecidos de interpretação falta-lhes significado: se lidos, mas não interpretados, os dados são neutros; se interpretados (portanto, tratados), são dados pessoais inseridos numa categoria especial

---

[41] Leal, Ana Alves, "Aspectos jurídicos …, *op. cit.*, p. 107-108. A autora refere-se a este tipo de dados desprovidos de significação como meras representações neutras de factos, que servem de matéria-prima a um conjunto de inferências. Estas últimas resultam, precisamente, do processamento e análise de dados em bruto.

[42] St. Louis, Erik / Frey, Lauren C., *Electroencephalography (EEG): An Introductory Text and Atlas of Normal and Abnormal Findings in Adults, Children and Infants*, Chicago, American Epilepsy Society, 2016, p. 9.

[43] Leal, Ana Alves, "Aspectos jurídicos …, *op. cit.*, p. 108.

[44] Herrmann, Ned, *What is the function of the various brainwaves?*, https://www.scientificamerican.com/article/what-is-the-function-of-t-1997-12-22/, consultado a 18 de janeiro de 2025.

de dados nos termos do art. 9.º, n.º 1, do RGPD[45]; se tratados para fins que não a interpretação clínica, prometem desvelar áreas de individualidade extrema.

No caso, a interpretação clínica confere aos neurodados um catalisador semelhante à linguagem. Temos na comunicação através da linguagem um meio falível, mas o mais experimentado e útil, de comunicar os nossos estados interiores ao outro; a linguagem como intermediário entre o sujeito e o seu interlocutor. Não é claro que venha a ser sempre assim.

A compreensão do que nos é revelado pelo outro é mediada pela linguagem, é certo. A comunicação, ou troca, entre dois sujeitos, tem lugar numa linguagem comum, um consenso entre ambos que permite assimilação. Isto não é dizer, contudo, que a linguagem como processo de compreensão do outro seja para sempre o único ou o melhor dos processos[46]. A linguagem é um meio de comunicação falível, seletivo e traiçoeiro, porque sujeito a construção linguística e interpretação; e é limitado, porque a velocidade a que o sujeito falante debita informação através da linguagem falada é manifestamente lenta[47]. Não

---

[45] Cfr. nota de rodapé 20.

[46] Rao, Rajesh P. N. / Stocco, Andrea / Bryan, Matthew et al., "A Direct Brain-to-Brain Interface in Humans", *PLoS ONE*, vol. 9, n.º 11, 2014. Os autores colocam a questão sobre se a informação disponível no cérebro de um sujeito pode ser transferida diretamente sob a forma de código neural para outro sujeito sem necessidade de recorrer à linguagem como meio de comunicação. A conclusão é de que é possível transmitir a informação extraída de um cérebro através de EEG a outro cérebro através de estimulação magnética transcraniana (TMS), permitindo assim que dois sujeitos utilizando apenas um *brain-to-brain interface* como canal de comunicação. O estudo é citado por Mark Digemanse, que contraria o otimismo de eventuais capacidades de comunicação desintermediadas, ou *brain-to-brain*. Digenmanse, Mark, *The space between our heads*, https://aeon.co/essays/why-language-remains-the-most-flexible-brain-to-brain-interface, consultado a 18 de janeiro de 2025.

[47] Se convertido o rácio de palavras por segundo em *bits* por segundo, o discurso falado atinge velocidades máximas de 40 a 60 bps. Reed, Charlotte M. / Durlach, Nathaniel I., "Note on Information Transfer Rates in Human Communication", *Presence: Teleoperators and Virtual Environments*, vol. 7, n.º 5, pp. 509–518. Como termo de comparação, tenha-se em conta, a título de exemplo, que, em Portugal, a velocidade de *download* em acesso fixo através de computador supera os 100 mbps em 50% dos casos, de acordo com dados da ANACOM, isto é, mais de um milhão e meio de vezes mais rápido do que a velocidade transferência de informação através da linguagem. Dados estatísticos disponíveis em https://netmede.pt/estatisticas. A promessa das técnicas *brain-to-brain* não está, contudo, necessariamente relacionada com a velocidade a que

faltam, portanto, incentivos para reformar os meios pelos quais nos expressamos.

Até ver, as vontades, opiniões e emoções requerem expressão, mas a expressão individual, feita em parte através da linguagem não se confunde com aquelas vontades, opiniões ou emoções: estas são objeto; aquela é mero expediente. Esta diferença é importante. A distinção entre o que pensamos e o que expressamos é uma fatalidade, porque, até ver, não nos foi possível transmitir o pensamento sem o entreposto da palavra (ou equivalente). Mas, para além de fatalidade, esse entreposto, que atrasa e descaracteriza o que de outra forma seria o mais puro pensamento, é uma garantia de existência de um núcleo pessoal irredutível e inacessível[48], e, portanto, uma condição indispensável à dignidade da pessoa humana, liberdade de pensamento e reserva da intimidade da vida privada.

Os filtros (o discurso, a expressão corporal, etc.) entre os estados interiores e o interlocutor conferem *controlo* ao titular dos dados, controlo que, como vimos, é um elemento definidor da noção moderna de *privacy*[49]. A privacidade está predicada na capacidade de conscientemente filtrar e reservar para si a informação[50]. O controlo da informação sobre si está assegurado ao titular através do domínio sobre *o que*, *quando*, e *como* comunica aos outros.

5 A insuficiência do enquadramento atual e proposta

O RGPD estabelece uma proibição específica de tratamento de dados pessoais considerados sensíveis, portanto enquadráveis em qualquer das categorias especiais de dados do n.º 1 do art. 9.º. Esta proibição, porque amplamente excecionada, funciona como um obstáculo ao

transmitimos e adquirimos informação. Não se espera que o desenvolvimento tecnológico neste campo permita acelerar conversas, ouvir várias conversas em simultâneo, ou compreender a informação conversada a uma velocidade significativamente mais rápida. A promessa está na precisão do que é transmitido, porque o pensamento já não seria peneirado pela escolha das palavras e sua interpretação pelo outro.

[48] Digenmanse, Mark, *The space between ..., op. cit.*

[49] Cf. nota 24.

[50] Ienca, Marcello / Fins, Joseph J. / Kellmeyer, Phillip et al., "Towards …, *op. cit.*

tratamento, não tanto como uma verdadeira proibição. O tratamento de neurodados é enquadrável em algumas categorias especiais de dados, o que não é dizer que aquele regime de proteção reforçada seja tutela bastante, perpetuamente.

Sem prejuízo do que concluímos adiante a respeito da hipótese de condicionar a possibilidade de prestação de consentimento para tratamento de neurodados fora do contexto clínico, a recolha e tratamento deste tipo de dados pessoais em contextos diversos daquele pacificamente aceite encontra obstáculos no próprio RGPD que podem, só por si, tornar inoperante a recolha e tratamento de neurodados em qualquer contexto que não seja o clínico.

Desde logo, o princípio de que a recolha e tratamento de dados pessoais devem ser adequados, pertinentes e limitados à finalidade não parece aproveitar à recolha e tratamento de quantidades imensas de neurodados de tal forma que não possa o responsável pelo tratamento razoavelmente demonstrar, nos termos do art. 5.º, n.º 2, do RGPD, aquela adequação, pertinência e limitação.

Quando durante a recolha de dados relativos a processos conscientes o titular dos dados partilha dados necessários e (involuntariamente) não necessários, a razoável demonstração da adequação, pertinência e limitação do tratamento pelo responsável pelo tratamento está, em princípio, comprometida, face à vastidão e imprevisibilidade dos dados que resultam de fluxos ininterruptos de pensamento e à própria incapacidade das neurotecnologias atuais discernirem quais os dados em relação aos quais foi prestado consentimento e aqueles para os quais não foi.

À hipótese de afastar o levantamento da proibição de tratamento de neurodados, interessam, sobretudo, fundamentos com aplicação no âmbito da autonomia privada do titular dos dados. No caso, interessa-nos o consentimento, conforme previsto no art. 6.º, n.º 1, alínea a), do RGPD. Os restantes fundamentos do tratamento lícito[51] situam-se fora

[51] O contrato, a obrigação jurídica, os interesses vitais, o interesse público e o interesse legítimo, conforme alíneas b) a f) do n.º 1 do art. 6.º do RGPD. Graça Canto Moniz, *Manual de Introdução à Proteção de Dados*, Coimbra, Almedina, 2024, 83-98.

do perímetro de escolha do titular dos dados, pelo que não podem ser estudados de uma perspetiva de limitação do exercício de direitos do titular de dados. Assim, tanto quanto releva para efeitos da presente análise, não se cumprindo os pressupostos do consentimento conforme estabelecido no RGPD, não há fundamento legítimo para a recolha e tratamento[52].

Para além disto, o tratamento de dados pessoais deve ser feito com exatidão[53], lealdade e transparência[54]. Neste sentido, não devem recolher-se ou tratar-se dados incorretos, e devem manter-se os dados atualizados. Novamente, não se afigura claro que a natureza dos processos conscientes e inconscientes permita cumprir estes requisitos do tratamento. Ao contrário da morada, do número de identificação fiscal, ou outros dados de natureza estática, os dados pessoais que traduzam o pensamento e consciência humana estão condenados a estarem desatualizados, porque o pensamento, estados emocionais, memória, cognição, etc., são inconstantes[55].

Não se afigura fácil concluir quanto à suficiência do regime de proteção reforçada daquele n.º 1 do art. 9.º, porque se, por um lado, conhecemos alguns tipos de dados pessoais que cabem na nossa noção de neurodados[56] e que são, hoje, pacificamente enquadrados naquele regime de proteção reforçada, por outro, a recolha e tratamento desses mesmos dados pessoais pode, em virtude da evolução dos meios técnicos, implicar um aprofundamento tal que a recolha e tratamento se tornem incompatíveis com a preservação simultânea de bens jurídicos

---

[52] Ienca, Marcello / Fins, Joseph J. / Kellmeyer, Phillip et al., "Towards …, *op. cit.*

[53] Art. 5.º, n.º 1, alínea d) do RGPD.

[54] Art. 5.º, n.º 1, alínea a) do RGPD.

[55] A Information Commissioner's Office (ICO), autoridade competente no Reino Unido em matéria de proteção de dados, sugere como princípio de solução que o responsável pelo tratamento trate os neurodados com base não em capturas únicas, mas num conjunto alargado que permita conhecer o fluxo de pensamento. Information Commissioner's Office (ICO), *ICO …, op. cit.* Para um estudo relevante sobre as alterações no cérebro que ocorrem com o envelhecimento, vide Peters, Ruth, "Ageing and the brain", *Postgraduate Medical Journal*, vol. 82, n.º 964, pp. 84–88.

[56] Cf. secção 2.

de personalidade vitais à conservação da dignidade individual dos titulares dos dados[57].

As conclusões sobre a suficiência da aplicação do atual regime de proteção reforçada aos neurodados carecem, portanto, do contexto em que aqueles dados pessoais são recolhidos e tratados. A recolha e tratamento de neurodados em contexto clínico, tal como o conhecemos hoje, é pacificamente aceite, porque o estado da arte, a escala dos meios técnicos, e, não de somenos, o objetivo da recolha e tratamento naquele contexto torna virtualmente inexistente o risco de que aquelas recolha e tratamento extravasem o contexto pacificamente aceite da recolha e tratamento para efeitos de prestação de cuidados ou tratamentos de saúde, conforme excecionado nos termos do art. 9.º, n.º 2, alínea h), do RGPD.

A recolha e tratamento de neurodados com propósitos de análise preditiva do pensamento estão, porém, além daquele contexto clínico estabilizado na ordem jurídica[58], aceite como compatível com a tutela de outros bens jurídicos[59], e representam uma invasão da individualidade inconciliável com a preservação de direitos de personalidade irrenunciáveis e absolutos[60]. O RGPD não traça, hoje, distintamente a linha entre um e outro tipo de recolha e tratamento.

---

[57] Ao que, nas palavras de Carlos Alberto da Mota Pinto a propósito dos direitos de personalidade, "é um conteúdo mínimo e imprescindível da esfera jurídica de cada pessoa". Mota Pinto, Carlos Alberto da, *Teoria Geral do Direito Civil*, 3.ª edição, Coimbra, Coimbra Editora, 1996, p. 87.

[58] A utilização fora do âmbito da prestação de serviços e cuidados de saúde varia desde o marketing,à análise de hábitos de consumo, e ao entretenimento. FARBER, Alex, *How brands can read your mind to create the perfect advert*, https://www.thetimes.com/uk/media/article/how-brands-use-brain-reading-tech-to-make-their-ads-hit-home-8gnfsszqw?utm_source=chatgpt.com&region=global, consultado a 6 de agosto de 2025. Agencia Española Protection de Datos (AEPD), *Neurodata and neurotechnology: privacy and protection of personal data*, https://www.aepd.es/en/prensa-y-comunicacion/blog/neurodata-and-neurotechnology-privacy-and-protection-personal-data?utm_source=chatgpt.com, consultado a 6 de agosto de 2025. Autoridade Europeia para a Proteção de Dados (EDPS), *TechDispatch …*, *op. cit.*

[59] Da mesma forma que é admissível a limitação voluntária do direito à integridade física para que um médico realize uma intervenção cirúrgica. Mota Pinto, Carlos Alberto da, *Teoria Geral …*, *op. cit.*, pp. 88 e 212.

[60] Sobre a irrenunciabilidade dos direitos de personalidade, *vide* Mota Pinto, Carlos Alberto da, *Teoria Geral …*, *op. cit.*, pp. 211 e 212. O autor justifica a irrenunciabilidade destes direitos de personalidade pela característica de serem essenciais à pessoa. Se o bem jurídico de personalidade é essencial, então é irrenunciável: é o caso da vida e a integridade física, da liberdade física, mas, também, da liberdade psicológica.

Não é possível – nem se pretende – proibir a recolha e tratamento de neurodados de forma *objetiva*, porque, como vimos, há pelos menos um contexto, o clínico, em que essas recolha e tratamento objetivamente não colidem com a tutela de bens jurídicos relevantes. Podemos até admitir que existam outros contextos, que não o clínico, em que a recolha e tratamento de neurodados não esvaziem a liberdade psicológica do titular dos dados: se a tecnologia utilizada estiver munida de mecanismos que tornem a recolha temporária, por exemplo, e isso seja uma característica relevante da recolha e tratamento, de tal modo que evite o esvaziamento daquele bem jurídico[61]. Nestes casos, a prestação de consentimento, sujeito a requisitos de validade, opera como uma limitação voluntária que se perspetivaria válida.

O RGPD estabelece quais são *objetivamente* os dados pessoais sensíveis. A diferença entre um e outro tipo de recolha e tratamento de neurodados está na finalidade da recolha e tratamento; é, portanto, *subjetiva*. Existem exceções à abordagem predominantemente objetiva do RGPD. Tomemos como referência os dados relativos à saúde e os dados biométricos. Os dados pessoais que se enquadrem nos dados relativos à saúde precisam apenas desse contexto, nada mais, para se sujeitarem ao regime de proteção reforçada, independentemente da finalidade da sua recolha e tratamento. Só cabem, porém, na noção de dados biométricos abrangidos pelo Artigo 9.º n.º 1 do RGPD aqueles que sirvam "para identificar uma pessoa de forma inequívoca"[62]. Não basta, portanto, que sejam biométricos para que seja proibida a sua recolha e tratamento. Quanto aos dados biométricos, a norma é volitiva: a mera fotografia da íris de uma pessoa não é enquadrável como dado biométrico à luz do Artigo 9.º n.º 1 do RGPD, salvo se, face aos meios e finalidade da recolha e tratamento, seja utilizada para "para identificar

[61] Exemplos práticos de contextos, que não o clínico, em que a recolha e tratamento de neurodados não lesione bem jurídicos essenciais (portanto, irrenunciáveis), nomeadamente a liberdade psicológica do titular dos dados, são dificilmente apreciáveis num momento histórico em que a aplicação e desenvolvimento da tecnologia não é cabal.

[62] De acordo com o art. 9.º, n.º 1 do RGPD, relevam os "… dados biométricos para identificar uma pessoa de forma inequívoca …".

uma pessoa de forma inequívoca". Da mesma forma que os dados biométricos merecem a injeção de elementos de vontade para o seu enquadramento no âmbito do regime de proteção reforçada, também os neurodados merecem, pelo menos, solução semelhante.

Mas, além dessa solução, se a recolha e tratamento de qualquer das categorias especiais de dados atualmente previstas está sujeita a um regime de proibição *relativa*, a que se aplicam as (muitas) exceções estabelecidas no n.º 2 do art. 9.º do RGPD, de entre as quais consta o consentimento explícito, aproveitaria à tutela dos neurodados um regime de proibição híper-reforçada. Não ignoramos que o direito da União ou de um Estado-Membro não pode impedir o responsável pelo tratamento de contar com qualquer outra das exceções previstas no art. 9.º, n.º 2, do RGPD, na medida em que consiga preencher os respetivos pressupostos. A restrição não é *absoluta*. Mas a alínea a) do n.º 2 daquele art. 9.º já admite a criação de regimes de proibição reforçada pelo direito da União ou de um Estado-Membro[63]. Não seria, por isso, dissonante sequer da lógica atual do RGPD, que se estabelecesse que a proibição da recolha e tratamento de neurodados para outros fins que não o clínico não pudesse ser *anulada* (nas palavras do legislador) pelo titular dos dados.

O termo *anulada* que é incluído na redação portuguesa do RGPD, equivale à expressão *ne peut pas être levée*, na redação francesa, ou *may not be lifted*, na versão inglesa, o que sugere o levantamento da proibição. De entre as várias exceções ao regime de proibição que constam do n.º 2 do art. 9.º, só uma, esta a que nos referimos, depende da vontade e ação direta do titular dos dados, através da prestação de consentimento explícito. Assim, a proibição específica do n.º 1 do art. 9.º pode ser levantada pelo titular dos dados, mediante consentimento pelo próprio, salvo se o direito da União ou do Estado-Membro limitar a prestação desse consentimento, o que defendemos.

---

[63] "Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o n.º 1 não pode ser anulada pelo titular dos dados."

Os neurodados relacionam-se com identidade, livre desenvolvimento e dignidade individuais, e são, inclusive, um elemento natural da liberdade psicológica do sujeito de direitos[64], pelo que o tema chama a si noções aplicáveis aos direitos de personalidade, nomeadamente a sua irrenunciabilidade. Estas noções afetam a liberdade de prestação de consentimento pelo titular de dados à recolha e tratamento de neurodados em contexto que represente um risco sério à reserva interior do sujeito.

Independentemente da prestação de consentimento pelo titular dos dados, a recolha e tratamento de neurodados geram riscos de intromissão (quiçá, controlo) no pensamento interior[65], que é marco distintivo da liberdade de pensamento, por sua vez fator necessário à integridade mental a que alude o art. 3.º da Carta dos Direitos Fundamentais da União Europeia; é, precisamente, aquilo que se pretende tutelar como direito humano inviolável. Em nosso entender, as consequências da autolimitação de direitos essenciais ao sujeito titular dos dados não se compadecem com a possibilidade de conceber como solução a mera proibição *salvo se* obtido o consentimento[66].

O direito da proteção de dados é convocado a tutelar, aqui, bens de personalidade, desde logo a liberdade psicológica e reserva de pensamento. Ambos são *aspetos específicos* (portanto, delimitados) de uma pessoa: o primeiro diz respeito à manutenção de um espaço interior livre de manipulações exteriores; o segundo, em manter secreto esse espaço. Aqueles são, ainda, aspetos específicos *de uma pessoa*, portanto não dizem respeito a quaisquer elementos exteriores, e estão *efetivamente*

---

[64] A liberdade psicológica, tal como a liberdade física, é um direito de personalidade com a prerrogativas e características naturais a essa posição jurídica, designadamente a irrenunciabilidade.

[65] Gilbert, Frederic / Russo, Ingrid, "Neurorights …, *op. cit.*

[66] Quanto à solução, não acompanhamos Jan Cristoph Bublitz, que propõe um princípio de não revelação do pensamento sem o prévio consentimento do sujeito. Bublitz, Jan Christoph, "Freedom of Thought …, *op. cit*. Tendemos a acompanhar uma solução absoluta de que neurodados de natureza não clínica não podem ser tratados legitimamente (independentemente do consentimento) quando o interesse do responsável pelo tratamento conflitue como os direitos fundamentais e as liberdades do sujeito titular dos dados. É o caso, na nossa opinião. Ienca, Marcello / Fins, Joseph J. / Kellmeyer, Phillip et al., "Towards …, *op. cit*.

presentes na pessoa. Finalmente, a liberdade psicológica e reserva de pensamento são bens que só são *suscetíveis de serem desfrutados pela própria pessoa*[67].

A tutela da disciplina da proteção de dados relacionados com bens jurídicos de personalidade encerra, por isso, dilemas comuns à tutela de bens desta categoria[68]: porque são direitos[69], estão, em princípio, na disponibilidade do sujeito titular; porque o objeto desses direitos é um bem identificável com o próprio sujeito de direito, a sua disponibilidade está comprometida[70]. Neste sentido, para além de funcionar como garantia de coerência lógica no tratamento de direitos que têm por "objeto" o próprio sujeito[71], funciona como garantia da dignidade da pessoa humana, princípio e fim da ordem jurídica[72], a limitação da liberdade de exercício e disponibilidade desses direitos, o que entendemos ser o grau exigível de proteção dos neurodados, quando recolhidos e tratados fora do contexto clínico.

Nem será necessário procurar encontrar tipificação de um direito à liberdade psicológica, interior ou de pensamento, ou um direito à liberdade e reserva de pensamento, porque a consagração da proteção

---

[67] Testamos, aqui, a definição de bem de personalidade avançada por António Menezes Cordeiro. Para o autor, um bem de personalidade corresponde a um aspeto específico de uma pessoa, efetivamente presente, e suscetível de ser disfrutado pelo próprio. Menezes Cordeiro, António, *Tratado de Direito Civil*, IV, Parte Geral, Pessoas, 5.ª edição, Coimbra, Almedina, 2019, pp. 106.

[68] Sobre a dimensão jusfundamental da disciplina, vide Graça Canto Moniz, *Manual* …, op. cit., pp. 15-16.

[69] Ou para alguns autores qualidades ou posições jurídicas garantidas pela lei. Sobre os direitos de personalidade como direitos que não se comparam aos restantes, *vide* Cabral de Moncada, *Lições de Direito Civil*, Coimbra, Atlântida – Livraria Editora, 1932, pp. 60-64.

[70] A tutela objetiva do direito de personalidade compromete a disponibilidade desse direito. Sobre a distinção entre direitos objetivos e subjetivos de personalidade, os primeiros indisponíveis ao próprio titular, *vide* Pais de Vasconcelos, Pedro / Pais de Vasconcelos, Pedro Leitão, *Teoria Geral do Direito Civil*, 9.ª edição, Coimbra, Almedina, 2019, pp. 41-46.

[71] Sobre o próprio sujeito ser objeto de direito (*ius in se ipsum*), *vide* Cabral de Moncada, *Lições* …, *op. cit*., pp. 62-63. Ainda, Vaz de Sequeira, Elsa, *Teoria Geral do Direito Civil*, 3.ª edição, Lisboa, Universidade Católica Editora, 2024.

[72] Referimos especificamente à ordem jurídica portuguesa, mas seria extensível a outras ordens jurídicas da mesma família. O ser humano como fundamento do Direito e único objetivo do ordenamento é uma linha de pensamento kantiana que está na génese do Direito português. Sobre o assunto, vide Menezes Cordeiro, António, *Tratado* …, *op. cit.*, pp. 32-35.

da personalidade é geral, direito-fonte[73], admitindo a tutela de bens não tipificados, precisamente porque só assim se assegura uma tutela resistente ao contexto histórico, social e tecnológico[74]. Ajuda à compreensão da liberdade de pensamento como direito irredutível, o facto de nem a Declaração Universal dos Direitos Humanos[75], nem a sua interpretação pelo Tribunal Europeu dos Direitos Humanos[76], avançarem qualquer tipo de cláusulas de exceção, no primeiro caso, ou interpretação relativista, no segundo, relativamente ao direito à liberdade de pensamento.

Se puder ser estabelecido consenso de que o pensamento e consciência humana são uma parte, senão o todo, do último reduto de individualidade do sujeito, então será de concluir que a prestação de consentimento para a recolha e tratamento de neurodados fora do contexto clínico de acordo com o regime de exceção da alínea a) do n.º 2 do art. 9.º do RGPD constitui uma limitação voluntária de direitos irrenunciáveis sem respaldo nos limites dos nossos princípios de ordem pública, pelo que admitimos que a prestação de consentimento para a recolha e tratamento de neurodados fora do contexto clínico seja condicionada, se não pelo direito da União, então pela nossa ordem jurídica. Quando sejam enquadráveis como categoria especial de dados, entendemos que o consentimento do titular dos dados deve ser afastado pelo legislador como exceção à proibição do art. 9.º, n.º 1, do RGPD, quando

---

[73] Não ignoramos as dificuldades da conceção do direito geral de personalidade como direito-fonte ou direito-quadro, ou a sua necessidade de concretização, mas rejeitamos que a tutela da personalidade requeira tipificação legal como prova de existência. O carácter geral do direito de personalidade permite, como identifica Menezes Cordeiro, "conquistar novos âmbitos [de proteção]". Menezes Cordeiro, António, *Tratado …*, *op. cit.*, p. 65. Contra uma conceção geral de tutela da personalidade, Gonçalves, Diogo Costa, *Pessoa e Direitos de Personalidade – Fundamentação Ontológica da Tutela*, Coimbra, Almedina, 2008.

[74] Mota Pinto, Carlos Alberto da, *Teoria Geral …*, *op. cit.*, pp. 208. No mesmo sentido, Vaz de Sequeira, Elsa, *Teoria Geral …*, *op. cit.*, e, ainda, Carvalho Fernandes, Luís A., *Teoria Geral do Direito Civil*, I, 6.º edição, Lisboa, Universidade Católica Editora, 2012, pp. 232-234.

[75] Art. 18.º da Declaração Universal dos Direitos do Homem.

[76] Por exemplo, Tribunal Europeu dos Direitos Humanos, Nolan c. Rússia (2512/04), 12 de fevereiro de 2009, parágrafo 61; mas, também, Tribunal Europeu dos Direitos Humanos, Kokkinakis c. Grécia (14307/88), 25 de maio de 1993, parágrafo 31.

(e se) os avanços tecnológicos assim o determinarem. Assim determina o carácter atentatório da recolha e tratamento generalizados de neurodados à liberdade e reserva interiores e, por consequência, à dignidade da pessoa humana[77].

6 Bibliografia

Agencia Española Protection de Datos (AEPD), *Neurodata and neurotechnology: privacy and protection of personal data*, https://www.aepd.es/en/prensa-y--comunicacion/blog/neurodata-and-neurotechnology-privacy-and-protection-personal-data?utm_source=chatgpt.com, consultado a 6 de agosto de 2025.

Alegre, Susie, *Freedom to Think – Protecting a Fundamental Human Right in the Digital Age*, Londres, Atlantic Books, 2023.

Autoridade Europeia para a Proteção de Dados (EPDS), *TechDispatch #1/2024 – Neurodata*, https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2024-06-03-techdispatch-12024-neurodata_en, consultado a 1 de março de 2025

Ascensão, José de Oliveira, *Direito Civil Teoria Geral*, I, 2.ª edição, Coimbra, Coimbra Editora, 2000

Baillet, Sylvain, "Magnetoencephalography for brain electrophysiology and imaging", *Nature Neuroscience*, vol. 20, n.º 3, 2017

Belliveau, John W. / Kennedy Jr., D. N. / McKinstry, R.C. et al., "Functional mapping of the human visual cortex by magnetic resonance imaging", *Science*, vol. 254, n.º 5032, 1991

Boto, Elena / Meyer, Sofie S. / Shah, Vishal, et al. "A new generation of magnetoencephalography: Room temperature measurements using optically-pumped magnetometers", NeuroImage, vol. 149, 2017

Bublitz, Jan Christoph, "Freedom of Thought in the Age of Neuroscience: A Plea and a Proposal for the Renaissance of a Forgotten Fundamental Right", *Archiv für Rechts- und Sozialphilosophie*, vol. 100, 1, 2014

[77] Global Privacy Assembly, 46th Closed Session …, *op. cit*. Lê-se a este propósito, na na referida resolução da Global Privacy Assembly, e com sugestão semelhante, que os legisladores devem estabelecer proibições claras à utilização de neurodados quando essa utilização viole a dignidade da pessoa humana, para isso considerando os avanços tecnológicos.

Cabral de Moncada, *Lições de Direito Civil*, Coimbra, Atlântida – Livraria Editora, 1932

Carvalho Fernandes, Luís A., *Teoria Geral do Direito Civil*, I, 6.º edição, Lisboa, Universidade Católica Editora, 2012

Chekroud, Adam M. / Everett, Jim A. C. / Bridge, Holly et al., "A review of neuroimaging studies of race-related prejudice: does amygdala response reflect threat?", *Front. Hum. Neurosci.*, vol. 8, n.º 179

Cohen, Julien E., "What privacy is for", *Harvard Law Review*, vol. 126, 2013, pp. 1904-1907

Das, Manasmita, *Neuroimaging Techiniques and What a Brain Image Can Tell Us*, https://www.technologynetworks.com/neuroscience/articles/neuroimaging-techniques-and-what-a-brain-image-can-tell-us-363422, consultado a 18 de janeiro de 2025.

Digenmanse, Mark, *The space between our heads*, https://aeon.co/essays/why-language-remains-the-most-flexible-brain-to-brain-interface, consultado a 18 de janeiro de 2025.

Eaton, M. L. / Illes, J., "Commercialising cognitive neurotechnology – the ethical terrain", *Nature Biotechnology*, vol. 25, 4, 2007, pp. 393-397.

FARBER, Alex, *How brands can read your mind to create the perfect advert*, https://www.thetimes.com/uk/media/article/how-brands-use-brain-reading-tech-to-make-their-ads-hit-home-8gnfsszqw?utm_source=chatgpt.com&region=global, consultado a 6 de agosto de 2025.

Ferrante, Matteo / Boccato, Tommaso / Ozcelik, Furkan et al., "Through their eyes: Multi-subject brain decoding with simple alignment techniques", *Imaging Neuroscience*, vol. 2, 2024, pp. 1-21

Fred, A.L. / Kumar, S.N. / Kumar Haridhas, A. et al., "A Brief Introduction to Magnetoencephalography (MEG) and Its Clinical Applications", Brain Sciences, vol. 12, n.º 6, 2022

Gilbert, Frederic / Russo, Ingrid, "Neurorights: The Land of Speculative Ethics and Alarming Claims?", *AJOB Neuroscience*, vol. 15, 2, 2007, pp. 113-115

Global Privacy Assembly, 46th Closed Session of the Global Privacy Assembly – Resolution on principles regarding the processing of personal information in neuroscience and neurotechnology, https://globalprivacyassembly.org/wp-content/uploads/2024/11/Resolution-on-Neurotechnologies.pdf, consultado a 5 de agosto de 2025.

Gonçalves, Diogo Costa, *Pessoa e Direitos de Personalidade – Fundamentação Ontológica da Tutela*, Coimbra, Almedina, 2008

Graça Canto Moniz, *Manual de Introdução à Proteção de Dados*, Coimbra, Almedina, 2024

Hallinan, Dara / Schütz, Philip / Friedewald, Michael et al., "Neurodata and Neuroprivacy: Data Protection Outdated?", Surveillance & Society, vol. 12, n.º 1, 2014, pp. 55-72

Hämäläinen, Matti / Hari, Riitta / Ilmoniemi, Risto et al., "Magnetoencephalography: theory, instrumentation and applications to the noninvasive study of human brain function", *Review of Modern Physics*, vol. 65, n.º 2, 1993

Herrmann, Ned, *What is the function of the various brainwaves?*, https://www.scientificamerican.com/article/what-is-the-function-of-t-1997-12-22/, consultado a 18 de janeiro de 2025.

Ienca, Marcello / Fins, Joseph J. / Kellmeyer, Phillip et al., "Towards a Governance Framework for Brain Data", *Neuroethics*, vol. 15, 20, 2022

Information Commissioner's Office (ICO), *ICO tech futures: neurotechnology*, https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/ico-tech-futures--neurotechnology/, consultado a 1 de março de 2025

Jayalath, Dulhan / landau, Gilad / Shillingford, Brendan et al., "The Brain's Bitter Lesson: Scaling Speech Decoding With Self-Supevised Learning", *Proceedings of the 42nd International Conference on Machine Learning*, Vancouver, Canadá

Jezzard, Peter / Toosy, Ahmed T., "Functional MRI", *MR Imaging in White Matter Diseases of the Brain and Spinal Cord*, Springer, Berlin, 2005

Jones, Owen D / Buckholtz, Joshua W. / Schali, Jeffrey D. et al, "Brain Imaging for Legal Thinkers: A Guide for the Perplexed", *Stanford Technology Law Review*, vol. 5, 2009

Kay, Kendrick N. / Gallant, Jack L., "I can see what you see", *Nature Neuroscience*, 12, 2009, pp. 245-246

Kwong, Kenneth K. / Belliveau, John W. / Chesler, David A. et al. "Dynamic magnetic resonance imaging of human brain activity during primary sensory stimulation", *Proceedings of the National Academy of Sciences*, vol. 89, 1992

Leal, Ana Alves, "Aspetos jurídicos da análise de dados na Internet (*big data analytics*) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação", *FinTech: Desafios da Tecnologia Financeira*, 2.ª edição, Almedina, 2019, pp. 89-220

Lévy, Jarod / Zhang, Mingfang (Lucy) / Pinet, Svetlana et al., "Brain-to-Text Decoding: A Non-invasive Approach via typing", 10.48550/arXiv.2502.17480.

Messinetti, Davide / Di Ciommo, Francesco, "Diritti della personalità" em *Diritto Civile*, coord. Martuccelli, Silvio / Pescatore, Valerio, Milano, Giuffré Editore, 2011

Menezes Cordeiro, António, *Tratado de Direito Civil*, vol. I, 4.ª edição, Coimbra, Almedina, 2016

Menezes Cordeiro, António, *Tratado de Direito Civil Português*, I, Tomo III, 2.ª edição, Coimbra, Almedina, 2007

Menezes Cordeiro, António, *Tratado de Direito Civil*, IV, Parte Geral, Pessoas, 5.ª edição, Coimbra, Almedina, 2019

Menezes Cordeiro, António, *Tratado de Direito Civil*, vol. XIII, 1.ª edição, Coimbra, Almedina, 2022

Miyawaki, Yoichi / Uchida, Hajime / Yamashita, Okito et al., "Visual Image Reconstruction from Human Brain Activity using a Combination of Multiscale Local Image Decoders", *Neuron*, vol. 60, 5, 2008, pp. 915-929

Mota Pinto, Carlos Alberto da, *Teoria Geral do Direito Civil*, 3.ª edição, Coimbra, Coimbra Editora, 1996

Naddaf, Miryam, *Brain-reading device is best yet at decoding 'internal speech'*, https://www.nature.com/articles/d41586-024-01424-7, consultado a 13 de dezembro de 2024

Nuñez, Paul L. / Srinivasan, Ramesh, *Electrical Fields of the Brain: The Neurophysics of EEG*, Oxford University Press, Nova Iorque, 2006

OCDE, *Recommendation of the Council on Responsible Innovation in Neurotechnology*, https://legalinstruments.oecd.org/en/instruments/oecd-legal-0457, consultado a 1 de março de 2025

Ogawa, Seiji / Tank, David W. / Menon, Ravi et al. "Intrinsic signal changes accompanying sensory stimulation: Functional brain mapping with magnetic resonance imaging", *Proceedings of the National Academy of Sciences*, vol. 89, 1992

Pais de Vasconcelos, Pedro / Pais de Vasconcelos, Pedro Leitão, *Teoria Geral do Direito Civil*, 9.ª edição, Coimbra, Almedina, 2019

Peters, Ruth, "Ageing and the brain", *Postgraduate Medical Journal*, vol. 82, n.º 964

Pinheiro, Alexandre Sousa, *Privacy e Proteção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, AAFDL, Lisboa, 2015

Pinto Monteiro, António, "A Tutela dos Direitos de Personalidade no Código Civil", *Revista Jurídica Portucalense*, 29, 2021

Powers, Benjamin, *Technology Melds Minds With Machines, and Raises Concerns*, https://undark.org/2020/04/22/brain-technology-interface/, consultado a 16 de dezembro de 2024

Rao, Rajesh P. N. / Stocco, Andrea / Bryan, Matthew et al., "A Direct Brain-to--Brain Interface in Humans", *PLoS ONE*, vol. 9, n.º 11, 2014

Reed, Charlotte M. / Durlach, Nathaniel I., "Note on Information Transfer Rates in Human Communication", *Presence: Teleoperators and Virtual Environments*, vol. 7, n.º 5, pp. 509–518

Reveley, Fletcher, *Advances in Mind-Decoding Technologies Raise Hopes (and Worries)*, https://undark.org/2024/01/03/brain-computer-neurorights/?utm_source=join1440&utm_medium=emai, consultado a 16 de dezembro de 2024

St. Louis, Erik / Frey, Lauren C., *Electroencephalography (EEG): An Introductory Text and Atlas of Normal and Abnormal Findings in Adults, Children and Infants*, Chicago, American Epilepsy Society, 2016

Teplan, Michal, "Fundamentals of EEG measurement", Measurement Science Review, vol. 2, n.º 2, 2002

Thirion, Bertrand / Duchesnay, Edouard / Hubbard, Edward et al., "Inverse retinotopy: Inferring the visual content of images from brain activation patterns", *NeuroImage*, vol. 33, 4, 2006, pp. 1104-1116

UNESCO, *Report of the International Bioethics Committee of UNESCO (IBC) on the ethical issues of neurotechnology*, https://unesdoc.unesco.org/ark:/48223/pf0000378724, consultado a 1 de março de 2025

Vaz de Sequeira, Elsa, *Teoria Geral do Direito Civil*, 3.ª edição, Lisboa, Universidade Católica Editora, 2024

Wandelt, Sarah K. / Bjånes, David A. / Pejsa, Kelsie et al., "Representation of internal speech by single neurons in human supramarginal gyrus", *Nature Human Behaviour*, 8, 2024, pp. 1136-1149

Westin, Alan F., *Privacy and Freedom*, IG Publishing, 2018

Yuste, Rafael / Goering, Sara / Agüera y Arcas, Blaise et al., "Four ethical priorities for neurotechnologies and AI", *Nature*, vol. 551, 2017, pp. 159-163

Os algoritmos e a transparência no tratamento de dados pessoais no contexto da internet: uma análise luso-brasileira

Camila Schwonke Zanatta[1]

Resumo: O artigo analisa o princípio da transparência no tratamento de dados pessoais no ambiente digital, com enfoque nas legislações brasileira (LGPD) e europeia (RGPD). Através de uma metodologia qualitativa e analítico-comparativa, explora os desafios da coleta automatizada, o uso de algoritmos e a opacidade das decisões baseadas em inteligência artificial. Defende a transparência como requisito essencial à autodeterminação informativa. Propõe a explicabilidade, auditoria e educação digital como formas de mitigar riscos, reforçando o papel da transparência como eixo estruturante da proteção de dados pessoais.

Palavras-chave: Transparência; Algoritmo; Dados Pessoais; LGPD; RGPD;

Abstract: This article analyzes the principle of transparency in personal data processing within the digital environment, with a focus on Brazilian (LGPD) and European (GDPR) legislation. Using a qualitative and analytical-comparative methodology, it explores the challenges of automated data collection, algorithmic use, and the opacity of artificial intelligence-based decisions. Transparency is defended as an essential requirement for informational self-determination. It proposes explainability, auditing, and digital education as means to mitigate risks, reinforcing transparency's role as a structural pillar of personal data protection.

---

[1] Mestre e Doutoranda em Direito e Ciência Jurídica na Faculdade de Direito da Universidade de Lisboa. camilaszanatta@gmail.com

Keywords: Transparency; Algorithm; Personal Data; LGPD; GDPR;

Introdução

A transparência no tratamento de dados pessoais obtidos na internet constitui princípio fundamental do Direito Digital contemporâneo. Em um cenário marcado pela natureza transfronteiriça e pelo anonimato característico da internet, compreender de que forma as informações dos usuários são tratadas, processadas e compartilhadas torna-se requisito essencial para a efetividade da autodeterminação informativa[2], direito intrinsecamente ligado à dignidade da pessoa humana.

No plano normativo, tanto o Regulamento Geral de Proteção de Dados (RGPD), aplicável em Portugal e na União Europeia, e a Lei Geral de Proteção de Dados (LGPD) no Brasil, consagram a transparência como princípio estruturante do direito de proteção de dados. Essas normas impõem o dever de informação e explicabilidade aos agentes de tratamento, de modo que eventuais decisões automatizadas ou o uso de algoritmos para perfilamento não resultem em discriminação injustificada ou violação de direitos individuais.

Entretanto, a opacidade que caracteriza muitos sistemas algorítmicos, somada à complexidade técnica das soluções de Inteligência Artificial (IA), desafia a concretização desse princípio. Em especial, há divergências relevantes entre o RGPD e a LGPD quanto ao alcance da obrigação de transparência, ao tratamento das decisões exclusivamente automatizadas e aos mecanismos de fiscalização e sanção.

Nesse contexto emerge uma questão: em que medida o princípio da transparência, tal como disciplinado no RGPD e na LGPD, é capaz de mitigar os riscos decorrentes da opacidade algorítmica, e quais são as implicações práticas das diferenças regulatórias entre Portugal/União Europeia e Brasil para a proteção de dados pessoais no ambiente digital?

---

[2] Artigo 2.º, inciso II, da LGPD.

Para tanto, adota-se uma abordagem qualitativa, de natureza exploratória e analítico-comparativa, voltada à compreensão das convergências e divergências entre o regime europeu e o brasileiro de proteção de dados pessoais partindo de uma revisão bibliográfica e normativa, abrangendo legislação, doutrina especializada, pareceres e documentos técnicos emitidos por autoridades de proteção de dados. A análise restringe-se ao tratamento de dados pessoais no contexto da internet, com ênfase nas práticas algorítmicas e nos processos de tomada de decisão automatizada.

1. A Noção de Transparência no Tratamento de Dados Pessoais

a. Origem e evolução do princípio da transparência

Inicialmente, há de se falar que a Constituição Portuguesa de 1976 foi uma das primeiras constituições do mundo a tratar da questão da proteção dos dados pessoais. Esta previa no artigo 35.º sob a epígrafe "Utilização da Informática" o direito de todos os cidadãos de tomar conhecimento do que constar dos registos mecanográficos a seu respeito e do fim a que se destinam as suas informações, podendo exigir a sua retificação dos dados e atualização[3]. Não permitia o uso da informática para o tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se tratasse do tratamento de dados não identificáveis para fins estatísticos[4].

O artigo 35.º na redação atual, que mantém a mesma epígrafe, prevê o direito de acesso aos dados informatizados que lhe digam respeito, direito de retificação e atualização, o direito a conhecer a finalidade a que se destinam[5]. Também veda a utilização da informática

[3] Versão inicial do artigo 35.º, 1.

[4] Versão inicial do artigo 35.º, 2.

[5] Versão (atual) Alterada pelo Artigo 18.º da Lei Constitucional n.º 1/97 – Diário da República n.º 218/1997, Série I-A de 1997-09-20, em vigor a partir de 1997-10-05 do Artigo 35.º, 1.

para tratamento de dados sensíveis, a não ser que haja o consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis[6] e proíbe o acesso a dados pessoais de terceiros, com as devidas exceções legais[7].

À nível europeu, em 23 de setembro de 1980 foram adotadas as Diretrizes da OCDE (Organização para a Cooperação e Desenvolvimento Econômico) sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais, que representam até hoje o consenso internacional sobre a orientação geral relativa à coleta e ao gerenciamento de informações pessoais estabelecendo princípios fundamentais e assistindo governos, empresas e representantes de consumidores em seus esforços para proteger a privacidade e os dados pessoais[8].

À época, as guidelines da OCDE o denominaram de *openness principle*, princípio da abertura, segundo o qual indicava a necessidade de haver uma política geral de abertura sobre as práticas e políticas com relação a dados pessoais. Orientavam que deveriam haver meios que indicassem a existência e a natureza dos dados pessoais, as principais finalidades de seu uso, bem como a identidade e a residência habitual do controlador de dados. [9]

Após, a Convenção 108 do Conselho Europeu de 1981 que teve lugar em Strasbourg foi o principal marco de uma abordagem da matéria de proteção de dados pessoais através da chave dos direitos fundamentais[10], sendo, assim, o primeiro tratado internacional sobre

---

[6] Consoante versão atual do Artigo 35.º, 3.

[7] Consoante versão atual do Artigo 35.º, 4.

[8] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Publishing, Paris, 2002 Disponível em: https://doi.org/10.1787/9789264196391-en. Acesso em: 03 mar. 2025.

[9] Openness Principle.:

[12.] There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

[10] DONEDA, Danilo. O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). Direito

proteção de dados pessoais. Ele introduziu a ideia de que o tratamento de dados deve ser realizado de forma leal e lícita, um conceito que prefigura o princípio da transparência.

Como se vê o princípio já era dotado de importante valor no tratamento de dados pessoais:

> **Artigo 5 – Legitimidade do tratamento de dados e qualidade dos dados**
> (...)
> 4. Os dados pessoais sujeitos a tratamento deverão ser:
> a. tratados de forma justa e transparente;
>
> **Artigo 8 – Transparência do tratamento**
> 1. Cada Parte deverá prever que o responsável pelo tratamento informa os titulares dos dados sobre:
> (…)
> b. o fundamento jurídico e as finalidades do tratamento previsto;
> (…)
>
> **Artigo 9 – Direitos do titular dos dados**
> 1. Todas as pessoas terão o direito de:
> (...) b. obter, mediante pedido, a intervalos razoáveis e sem demora ou despesas excessivas, a confirmação do tratamento dos dados pessoais que lhe digam respeito, a comunicação, sob forma inteligível, dos dados tratados, toda a informação disponível sobre a sua origem e o período de conservação, bem como qualquer outra informação que o responsável pelo tratamento seja obrigado a fornecer a fim de assegurar a transparência do tratamento nos termos do artigo 8.º, n.º 1;

digital: direito privado e internet. 3. ed. Indaiatuba: Editora Foco, 2020. p.27.

Após a Convenção 108 do Conselho da Europa de 1981, um marco relevante foi a Diretiva 95/46/CE de 24 de Outubro de 1995, aprovada pela União Europeia em 1995. Essa norma consolidou a proteção de dados pessoais, exigindo que os Estados-Membros harmonizassem suas legislações nacionais com as diretrizes estabelecidas. A diretiva abordou aspectos como privacidade, transparência e direitos dos titulares, promovendo um ambiente legal uniforme para a gestão e proteção de informações pessoais em toda a Europa.

Segundo António Barreto Menezes Cordeiro, o princípio da transparência seria uma novidade no RGPD, por considerar que durante a vigência da Diretiva 95/46/CE era abrangido pelo princípio da lealdade[11][12]. O princípio da lealdade estava previsto na alínea a) do n.º 1 do artigo 6.º da Diretiva 95/46/CE:

> **Artigo 6.º**
> 1. Os Estados-membros devem estabelecer que os dados pessoais serão:
> a) Objecto de um tratamento leal e lícito;

Porém, nos Considerandos desta Diretiva já havia a indicação do o dever de transparência do tratamento de dados pelas autoridades de controlo dos Estados-Membros[13]. Além disso, pode-se dizer que o princípio da transparência no tratamento de dados na Diretiva 95/46/CE estava previsto nos arts. 10 e 11, os quais exigiam que o responsável pelo tratamento fornecesse informações claras e acessíveis aos titulares

---

[11] O princípio da lealdade estava previsto no Artigo 6.º, 1, a da Diretiva 95/46/CE
1. Os Estados-membros devem estabelecer que os dados pessoais serão:
a) Objecto de um tratamento leal e lícito;

[12] CORDEIRO, A. Barreto Menezes. Direito da proteção de dados: à luz do RGP e da Lei n.º 58/2019. Coimbra: Almedina, 2022. p.155

[13] (62) Considerando que a criação nos Estados-membros de autoridades de controlo que exerçam as suas funções com total independência constitui um elemento essencial da protecção das pessoas no que respeita ao tratamento de dados pessoais;
(63) (...) que essas autoridades devem ajudar a garantir a transparência do tratamento de dados efectuado no Estado-membro sob cuja jurisdição se encontram;

sobre o processamento de seus dados com o objetivo de garantir que os titulares tivessem plena compreensão de como seus dados seriam utilizados, promovendo confiança e controle.

No RGPD, a transparência é mencionada por diversas vezes ao longo do texto como princípio fundamental do tratamento de dados pessoais, como se vê nas alíneas a) e d) do n.º 1 do artigo 5.º[14] e no artigo12.º[15], além de contar com uma seção inteiramente dedicada para a transparência e o cumprimento dos direitos dos titulares de dados[16][17]. Ainda, conta com uma seção inteiramente dedicada para a transparência e o cumprimento dos direitos dos titulares de dados.

Assim, verifica-se que a transparência no tratamento de dados pessoais consiste em assegurar que os indivíduos sejam informados de maneira clara e acessível sobre a forma como seus dados são coletados, utilizados, armazenados e compartilhados. Esse princípio requer que as informações sejam apresentadas de forma compreensível, permitindo que qualquer pessoa, independentemente de seu nível de conhecimento técnico, possa entender os processos que envolvem seus dados.

---

[14] Artigo 5.º Princípios relativos ao tratamento de dados pessoais

1. Os dados pessoais são:

a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);

(…) d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);

[15] O artigo 12 estabelece as regras gerais que se aplicam a: fornecimento de informações aos titulares de dados (de acordo com os arts. 13 a 14); comunicações com os titulares de dados sobre o exercício de seus direitos (de acordo com os arts. 15 a 22); e comunicações relacionadas a violações de dados (artigo 34).

[16] CAPÍTULO III, Direitos do titular dos dados, Secção 1 Transparência e regras para o exercício dos direitos dos titulares dos dados.

[17] Porém, não há qualquer previsão expressa e detalhada sobre o que, de fato, seja a transparência. No RGPD esta acaba por ser uma norma-princípio, orientando a interpretaçao de outras normas e sua compreensãoé constuída a partir do contexto do RGPD, seus considerandos, da jurisprudência e das orientações do Comitê Europeu para Proteção des Dados. Portanto, a definição é implícita.

No Brasil, a regulação sobre o tema tardou mais a chegar, pelo que a Lei Geral de Proteção de Dados (LGPD)[18] é datada de agosto de 2018 e entrou totalmente em vigor dois anos depois[19]. Porém, ante os desafios da era digital, fez-se necessária para garantir que as pessoas tenham clareza sobre como seus dados são coletados, processados, protegidos e seus direitos.

A LGPD brasileira é uma lei principiológica e prevê o princípio da transparência como um dos princípios que devem reger as atividades de tratamento de dados pessoais, juntamente da boa-fé[20].

Até a entrada em vigor do LGPD a transparência no tratamento de dados pessoais era protegida de forma fragmentada e indireta, sob princípios constitucionais, normas consumeristas e, a partir de 2014, com o Marco Civil da Internet.

Os direitos à inviolabilidade da intimidade e da vida privada e do sigilos das comunicações, previstos no artigo 5.º, incisos X e XII[21] eram interpretados como uma base principiológica para a proteção de dados pessoais e para a exigência de transparência no seu tratamento.

No Código de Defesa do Consumidor[22], datado de 1990, já havia o direito do consumidor acessar as informações existentes em cadastros, fichas, registros e dados pessoais e de consumo sobre ele, bem como suas fontes.[23]

---

[18] Lei n.º 13.709, de 14 de AGOSTO de 2018.

[19] Consoante previsão do artigo 65, II da Lei.

[20] artigo 6.º, caput e VI da LGPD.

[21] artigo 5.º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

(…) X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

(…) XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

[22] Lei n.º 8.078, de 11 de setembro de 1990 – Dispõe sobre a proteção do consumidor e dá outras providências.

[23] artigo 43 do CDC.

Ademais, o Marco Civil da Internet[24] também trata da proteção dos dados pessoais, prevendo o consentimento na coleta dos dados e o agir de maneira transparente. Foi um dos instrumentos mais relevantes no contexto digital brasileiro pré-LGPD, demonstrando a necessidade da transparência e do consentimento informado nas relações firmadas no contexto da internet.

Assim, vê-que a transparência tem como objetivo fortalecer a confiança dos titulares ao promover práticas que respeitem seus direitos e assegurem maior controle sobre suas informações pessoais, sendo um aspecto central nas regulamentações modernas de proteção de dados, como o RGPD na Europa e a LGPD no Brasil.

b. Noção de transparência

Danilo Doneda sintetiza o princípio da publicidade ou da transparência, como aquele "pelo qual a existência de um banco de dados pessoais deve ser de conhecimento público, seja através da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência ou do envio de relatórios periódicos".[25]

A transparência no tratamento dos dados pessoais não se limita à mera transferência de informações de um agente a outro: é complexa pois pode se referir à capacidade de explicação do tratamento dos dados, à capacidade de interpretação, acessibilidade, abertura e visibilidade deste[26].

Segundo Filipe Magalhães, o direito à transparência tendo como principais destinatários os titulares de dados pessoais nada mais é do

---

[24] Lei n.º 12.965, de 23 de abril de 2014 – Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

[25] DONEDA, Danilo. O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS. p.26.

[26] FÁCIO, Rafaella Nátaly. "A transparência e o direito de acesso no tratamento de dados pessoais: considerações sobre intersecções entre Lei Geral de Proteção de Dados e Lei de Acesso à Informação no Brasil." *Rev. Eurolatin. de Derecho Adm.*, Santa Fe, v. 10, n. 2, e247, jul./dic. 2023.p.8

que a consagração da necessidade de utilização de uma linguagem e procedimentos transparentes[27].

O princípio da transparência está presente em todas as etapas do tratamento de dados, abrangendo desde os primeiros contatos entre o responsável pelo tratamento e os potenciais titulares de dados (fase de formação), passando pela coleta e pelas demais operações de tratamento (fase de execução), mantendo-se aplicável mesmo após o encerramento da relação.[28]

Apesar de não haver uma definição expressa de transparência no RGPD, o considerando 39 do é informativo quanto ao seu significado e ao efeito do princípio da transparência no contexto do processamento de dados[29]:

> (39) O tratamento de dados pessoais deverá ser efetuado de forma lícita e equitativa. Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados. **O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a**

[27] MAGALHÃES, Filipe. *Manual RGPD*. Ordem dos Contabilistas Certificados (OCC), 2018. p.13.

[28] CORDEIRO, A. Barreto Menezes. Direito da proteção de dados, p.154

[29] Article 29 Data Protection Working Party. **Guidelines on transparency under Regulation 2016/679**. Adopted on 29 November 2017. Revised and adopted on 11 April 2018. Disponível em: https://ec.europa.eu/newsroom/article29/items/622227. Acesso em: 06 fev 2025.

> **confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados**. As pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento. (grifo nosso)

A LGPD brasileira prevê explicitamente a noção do princípio da transparência: "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial."[30].

Trata-se de um princípio que se converte em uma regra jurídica, como se vê do § 1.º do artigo 9.º, que considera nulo o consentimento que não tenha cmprido com informar de forma transparente, clara e inequívoca o titular dos dados[31].

2. O Tratamento de Dados Pessoais na Internet

a. Caracterização de dados pessoais e sensíveis na era digital

Dado pessoal, enquanto, "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)" consoante artigo 4.º, n.º 1 do RGPD, e, do mesmo modo, "informação relacionada a pessoa natural identificada ou identificável" no artigo 5.º, n.º 1 da LGPD, é facilmente vinculada à informações que aparecem em sistemas eletrônicos, mas também nas vias físicas.

---

[30] artigo 6.º, VI

[31] artigo 9.º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: (…) § 1.º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. (grifo da autora)

No ambiente digital, a coleta de dados pessoais tornou-se ampla e constante, frequentemente ocorrendo sem que os indivíduos tenham plena ciência ou forneçam consentimento expresso. Serviços online, redes sociais, aplicativos e plataformas digitais acessam grandes volumes de informações pessoais por meio de práticas como monitoramento contínuo, análise de metadados e aplicação de algoritmos que antecipam comportamentos, muitas vezes de maneira pouco evidente para os usuários.

Portanto, cabe nominar exemplos de dados pessoais específicos do uso da internet. Primeiramente, informações de navegação online são consideradas dados pessoais, como endereços IP (protocolo internet), cookies (testemunhos de conexão), comportamento de navegação e histórico de buscas. Ademais, dados de localização do usuário (titular dos dados), como informações sobre onde o usuário se encontra em tempo real por meio de dispositivos móveis e aplicativos.

Os metadados são informações como hora e data de envio de e-mails, mensagens ou interações em plataformas digitais. Ao associá-los com outros dados, permitem identificar o seu titular, por exemplo.[32] No âmbito das redes sociais, perfil do usuário, seus posts, as fotos postadas, interações, etc, também são considerados dados pessoais.

Em tratando-se de dados sensíveis de um subconjunto dos dados pessoais que podem revelar aspectos íntimos da vida do indivíduo, exigem um nível mais alto de proteção, como se vê do Considerando 51[33] e do artigo 9.º do RGPD e do artigo 11 da LGPD.

---

[32] "A palavra metadados significa algo como "*além dos dados*". Dito de outra forma, os metadados são dados sobre outros dados, ou seja, permitem auxiliar na identificação, descrição e localização de informação." Ver: https://www.cgd.pt/Site/Saldo-Positivo/formacao-e-tecnologia/Pages/metadados-o-que-sao.aspx#:~:text=para%20que%20serve–,O%20que%20s%C3%A3o%20os%20metadados%3F,descri%C3%A7%C3%A3o%20e%20localiza%C3%A7%C3%A3o%20de%20informa%C3%A7%C3%A3o. Acesso em 11 ago 2025.

[33] "Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais.(…)"

Assim, em meio digital, os dados sensíveis são aqueles de origem racial ou étnica obtidos através de plataformas que coletam dados sobre a aparência, comportamento ou preferências culturais, incluindo redes sociais. Igualmente, opiniões políticas e crenças religiosas compartilhadas em redes sociais ou coletadas por serviços de publicidade online. Ainda, dados sobre a saúde do usuário como históricos médicos, tratamentos, diagnósticos e informações sobre condições de saúde compartilhadas em aplicativos ou dispositivos de monitoramento de saúde, como os relógios inteligentes.[34] Informações baseadas em comportamentos online sobre a vida sexual e/ou orientação sexual do usuário[3536], como as interações realizadas em plataformas de namoro ou consumo de conteúdo são consideradas dados pessoais sensíveis.

Há de se falar também nas informações extraídas de tecnologias de reconhecimento facial, impressões digitais, muitas vezes coletadas em aplicativos de segurança ou plataformas que utilizam autenticação biométrica, e informações sobre DNA obtidas em sites de testes genéticos[37]: trata-se de dados biométricos e genéticos, portanto, são dados pessoais sensíveis.

Os dados sensíveis se tornaram ainda mais acessíveis e suscetíveis a abusos na era digital, principalmente devido à utilização massiva de tecnologias de coleta e inteligência artificial, que podem processar grandes volumes de dados e inferir informações sensíveis a partir de comportamentos ou padrões de consumo. Por isso, a transparência

---

[34] Consoante definição do artigo 5.º, II da LGPD e artigo 9.º, 1 do RGPD.

[35] Apesar do rol de dados sensíveis previsto na LGPD não incluir expressamente "orientação sexual" e "identifdade de gênero", indica que a informação acerca da vida sexual de um sujeito é um dado sensível.

[36] Ver: FICO, Bernardo de Souza Dantas; NÓBREGA, Henrique Meng. "The Brazilian Data Protection Law for LGBTQIA+ People: Gender identity and sexual orientation as sensitive personal data" Revista Direito e Práxis, v. 13, n. 2, p. 1262–1288, 2022.

Disponível em: https://www.e-publicacoes.uerj.br/revistaceaju/article/view/66817. Acesso em: 19 abr. 2025.

[37] "Dados genéticos são o que há de mais pessoal e não podem ser alterados. Caso haja uma violação de dados, por exemplo, o indivíduo fica exposto definitivamente. Não é como a senha do Facebook, que basta alterar e atualizar em todos os dispositivos para garantir sua segurança novamente." BERTOLLI, Emilia.Os riscos dos testes genéticos. *Varonis*, 2023. Disponível em: https://www.varonis.com/pt-br/blog/os-riscos-dos-testes-geneticos. Acesso em: 20 jan. 2025.

acerca do processamento dos dados pessoais dos usuários é de extrema importância no quotidiano dos internautas.

b. Os desafios da coleta e armazenamento de dados na internet

A proteção de dados pessoais e sensíveis na era digital envolve desafios complexos, dentre eles, a coleta em massa, armazenamento e compartilhamento de dados, decisões automatizadas e discriminação algorítmica.

No que diz respeito à coleta em massa de dados pessoais na internet, há de sew falar na consequente invasão da privacidade do titular destes. Essa coleta é muitas vezes realizada sem o conhecimento do titular, utilizando tecnologias como rastreamento de localização e monitoramento de comportamento online, o que gera insegurança jurídica.

Ainda, é um fato inegável que a natureza transfronteiriça da internet permite a armazenagem de dados em servidores do mundo todo, o que acaba por dificultar a proteção. Daí a importância da transparência quando houver a intenção de tratamento dos dados, de forma a obter um consentimento lícito.

Dados aparentemente inocentes como um número de telefone associado ao artigo comprado em determinada loja virtual permitem o estabelecimento de um perfil de consumo sobre um sujeito, principalmente quando associado a informações vindas de outras bancos de dados.[38]

Ademais, identificadores fornecidos pelos aparelhos eletrônicos, aplicações, ferramentas e protocolos podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos algoritmos, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares.[39]

---

[38] Sobre a possibilidade de identificar um sujeito com base no comportamento online e poucos dados pessoais, ver: RUIZ, Evandro Eduardo Seron. Anonimização, pseudonimização e desanonimização de dados pessoais. Comentários à Lei Geral de Proteção de Dados – Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina Brasil, 2020. Pp.104-105

[39] Considerando 30 do RGPD

O uso de inteligência artificial é cada vez mais usual nas práticas de publicidade e no tratamento de dados pessoais, o que, com base em dados estatísticos e as "regras" que alimentaram o algoritmo existente, podem levar à uma discriminação indireta, prejudicando determinados grupos de pessoas com base em dados sensíveis, como etnia ou orientação sexual.

c. A transparência como dever: obrigações legais nos regimes de proteção dos dados pessoais

Em aspectos práticos há de se levar em conta o considerando 58 do Regulamento, o qual clarifica a forma como deve se dar a informação ao titular dos dados: "concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples, e que se recorra, adicionalmente, à visualização sempre que for adequado", podendo ser fornecidas por via eletrónica.

Consoante os direitos de informação e acesso presentes nos arts. 13.º a 15.º do RGPD, os titulares dos dados têm o direito de ser informados pelos responsáveis pelo tratamento de dados sobre a existência de decisões automaticamente e de receber informações sobre a lógica envolvida e as consequências previstas deste tratamento automatizado[40], bem como de receber detalhes sobre os seus dados pessoais que estão a ser utilizados para *automated decision-making* (ADM) [41].

Segundo Barbosa, estes direitos de informação e acesso podem ser entendidos como um direito a uma explicação genérica *ex ante* sobre a funcionalidade do sistema e as suas consequências para a pessoa em causa, embora o direito a uma explicação *ex post* não esteja incluído na disposição[42].

---

[40] Consoante arts. 13.º, n.º 2, alínea f), e 14.º, n.º 2, alínea g).

[41] artigo 15.º, n.º 1, alínea h).

[42] BARBOSA, Sandra. A importância da transparência e explicabilidade no uso de decisões automatizadas pelo artigo 22.º do RGPD. Cadernos de Proteção de Dados da União Europeia, Lisboa: CEDIS, Faculdade de Direito da Universidade Nova de Lisboa, 2022. Disponível em: https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/10/3.-Sandra-Barbosa.pdf.

Como consequência da transparência, tem-se os direitos de acesso, retificação, apagamento e portabilidade, os quais encontram-se previstos nos artigos 15 a 22 com a forma de exercê-los. Além disso, há a salvaguarda do direito de "obter intervenção humana" mencionado no artigo 22.º, a que se convencionou chamar "direito à explicação" com base na expressão "obter uma explicação sobre a decisão tomada" utilizada no considerando 71 do Regulamento.

Ao estabelecer a obrigação de o controlador informar os titulares sobre violações de dados pessoais que representem alto risco aos seus direitos e liberdades, o artigo 34.º do RGPD acaba por concretizar, de algum modo, o princípio da transparência.[43]

Ainda, é possível afirmar que a designação do Encarregado de Proteção de Dados (DPO), ao garantir que exista uma figura responsável por supervisionar o cumprimento da legislação e facilitar a comunicação entre o controlador, os titulares de dados e as autoridades de supervisão, seja uma materialização do princípio da transparência. Isso porque a presença do DPO promove clareza e acessibilidade para os titulares, que podem vir a buscar informações ou exercer seus direitos, reforçando a transparência nos processos de tratamento de dados pessoais.

Na LGPD brasileira, o princípio da transparência (artigo 6.º, VI)[44], juntamente do princípio do livre acesso (artigo 6.º, IV)[45], dá origem ao direito de acesso aos dados pessoais[46], este, que por sua vez, é consolidado pelos artigos 18 e 19[47]:

Acesso em: 17 jan. 2025. p.70

[43] Essa comunicação deve ser clara, compreensível e fornecer detalhes sobre a natureza da violação, os possíveis impactos e as medidas adotadas. Assim, promove-se a transparência ao garantir que os titulares sejam informados de forma adequada e possam tomar medidas para proteger seus interesses.

[44] (...) IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

[45] (...) IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

[46] artigo 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I – confirmação da existência de tratamento; II – acesso aos dados;(...)

[47] SCHLOTTFELDT, Shana. REVISÃO DE DECISÃO TOMADA COM BASE EM

> artigo 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I – confirmação da existência de tratamento;
> II – acesso aos dados;
> (…)
> VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> (…)
>
> artigo 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:
> I – em formato simplificado, imediatamente; ou
> II – por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular. (…)

Juntos, estes dispositivos permitem ao titular tomar conhecimento dos dados utilizados para as decisões automáticas, além da forma e da duração do tratamento.

Ademais, derivado do princípio da transparência, há de se falar no princípio da qualidade dos dados previsto no artigo 6.º V[48], que permite

---

TRATAMENTO AUTOMATIZADO: PREOCUPAÇÕES E CONSIDERAÇÕES SOBRE A EFETIVAÇÃO DA TRANSPARÊNCIA PARA COBRIR A DISCRIMINAÇÃO ALGORÍTIMICA E O PROFILING. In: MENDES, Laura Schertel Ferreira (Org.) et al. Anuário do Observatório da LGPD da Universidade de Brasília: análise comparada entre elementos da LGPD e do GDPR. Brasília: Universidade de Brasília, Faculdade de Direito, 2024. 2 v. pp. 117-136

[48] Artigo 6.º (...) V – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

que o titular demande a atualização e a correção de dados incompletos, inexatos ou desatualizados (artigo 18, III[49]).[50] Igualmente, se materializa através dos direitos à oposição e à exclusão (artigo18, VI)[51] e o princípio da não-discriminação (artigo 6.º, IX)[52], acionado caso o titular suponha estar sofrendo discriminação em razão do tratamento dos seus dados.

É imperioso que seja dessa forma ante a velocidade do avanço da tecnologia e do caráter transfronteiriço da internet, pelo que sem a devida transparência se torna praticamente impossível o controle pelo titular do fluxo de seus dados, bem como quaisquer fiscalizações pelos órgãos de controle.[53]

Por último, mas não menos importante, há de se falar na possibilidade de revisão de decisões automatizadas, previsto no artigo 20, *caput*, o que sugere acesso sempre em momento posterior à coleta de dados e desenvolvimento do algoritmo que os processa[54].

---

[49] artigo 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (…) III – correção de dados incompletos, inexatos ou desatualizados;

[50] SCHLOTTFELDT, Shana. REVISÃO DE DECISÃO TOMADA COM BASE EM TRATAMENTO AUTOMATIZADO: PREOCUPAÇÕES E CONSIDERAÇÕES SOBRE A EFETIVAÇÃO DA TRANSPARÊNCIA PARA COBRIR A DISCRIMINAÇÃO ALGORÍTIMICA E O PROFILING. In: MENDES, Laura Schertel Ferreira (Org.) et al. Anuário do Observatório da LGPD da Universidade de Brasília: análise comparada entre elementos da LGPD e do GDPR. Brasília: Universidade de Brasília, Faculdade de Direito, 2024. 2 v. pp. 117-136

[51] artigo 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...) VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no artigo 16 desta Lei;

[52] IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

[53] FLUMIGNAN, Silvano José Gomes; FLUMIGNAN, Wévertton Gabriel Gomes. Princípios que Regem o Tratamento de Dados no Brasil. In: LIMA, Cíntia Rosa Pereira de (Coord.) Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020. p.132.

[54] FERNANDES, Micaela Barros Barcelos; OLIVEIRA, Camila Helena Melchior Baptista de. "O artigo 20 da LGPD e os desafios interpretativos ao direito à revisão das decisões dos agentes de tratamento pelos titulares de dados." Revista de Direito e as Novas Tecnologias. V.8/2020, jul.-set./2020

3. Algoritmos, Inteligência Artificial e os Desafios de Transparência

a. O processamento de dados pessoais pelos algoritmos

Os dados pessoais ganharam importância mercadológica enorme conforme o avanço tecnológico passou a permitir a vinculação destes a pessoas reais, tornando-se uma extensão de suas personalidades no meio digital. A possibilidade de processar grandes bases de dados por algoritmos permitiu a criação de ferramentas cada vez mais precisas e capazes de prever tendências e comportamentos humanos.[55] Segundo o ChatGPT[56], um algoritmo é uma sequência finita de instruções bem definidas e ordenadas que, quando executadas, visam resolver um problema específico ou realizar uma tarefa determinada.[57]

É um fato inegável que os algoritmos são alimentados por dados[58-59]. Com base nestes, algoritmos que usam da inteligência artificial podem vir a negar crédito a pessoas, demitir ou contratar pessoas com base em seus dados ou padrões estatísticos dos dados que possui, dentre outras situações que podem ocorrer. Assim que os algoritmos

---

[55] WANDERER, Bertrand. Economia movida a dados e o papel das plataformas digitais. Journal of Law and Regulation, v. 9, n. 2, p. 22–43, 2023. p.26.

[56] "Embora o ChatGPT possa ser tecnicamente descrito como um algoritmo de IA, sua complexidade o aproxima mais de um modelo estatístico baseado em aprendizado de máquina, diferindo dos algoritmos tradicionais em sua forma de funcionamento, transparência e interpretabilidade." OPENAI. Resposta gerada pelo modelo ChatGPT. Disponível em: https://chat.openai.com/. Acesso em: 06 fev. 2025.

[57] OPENAI. Resposta gerada pelo modelo ChatGPT. Disponível em: https://chat.openai.com/. Acesso em: 21 jan. 2025.

[58] RIBEIRO, Elieser. "A potência dos dados para a inteligência artificial." Medium, 17 ago. 2020. Disponível em: https://medium.com/@elieser_ribeiro/a-pot%C3%AAncia-dos-dados-para-a-intelig%C3%AAncia-artificial-703f1c05750f. Acesso em: 21 jan. 2025.

[59] "Sim, é correto afirmar que um algoritmo é alimentado por dados. Um algoritmo utiliza entradas (dados) para executar sua sequência de instruções e produzir saídas (resultados). Esses dados podem ser estáticos (pré-definidos) ou dinâmicos (fornecidos em tempo real), e sua qualidade e relevância são cruciais para o desempenho e a precisão do algoritmo, especialmente em sistemas baseados em aprendizado de máquina." OPENAI. Resposta gerada pelo modelo ChatGPT para a seguinte pergunta: "é correto afirmar que o algoritmo é alimentado por dados?". Disponível em: https://chat.openai.com/. Acesso em: 21 jan. 2025.

estão presentes no dia a dia da população sem que muitas vezes saiba: vive-se numa verdadeira vigilância algorítmica.[60]

Segundo o Regulamento de IA europeu, entende-se por Sistema de IA:

> (...) um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais.[61]

Para além dos algoritmos tradicionais, há de se falar na técnica de aprendizagem de máquina (*machine learning*)[62], impulsionada pela explosão do volume de dados digitais. Nessa, os sistemas são expostos a um grande número de exemplos (dados) e devem extrair deles padrões recorrentes.[63]

---

[60] "Dataveillance is the systematic creation and/or use of personal data for the investigation or monitoring of the actions or communications of one or more persons." CLARKE, Roger; GREENLEAF, Graham. Dataveillance Regulation: A Research Framework. UNSW Law Research Series, 7 nov. 2017. P.3.

[61] Artigo 3.º (1) do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de junho de 2024 que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.o 300/2008, (UE) n.o 167/2013, (UE) n.o 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial).

[62] O termo "aprendizado de máquina" (machine learning, em inglês) faz referência a um método algorítmico que permite a um sistema chegar a conclusões mediante tentativas e erros, até alcançar o resultado almejado. O sistema aprende com seus erros em uma espécie de inteligência artificial. Entre as modalidades de aprendizado de máquina, existe o "aprendizado profundo" (deep learning, em inglês), que utiliza sistemas paralelos para aprender e, muitas vezes, seu resultado final pode ser diferente do antevisto por quem desenvolveu o algoritmo. Ver: BURRELL, Jenna. "How the machine 'thinks': Understanding opacity in machine learning algorithms. Big Data & Society, v. 3, n. 1. SAGE Publications, 2016.

[63] DEVILLÉ, Rembrandt; SERGEYSSELS, Nico; MIDDAG, Catherine. Basic Concepts of AI for Legal Scholars. In: BRUYNE, Jan De; VANLEENHOVE, Cedric (ed.). Artificial Intelligence and the Law. Antuérpia: Intersentia, 2021. p. 1-22, p. 5.

A depender da forma como os dados são apresentados ao sistema, a aprendizagem de máquina pode seguir diferentes metodologias. Na aprendizagem supervisionada, o algoritmo é treinado com exemplos cujas respostas corretas já são conhecidas, permitindo-lhe ajustar seus parâmetros com base nesse feedback. Na aprendizagem não supervisionada, o sistema apenas recebe dados brutos e deve, por si só, identificar agrupamentos, relações ou estruturas internas.[64]

Em razão desta capacidade dos algoritmos de gerar um padrão comportamental dos sujeitos através de uma correlação dos dados que possui, surge a preocupação com os dados pessoais que os alimentam.[65]

Inclusive, o artigo 4.º, n.º 4 do RGPD aborda o *profiling* com ênfase em uso para previsão comportamental. E, para que seja caracterizado como criação de perfil, há de haver algum processamento automatizado, pelo que qualquer participação humana no processo não descaracteriza o fenômeno[66].

Há de se falar, também, que em sistemas mais complexos, as sequências pré-definidas podem ser alteradas de acordo com os dados que os alimentam e também pelas conclusões intermediárias. Essa natureza adaptativa tem se tornado mais comum nos sistemas de inteligência artificial e aprendizado de máquina capazes de influenciar as conclusões intermediárias – de modo que não seja mais possível prever os resultados finais ou entender sua lógica subjacente.[67]

---

[64] Ibidem, p.6.

[65] ABRANTES, Paula Cotrim de. "Desafios e dilemas da proteção de dados pessoais na era da cultura algorítmica." In: SciELO Preprints. DOI 10.1590/SciELOPreprints.7141. p. 1-27, 2023. p.11.

[66] Article 29 Working Party. 2018. Guidelines on Autoimated «individual decision-making and Profiling for the purposes of Regulation 2016/679. WP251revb.01

[67] "Algoritmos baseados em metodologias de aprendizado de máquina e aprendizado profundo podem chegar a várias conclusões intermediárias antes de atingir o seu resultado final. Estas servem para ensinar o algoritmo a atingir o resultado correto, a partir de tentativa e erro, ou até mesmo alterar o algoritmo para atingir outros resultados, alguns deles não antevistos por seus desenvolvedores." MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? Rio de Janeiro: Instituto Igarapé, 2018. 27 p. (Artigo Estratégico, 39). p.2.

Segundo Goodman e Flaxman, algoritmos de aprendizado de máquina supervisionado para regressão ou classificação são baseados na descoberta de associações e/ou correlações confiáveis para auxiliar na previsão precisa fora da amostra, sem a preocupação acerca do raciocínio causal ou de explicação para além do sentido estatístico, através do qual é possível medir a quantidade de variância explicada por um preditor.[68] Daí surge a preocupação com a transparência destes processos.

Essa complexidade pode ser entendida como opacidade, vez que impede que as pessoas entendam e verifiquem se seus dados pessoais são tratados de forma legítima, adequada e proporcional. Daí surge uma preocupação: a falta de transparência sobre o funcionamento dos algoritmos indica a tendência de que esses mecanismos venham a segregar determinadas informações, privilegiem outras, reproduzindo padrões de preconceito e discriminação, reforçando, assim, o aprofundamento das desigualdades da sociedade[69-70].

Essa opacidade pode se apresentar em diferentes formas: a opacidade intencional por parte de corporações ou instituições que mantém seus processos de tomada de decisão longe do escrutínio público;[71] a opacidade enquanto falta de conhecimento técnico[72], a qual decorre do reconhecimento de que compreender a operação é uma habilidade especializada restrita a minoria da população; e a opacidade de quando há desalinhamento entre as complexas operações matemáticas por certos

---

[68] GOODMAN, Bryce; FLAXMAN, Seth. European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation". AI Magazine, v. 38, n. 3, p. 50-57, 2017. p. 6.

[69] Vê-se o uso desse tipo de inteligência artificial em atividades como processos seletivos para empregos, aplicação de tarifas de planos de saúde, obtenção de crédito, dentre outros.

[70] Nesse sentido, Cathy O'NEIL já considerou os algoritmos como armas de destruição matemática: O'NEIL, Cathy. Weapons of math destruction: how big data increases inequality and threatens democracy. New York: Crown Publishing Group, 2016.

[71] Segundo Diego Machado, pode se dar através do uso de técnicas computacionais para controlar a burla do sistema e da tutela jurídica do segredo comercial ou industrial para ofuscar o real funcionamento do algoritmo. MACHADO, Diego. Algoritmos e Proteção de Dados Pessoais. São Paulo: Almedina, 2023. E-book. p.178.

[72] Chamado por Jenna Burrell, de "Opacity as technical illiteracy", em tradução livre "opacidade como analfabetismo técnico". Burrell, Jenna. How the machine "thinks": Understanding opacity in machine learning algorithms. Big Data & Society, 2016 3(1), p.4.

algoritmos de aprendizado de máquina e a interpretação feita pelo ser humano.[73]

Colocando o direito à proteção de dados pessoais em perspectiva, a existência de opacidade e invisibilidade no processo de formação e de aplicação do perfilamento automatizado confronta a própria configuração deste direito fundamental como instrumento de transparência. A opacidade pontuada pode criar verdadeiros embaraços ao uso de mecanismos de controle e responsabilização do poder exercido por agentes de tratamento, públicos ou privados. Isso somado da invisibilidade ou dificuldade de compreensão das aplicações tecnológicas, pelo que cresce o perigo de inviabilizar a contestabilidade das operações de tratamento e decisões automatizadas, ferindo a participação dos titulares dos dados no processo de tomada de decisão algorítmica.

Porém, nesse contexto torna-se necessário reconhecer que a intensidade e a natureza dos riscos associados à opacidade algorítmica e o consequente impacto sobre a privacidade podem variar de acordo com a interação realizada entre o titular dos dados (usuário) e a tecnologia, o processamento adotado e o grau de intermediação da inteligência artificial.

No caso do uso individual de um navegador ou de uma aplicação proprietária de IA generativa – como o ChatGPT, Copilot e Gemini, os dados introduzidos pelo utilizador, bem como os de interação, são processados e armazenados em servidores externos, sob regime jurídico e técnico definido pelo fornecedor, com elevada possibilidade de transferência internacional e reutilização para fins de treino.[74] [75]

---

[73] MACHADO, Diego. Algoritmos e Proteção de Dados Pessoais. São Paulo: Almedina, 2023. E-book. p.178.

[74] "The terms say ChatGPT may automatically collect personal information and usage information about a user's use of the services, such as the types of content that they view or engage with, the features they use and the actions they take. The terms say OpenAI may use the data users provide to improve their future models. (...)However, the terms do not disclose whether ChatGPT can display targeted advertisements to users, send third-party marketing communications, or track users based on their interactions with ChatGPT on other apps or services across the internet for advertising purposes." COMMON SENSE. Privacy Evaluation for ChatGPT. 26 jan. 2024. Disponível em: https://privacy.commonsense.org/evaluation/ChatGPT Acesso em 10 ago 2025. Ver também: OpenAI. How your data is used to improve model performance. Disponível em: https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance Acesso em 11 ago 2025.

[75] Em se tratando de metadados de interação (data e hora da solicitação, endereço IP,

De outro lado, ao utilizar plataformas de redes sociais, o titular de dados, apesar de não necessariamente interagir diretamente com a IA, permanece sujeito à análise comportamental e à segmentação algorítmica não transparente, cujo processamento decorre de observação contínua e agregada, tornando mais difícil a percepção e a contestação do tratamento.

Tal diversidade de contextos impõe que a concretização do princípio da transparência seja sensível à configuração técnica do tratamento, pois o grau de exposição e as salvaguardas necessárias variam substancialmente em função da arquitetura adotada. Considerando os potenciais riscos para os interesses e direitos do titular dos dados, uma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis é vedada pelo artigo 22, n.º 1 do RGPD[76]. A LGPD, ainda que inspirada na norma europeia, não proíbe o tratamento totalmente automatizado de dados. Muito pelo contrário, ela o autoriza no artigo 20, prevendo o direito à revisão como forma de proteção aos titulares.

b. Transparência no uso de algoritmos

Na maioria das vezes, as pessoas não sabem o peso dos seus dados utilizados pelos algoritmos e quais fatores são levados em consideração para a tomada de decisão. Se não houver a devida transparência, a probabilidade de que a programação do algoritmo esteja permeada de vieses e preconceitos dos programadores, intencionais ou não, que

parâmetros técnicos da sessão, tipo de dispositivo e navegador, etc.), estes podem ser processados com a finalidade de prestar o serviço, manter a segurança operacional e, salvo manifestação em contrário do utilizador, contribuir para o treino e melhoria dos modelos de linguagem. Tal enquadra-se no previsto no artigo 4.º, n.º 2, do RGPD e no artigo 5.º, X, da LGPD, abrangendo tratamento de dados desde a coleta até o armazenamento, independentemente de o dado ser textual ou técnico (metadado).

[76] O termo "direito" contido nesta disposição não significa que o artigo 22.º, n.º 1, seja aplicável somente quando ativamente invocado pelo titular dos dados. O artigo 22.º, n.º 1 estabelece uma proibição geral da tomada de decisões com base exclusivamente no tratamento automatizado, a qual aplica-se independentemente de o titular dos dados adotar uma medida relativa ao tratamento dos seus dados pessoais.

podem levar a erros de diagnóstico e a graves discriminações é altíssima. Além disso, é possível que as correlações encontradas no processamento sejam consideradas causalidades de forma equivocada, reforçando discriminações[77].

Segundo Castelluccia e Métayer, transparência não significa necessariamente disponibilidade para o público, mas a disponibilidade para agente de auditoria ou certificação da codificação do processo de tomada de decisões com sua documentação de projeto, parâmetros e o conjunto de dados de aprendizado quando a tomada de decisão algorítmica se baseia no aprendizado de máquina.

Já a explicabilidade seria a disponibilidade de explicações sobre o processo de tomada de decisões, exigindo-se o fornecimento de informações além da própria tomada de decisão algorítmica. Explicações estas que podem ser de diferentes operacionais, causais, globais (sobre todo o algoritmo) ou sobre resultados específicos. Ademais, há de haver diferentes modos de explicação a depender dos destinatários desta (por exemplo, profissionais ou indivíduos), seu nível de especialização e seus objetivos (contestar uma decisão, tomar medidas para obter uma decisão, verificar a conformidade com as obrigações legais etc.).

Quando o algoritmo toma decisões baseadas em regras predefinidas é mais fácil de haver a explicação, providenciando a informação do tratamento de forma compreensível ao usuário, como o princípio da transparência exige. Porém, em se tratando de machine learning, como demonstrado, há uma dificuldade a ser enfrentada.

Em âmbito europeu, no que diz respeito à tomada de decisões automatizada, o princípio da transparência, ao lado da legalidade e da equidade devem reger a utilização e a criação de algoritmos, que por sua vez, tratam e processam dados pessoais, consoante o artigo 5.º, n.º1, alínea a) do RGPD.

---

[77] FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019. p. 39.

Assim, o responsável pelo tratamento de dados tem a transparência enquanto base dos seus deveres, pelo que deve certificar-se de que explique de forma clara e inteligível aos titulares dos dados estes processos, as suas consequências e fornece-lhes ferramentas para agirem contra eles, se assim o pretenderem[78], ou seja, deve informar a pessoa em causa sobre a lógica subjacente aos algoritmos. É possível afirmar que a transparência seja uma das principais formas de compreensibilidade do processo de tomada de decisões pelo algoritmo.

Alinhando-se com os requisitos de informação e acesso presentes nos arts. 13.º a 15.º do RGPD, enquanto forma de materialização da transparência, a informação fornecida tem de abordar quais os dados que foram recolhidos, que estão a ser processados ao abrigo desses meios, e as suas consequências[79]. Ademais, o princípio do tratamento transparente exige que o titular dos dados seja informado da definição de perfis e das consequências que daí advêm[80]. Portanto publicidade direcionada frutos de *profiling* deveriam dar um tratamento transparente de seus dados.

O uso de algoritmos cada vez mais corriqueiro no *online*, especialmente nos sistemas de recomendação e de publicidade direcionada coloca a transparência no tratamento dos dados pessoais nesse contexto no centro do direito digital europeu para além do RGPD. Tanto o Regulamento dos Mercados Digitais (DMA) quanto no Regulamento dos Serviços Digitais (DSA)[81] tratam expressamente deste tema.

O DMA impõe aos gatekeepers a obrigação de divulgar, de forma clara e acessível, os critérios utilizados nos sistemas de recomendação e a lógica utilizada, para que os usuários possam entender por qual razão

---

[78] BARBOSA, Sandra. "A importância da transparência e explicabilidade no uso de decisões automatizadas pelo artigo 22.º do RGPD." p.82

[79] Idem, p.70

[80] Considerando 60 do RGPD.

[81] Ambos os regulamentos Digital Markets Act (DMA) e Digital Services Act (DSA) são frutos do pacote legislativo da União Europeia chamado Pacote dos Serviços Digitais – Digital Services Package. Ver: Digital services package. Disponível em: https://www.consilium.europa.eu/en/policies/digital-services-package/

determinados conteúdos lhes são exibidos[82]. O DSA reforça essa perspectiva ao exigir que as plataformas digitais informem, inclusive nos casos de anúncios personalizados, se houve uso de dados pessoais e com base em quais parâmetros estes lhe foram direcionadas, além de proibir a segmentação com base em dados sensíveis[83].

Conforme anteriormente demonstrado, a LGPD brasileira prevê, no seu artigo 20, aos titulares o direito à revisão das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses. E como pressuposto ao exercício desse direito, previu que o titular dos dados deverá tenha acesso, sempre que solicitado, a informações claras e adequadas sobre os procedimentos utilizados para se chegar a decisões que interfiram em sua esfera jurídica, resguardando-se os segredos comercial e industrial do controlador (artigo 20 § 1.º, da LGPD).

c. A tensão entre inovação tecnológica e proteção de dados

É fato que os algoritmos funcionam transformando dados de entrada em resultados com base em regras estabelecidas e objetivos previamente definidos, como a identificação de padrões ou correlações. No entanto, compreender plenamente como determinados resultados são alcançados a partir de *inputs* específicos pode ser uma tarefa extremamente complexa.

O ambiente digital automatizado e telemático apresenta particularidades que intensificam a exposição dos indivíduos a riscos técnicos. Diante da complexidade dos sistemas computacionais, das infraestruturas de rede e das técnicas avançadas de processamento de dados, os usuários, em sua maioria, não possuem conhecimento especializado para compreender integralmente os mecanismos que regem a coleta, o armazenamento e o tratamento de suas informações. A crescente

[82] Artigo 27.o
[83] Artigo 26.º.

digitalização das interações, impulsionada pelas plataformas digitais, pela massificação do uso de dados e pelo avanço da inteligência artificial, amplia essa condição de vulnerabilidade, tornando os titulares de dados mais suscetíveis a práticas tecnológicas cuja transparência nem sempre é acessível ao público leigo.[84]

Assim, o titular dos dados ocupa uma posição fragilizada, marcada por uma relação desigual em face do responsável pelo tratamento. Geralmente, o tratamento de dados pessoais é impulsionado por interesses econômicos, seja pela geração direta de lucro, seja pela redução de custos ou aumento de eficiência, muitas vezes de forma discreta e quase imperceptível pelo usuário.

Por outro lado, o titular encontra-se exposto a operações de tratamento que podem invadir sua esfera jurídica, frequentemente sem que ele tenha qualquer conhecimento sobre elas. Durante todas as etapas desse processo informações que pertencem ao titular são passíveis de análise para a criação de perfis baseados em deduções e correlações, as quais servirão de base para decisões posteriormente. Em geral, o indivíduo impactado pela decisão não tem clareza sobre os motivos que a embasaram.[85] Daí a importância do princípio da transparência no tratamento de dados pessoais obtidos na internet, que deve ser colocado em prática e fiscalizado pelas autoridades competentes.

Pasquale defende o uso de auditores que tenham acesso ao algoritmo de modo a garantir que as classificações sejam não-discriminatórias, de modo a combater a opacidade intencional[86]. Ademais, a educação computacional faz-se necessária para um melhor entendimento do que se passa com os dados pessoais.

---

[84] MARQUES, Claudia Lima; MUCELIN, Guilherme. "Vulnerabilidade na era digital: um estudo sobre os fatores de vulnerabilidade da pessoa natural nas plataformas, a partir da dogmática do Direito do Consumidor." Civilistica.com, Rio de Janeiro, v. 11, n. 3, p. 1–30, 2022. p.8.

[85] COSTA, Inês. A proteção de dados pessoais no contexto da União Europeia. Revista Electrónica de Direito, n.º 1, v. 24, fev. 2021, p. 65-66.

[86] PASQUALE, Frank. The Black Box Society.

Considerações finais

Embora a transparência seja fundamental para um meio digital seguro, sua implementação enfrenta desafios significativos, especialmente em um contexto marcado por tensões entre direitos fundamentais e práticas de vigilância. Faz-se, então, necessário um equilíbrio cuidadoso entre a proteção da privacidade e a promoção da transparência para garantir a confiança dos usuários.

Buscou-se demonstrar no presente artigo que a concretização do princípio da transparência no tratamento de dados pessoais na internet manifesta-se por meio da clara comunicação das práticas de coleta, uso e armazenamento de dados. Especialmente nas práticas algorítmicas, as plataformas digitais devem disponibilizar políticas de privacidade acessíveis e compreensíveis, indicando explicitamente quais informações são coletadas, com que finalidades e por quanto tempo serão mantidas. Além disso, deve ser garantido o direito dos usuários de acessar, corrigir e excluir seus dados de forma simples e eficaz. Essas medidas asseguram que os indivíduos possam tomar decisões informadas sobre o compartilhamento de suas informações pessoais online.

Ao longo do estudo, foram apontadas diversas convergências entre a LGPD e o RGPD com relação à transparência e à proteção de dados pessoais, porém, com relação às decisões automatizadas nota-se uma divergência relevante: enquanto o modelo europeu preza pela intervenção humana prévia como salvaguarda, o modelo brasileiro estabelece a revisão posterior como forma de contestação. Essa distinção regulatória reflete visões diferentes sobre o equilíbrio entre a inovação tecnológica e o direito à proteção dos dados pessoais.

A falta de transparência sobre como algoritmos processam os dados e a lógica por trás de perfis automatizados e decisões baseadas em IA não podem ser normalizadas, nas suas diferentes formas de apresentação. Desafios podem ser mitigados através da educação digital, promovendo a conscientização dos usuários sobre seus direitos e práticas de privacidade. No âmbito da criação dos algoritmos, deve haver o

fomento para que o *design* das ferramentas respeitem a privacidade desde a concepção. E, através de fiscalização e auditorias, deve haver a garantia do cumprimento das disposições legais mencionadas ao longo do artigo.

Referências Bibliográficas

ABRANTES, Paula Cotrim de. "Desafios e dilemas da proteção de dados pessoais na era da cultura algorítmica." In: *SciELO Preprints*. DOI 10.1590/SciELOPreprints.7141. p. 1-27, 2023. Disponível em: https://preprints.scielo.org/index.php/scielo/preprint/view/7141 Acesso em 08 jan 2025.

BARBOSA, Sandra. "A importância da transparência e explicabilidade no uso de decisões automatizadas pelo artigo 22.º do RGPD." *Cadernos de Proteção de Dados da União Europeia*, Lisboa: CEDIS, Faculdade de Direito da Universidade Nova de Lisboa, 2022.

BERTOLLI, Emilia. "Os riscos dos testes genéticos." *Varonis*, 2023. Disponível em: https://www.varonis.com/pt-br/blog/os-riscos-dos-testes-geneticos. Acesso em: 20 jan. 2025.

BEZERRA, Daniel Teixeira; FURTADO, Gabriel Rocha. "A (in)constitucionalidade da Medida Provisória n.º 954/2020: o marco jurisprudencial brasileiro do direito fundamental à proteção de dados pessoais." *Civilistica.co*m, Rio de Janeiro, v. 12, n. 1, p. 1–13, 2023. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/849. Acesso em: 6 fev. 2025.

BRANCO, Sérgio; TEFFÉ, Chiara de (coord.). *Plataformas digitais e proteção de dados pessoais*. Rio de Janeiro: ITS – Instituto de Tecnologia e Sociedade, 2023. (Diálogos da pós-graduação em direito digital). Disponível em: https://itsrio.org/wp-content/uploads/2016/12/20231023_Livro_Pos_ITS-UERJ_Plataformas-digitais-protecao-de-dados_COMPLETO.pdf. Acesso em: 11 jan. 2025.

BURRELL, Jenna. "How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, v. 3, n. 1. SAGE Publications, 2016.

CASTELLUCCIA, Claude; MÉTAYER, Daniel Le. "Understanding algorithmic decision-making: Opportunities and challenges." *European Parliamentary Research Service,* 2019. Disponível em: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2019)624261. Acesso em: 31 jan 2025.

COSTA, Inês. "A proteção de dados pessoais no contexto da União Europeia." *Revista Electrónica de Direito*, n.º 1, v. 24, fev. 2021

CORDEIRO, A. Barreto Menezes. *Direito da proteção de dados: à luz do RGPD e da Lei n.º 58/2019.* Coimbra: Almedina, 2022.

CLARKE, Roger; GREENLEAF, Graham**.** "Dataveillance Regulation: A Research Framework*." UNSW Law Research Series*, 7 nov. 2017. Disponível em: https://ssrn.com/abstract=3073492. Acesso em: 20 jan. 2025.

FICO, Bernardo de Souza Dantas; NÓBREGA, Henrique Meng. "The Brazilian Data Protection Law for LGBTQIA+ People: Gender identity and sexual orientation as sensitive personal data" *Revista Direito e Práxis*, v. 13, n. 2, p. 1262–1288, 2022.

DEVILLÉ, Rembrandt; SERGEYSSELS, Nico; MIDDAG, Catherine. Basic Concepts of AI for Legal Scholars. In: BRUYNE, Jan De; VANLEENHOVE, Cedric (ed.). **Artificial Intelligence and the Law**. Antuérpia: Intersentia, 2021. p. 1-22.

DONEDA, Danilo. "O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS." In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito digital*: direito privado e internet. 3. ed. Indaiatuba: Editora Foco, 2020. pp.33-49.

FÁCIO, Rafaella Nátaly. "A transparência e o direito de acesso no tratamento de dados pessoais: considerações sobre intersecções entre Lei Geral de Proteção de Dados e Lei de Acesso à Informação no Brasil." *Rev. Eurolatin. de Derecho Adm*., Santa Fe, v. 10, n. 2, e247, jul./dic. 2023.

FERNANDES, Micaela Barros Barcelos; OLIVEIRA, Camila Helena Melchior Baptista de. "O artigo 20 da LGPD e os desafios interpretativos ao direito à revisão das decisões dos agentes de tratamento pelos titulares de dados." *Revista de Direito e as Novas Tecnologias*. V.8/2020, jul.-set./2020

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019

FLUMIGNAN, Silvano José Gomes; FLUMIGNAN, Wévertton Gabriel Gomes. "Princípios que Regem o Tratamento de Dados no Brasil." In: LIMA, Cíntia Rosa Pereira de (Coord.) *Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019*. São Paulo: Almedina, 2020.

GOODMAN, Bryce; FLAXMAN, Seth. European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation". *AI Magazine*, v.

38, n. 3, p. 50-57, 2017. Disponível em: https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/2741. Acesso em: 10 ago. 2025.

HOOFNAGLE, Chris Jay; SOLTANI, Ashkan; GOOD, Nathan; WAMBACH, Dietrich James; AYENSON, Mika D. "Behavioral Advertising: The Offer You Cannot Refuse." *Harvard Law & Policy Review*, vol.6, n. 273, 2012. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2137601

KHAN, Lina. "What makes tech platforms so powerful. Digital Platforms and Concentration." *Second Annual Antitrust and Competition Conference Stigler Center for the Study of the Economy and the State University of Chicago Booth School of Business*. A Pro-Market Production. 2018. p. 14.

LUCCA, Newton De, MACIEL, Renata Mota. "A PROTEÇÃO DOS DADOS PESSOAIS NO BRASIL A PARTIR DA LEI 13,709/2018: EFETIVIDADE?" In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito digital: direito privado e internet.* 3. ed. Indaiatuba: Editora Foco, 2020. pp.211-228.

MACHADO, Diego. *Algoritmos e Proteção de Dados Pessoais*. São Paulo: Almedina, 2023. *E-book.* ISBN 9786556279602.

MAGALHÃES, Filipe. *Manual RGPD*. Ordem dos Contabilistas Certificados (OCC), 2018. Disponível em: https://www.occ.pt/fotos/editor2/rgpd--fmagalhaesmanual.pdf. Acesso em: 11 jan. 2025.

MARQUES, Cláudia Lima; MUCELIN, Guilherme. "Vulnerabilidade na era digital: um estudo sobre os fatores de vulnerabilidade da pessoa natural nas plataformas, a partir da dogmática do Direito do Consumidor." *Civilistica.com*, Rio de Janeiro, v. 11, n. 3, p. 1–30, 2022. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/872. Acesso em: 5 jan. 2025.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? Rio de Janeiro: Instituto Igarapé, 2018. 27 p. (Artigo Estratégico, 39). Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao--de-Dados-no-Brasil.pdf Acesso em 10 jan. 2025.

Organisation for Economic Co-operation and Development (OECD). "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", *OECD Publishing*, Paris, 2002 https://doi.org/10.1787/9789264196391-en.

O'NEIL, Cathy. *Weapons of math destruction: how big data increases inequality and threatens democracy*. New York: Crown Publishing Group, 2016.

PASQUALE, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*-. Cambridge: Harvard University Press, 2015.

PUNIT BHATIA. *Intro to GDPR : A Plain English Guide to Compliance*. Zagreb, Croatia: Advisera Expert Solutions Ltd, 2018. Disponível em: https://research.ebsco.com/linkprocessor/plink?id=15c0c5c9-ff48-39f7-8af6-e648dbb1ae5a. Acesso em: 12 jan. 2025.

RIBEIRO, Elieser. "A potência dos dados para a inteligência artificial." *Medium*, 17 ago. 2020. Disponível em: https://medium.com/@elieser_ribeiro/a-pot%C3%AAncia-dos-dados-para-a-intelig%C3%AAncia-artificial-703f1c05750f. Acesso em: 21 jan. 2025.

ROWLAND, Diane; MACDONALD, Elizabeth; OVERTON, Andrew Charles. *Information technology law*. 3rd ed. London: Cavendish Publishing, 2005.

RUIZ, Evandro Eduardo Seron. Anonimização, pseudonimização e desanonimização de dados pessoais. In: LIMA, Cíntia Rosa Pereira. *Comentários a Lei Geral de Proteção de Dados – Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019.* São Paulo: Almedina Brasil, 2020.

SCHLOTTFELDT, Shana. "REVISÃO DE DECISÃO TOMADA COM BASE EM TRATAMENTO AUTOMATIZADO: PREOCUPAÇÕES E CONSIDERAÇÕES SOBRE A EFETIVAÇÃO DA TRANSPARÊNCIA PARA COBRIR A DISCRIMINAÇÃO ALGORÍTIMICA E O PROFILING." In: MENDES, Laura Schertel Ferreira (Org.) et al. *Anuário do Observatório da LGPD da Universidade de Brasília: análise comparada entre elementos da LGPD e do GDPR*. Brasília: Universidade de Brasília, Faculdade de Direito, 2024. 2 v. pp. 117-136

SUNYAEV, Ali. *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies.* Cham: Springer, 2020.

WANDERER, Bertrand. "Economia movida a dados e o papel das plataformas digitais." *Journal of Law and Regulation*, v. 9, n. 2, p. 22–43, 2023. Disponível em: https://periodicos.unb.br/index.php/rdsr/article/view/43231. Acesso em: 6 fev. 2025.

A Tutela Jurisdicional das ações propostas para reagir às decisões sancionatórias da CNPD: uma análise crítica do regime consagrado na Lei n.º 58/2019, de 8 de agosto

Diana Camões[1]

Resumo: Este estudo visa refletir sobre a tutela jurisdicional das ações propostas para reagir às decisões sancionatórias da Comissão Nacional de Proteção de Dados, analisando a incoerência entre a Lei n.º 58/2019 e o Estatuto dos Tribunais Administrativos e Fiscais. A incompreensível desatenção do legislador tem levado a sucessivos conflitos negativos de jurisdição. Estas ações não podem continuar dependentes da incerteza quanto ao tribunal competente. Analisamos a jurisprudência do Tribunal de Conflitos, bem como as possíveis soluções para este problema.

Palavras-chave: Regulamento Geral sobre a Proteção de Dados; Lei n.º 58/2019; Estatuto dos Tribunais Administrativos e Fiscais; Jurisdição; Comissão Nacional de Proteção de Dados.

Abstract: This study aims to reflect on the jurisdictional protection of actions brought to challenge the sanctioning decisions of the Portuguese Data Protection Authority, by analyzing the inconsistency between Law no. 58/2019 and the Statute of the Administrative and Tax Courts. The legislator's incomprehensible inattention has resulted in successive

[1] Doutoranda em Ciências Jurídico-Políticas na Faculdade de Direito da Universidade de Lisboa.
ORCID: 0000-0001-8827-007X

negative conflicts of jurisdiction. These actions cannot remain subject to uncertainty regarding the competent court. We will examine the case law of the Court of Conflicts and consider possible solutions to address this issue.

Key Words: General Data Protection Regulation; Law no. 58/2019; Statute of the Administrative and Tax Courts; Jurisdiction; Portuguese Data Protection Authority.

1. Introdução[2]

O nosso estudo visa refletir sobre a tutela jurisdicional conferida pela Lei n.º 58/2019[3], de 8 de agosto, a qual procedeu à execução na ordem jurídica nacional do RGPD[4], relativamente às ações propostas em reação às decisões sancionatórias da CNPD. A verdade é que o legislador português, aquando da execução para o ordenamento jurídico nacional, cometeu vários erros e imprecisões, sendo que a versão final do diploma

[2] Lista de siglas e abreviaturas: AEPD – Autoridade Europeia para a Proteção de Dados; Art. – Artigo; CC- Código Civil; CDFUE- Carta dos Direitos Fundamentais da União Europeia; CNPD – Comissão Nacional de Proteção de Dados; CPC- Código do Processo Civil; CRP – Constituição da República Portuguesa; ETAF – Estatuto dos Tribunais Administrativos e Fiscais; LOSJ – Lei da Organização do Sistema Judiciário; N.º – Número; p. – página; pp. – páginas; RGPD – Regulamento Geral sobre a Proteção de Dados; UE – União Europeia; TFUE – Tratado sobre o Funcionamento da União Europeia; TJ – Tribunal de Justiça; TJUE – Tribunal de Justiça da União Europeia; STA – Supremo Tribunal Administrativo; STJ – Supremo Tribunal de Justiça.

[3] Lei n.º 58/2019, de 8 de agosto. Revogou a Lei n.º 67/98, de 26 de outubro.

[4] Regulamento (UE) 2016/679, de 27 de abril, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Revogou a Diretiva (UE) 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. O atual estado de arte é resultado de uma longa evolução operada ao nível do direito derivado, direito primário e jurisprudência do TJUE. Sobre esta evolução *vide* MONIZ, Graça Canto – *Manual de Introdução à Proteção de Dados Pessoais,* Almedina, 2023, Coimbra, pp. 8-16.

contém disposições contrárias ao RGPD. [5][6]

Um dos preceitos mais controversos, fruto de alguma desatenção do legislador, está relacionado com a competência dos tribunais para avaliar a validade de coimas aplicadas pela autoridade de controlo nacional. De facto, a Lei de Execução n.º 58/2019 é clara ao afirmar que "as ações propostas contra a CNPD são da competência dos tribunais administrativos."[7] Porém, tal disposição entra (como veremos) em confronto com o ETAF[8], algo que gera incerteza para o julgador no momento da aplicação da Lei.

Se o RGPD permitiu dar um passo muito importante no sentido de atualizar o escopo normativo em matéria de direito da proteção de

---

[5] Problema para o qual a CNPD, no Parecer 20/2018, alertou o legislador, aquando da apresentação da proposta final do diploma. Inclusive, na Deliberação 2019/494, a CNPD declarou desaplicar, em ordem a assegurar o princípio do primado e a efetividade do RGPD, as seguintes normas: n.os 1 e 2 do art. 2.º, n.º 1 do art. 20.º, art. 23.º, al. a) do n.º 3 do art. 28.º, al. a), h) e k) do n.º 1 do art. 37.º, n.º 2 do art. 37.º, al. b) do n.º 1 do art. 38.º, n.º 2 do art. 38.º, n.os 1 e 3 do art. 39.º, n.º 2 do art. 61.º, n.º 2 e n.º 2 do art. 62.º. Sobre o tema na doutrina *vide* CORDEIRO, A. Barreto Menezes – "A Interpretação dos Regulamentos Europeus das correspondentes leis de execução: o caso paradigmático do RGPD e da Lei n.º 58/2019", *Revista de Direito e Tecnologia,* Volume 1, N.º 2, 2019, pp. 175-200(194-195) e CALVÃO, Filipa Urbano – "A Lei n.º 58/2019, de 8 de agosto: incongruências e insuficiências na execução do RGPD", *Revista de Direito Administrativo,* Ano III, n.º 8, 2020, pp. 45-53 e CUNHA, Ricardo Sousa da – "A vinculação administrativa ao Direito da União Europeia: a propósito da desaplicação da lei n.º 58/2019, de 8/8, pela CNPD com fundamento na violação do RGPD", *Cadernos de Justiça Administrativa,* n.º 142, julho-agosto 2020, pp. 3-10. Assim, devemos ter em consideração a natureza única do RGPD já que, como denota CORDEIRO, A. Barreto Menezes – *Direito da Proteção de Dados à Luz do RGPD e da Lei n.º 58/2019,* Reimpressão, Almedina, 2020, Coimbra, pp. 41-42, não obstante ter aplicação direta (afinal de contas é um Regulamento, nos termos do art. 288.º do TFUE) contém 70 cláusulas de abertura, as quais atribuem competências legislativas aos Estados-Membros e à União, permitindo-se que estes apliquem medidas concretizadoras ou modificativas do regime.

[6] As incongruências podem ser divididas em dois grupos distintos: violações diretas do RGPD (caso em que as disposições da Lei n.º 58/2019 entram em contradição direta com o RGPD) ou indiretas (artigos que vão além da competência legislativa conferida aos Estados-Membros nas cláusulas de abertura). A adotar esta formulação CORDEIRO, A. Barreto Menezes – "Portugal: an overview of the GDPR Implementation", *European Data Protection Law Review,* 5, n.º 4, 2019, pp. 533-536.

[7] N.º 2 do Art. 34.º da Lei n.º 58/2019.

[8] Lei n.º 13/2002, de 19 de fevereiro.

dados[9], a verdade é que várias dúvidas subsistem[10] no nosso ordenamento jurídico devido à "inconstância do legislador nacional"[11]. Neste sentido, importa refletir sobre os mecanismos necessários para mitigar o problema existente, garantindo-se que o contencioso de proteção de dados não fica limitado por uma formalidade de competência[12], sob pena de se desvirtuar todo o sistema.

2. Breves notas sobre o direito de acesso aos tribunais, a tutela jurisdicional efetiva e a dualidade de jurisdições

O princípio da tutela jurisdicional efetiva assume uma "estrutura multifacetada"[13], sendo um dos princípios estruturantes do Estado de

---

[9] De acordo com o disposto nos n.os 2 e 3 do art. 1.º do RGPD, o regulamento tem como objetivo principal a livre circulação dos dados pessoais e a proteção dos direitos fundamentais. Para uma análise da estratégia da UE para os Dados, matéria que não nos incumbe aqui tratar, *vide* MONIZ, Graça Canto – *A Estratégia da UE para os Dados, Coimbra*, Almedina, 2024, pp. 33 e ss.

[10] Não nos iremos debruçar sobre a problemática da aplicabilidade das coimas pela CNPD às entidades públicas. Cumpre-nos apenas mencionar que o legislador europeu, no art. n.º 7 do art. 83.º do RGPD (interpretação que pode ser confirmada através de uma análise do Considerando 150), deixou abertura aos Estados-Membros, em consonância com o seu direito nacional, para estabelecer a possibilidade de coimas às entidades públicas. Portugal previu essa possibilidade, podendo a CNPD proceder à dispensa, verificados determinados requisitos. Remetemos, relativamente a esta questão, para o estudo já efetuado por COELHO, Cristina Pimenta – "A Lei n.º 58/2019, de 8 de agosto, e a aplicabilidade de coimas a entidades públicas", *Revista de Direito Administrativo,* Ano III, n.º 8, 2020, pp. 61-68. Igualmente, ROCHA, Francisco Chilão da – "Sanções a entidades públicas", *in* Domingos Farinho, Francisco Paes Marques e Tiago Fidalgo de Freitas (Coord.) *Direito da Proteção de Dados – Perspetivas Públicas e Privadas,* Almedina, 2023, Coimbra, pp. 491-523(493-494) e SIMÕES, Maria Inês, "O regime sancionatório em matéria de proteção de dados: aplicação (total ou parcial), isenção ou dispensa de aplicação ao setor público", Isabel Celeste M. Fonseca (Coord.) *Estudos de E. Governação, Transparência e Proteção de Dados,* Almedina, 2021, Coimbra, pp. 147-174.

[11] CALVÃO, Filipa Urbano – "Novos âmbitos da justiça administrativa: a proteção de dados", *Cadernos de Justiça Administrativa,* n.º 136, julho-agosto, 2019, pp. 34-42(39).

[12] Para uma análise da competência para dirimir litígios no contexto da Internet, remetemos para SIMÕES, Henrique – "Os tribunais internacionalmente competentes para dirimir litígios relativos à responsabilidade civil do responsável pelo tratamento ou de um subcontratante por violação do direito à proteção de dados pessoais no contexto da internet", *O Direito*, Ano 156, 2024, pp. 369-414.

[13] Expressão usada por BOTELHO, Catarina Santos – "O Tribunal de Estrasburgo, o Tribunal de Justiça da União Europeia e os Tribunais Constitucionais nacionais: perigo de um

Direito democrático, enquanto garantia imprescindível na defesa dos direitos fundamentais[14]. Assim, a todos os cidadãos deve ser conferida a possibilidade de acesso ao direito e aos tribunais para assegurar os seus interesses legalmente protegidos, algo que encontra reflexo no art. 20.º da CRP (acesso ao direito e tutela jurisdicional efetiva).[15]

Pressupõe-se, deste modo, a sua concretização processual[16], tratando-se, na formulação adotada por JORGE MIRANDA[17] de uma norma precetiva não exequível por si mesma. Por um lado, há um comando que fixa determinado objetivo, atribuindo um direito. Por outro, "um segundo comando implícito ou não, que exige do Estado a realização desse objetivo (…), mas que fica dependente de normas que disponham as vias ou os instrumentos adequados."[18] Deste modo, o art. 20.º da CRP inclui "um feixe de direitos, com vários afloramentos no texto constitucional."[19]

"Triângulo das Bermudas"? – A Complexa Interação Multinível entre as Instâncias Jurisdicionais de Protecção dos Direitos Fundamentais", Clotilde Celorico Palma, Eduardo Paz Ferreira e Heleno Taveira Torres (Coord.) *Estudos em Homenagem ao Professor Doutor Alberto Xavier*, Volume III, Almedina, 2012, Coimbra, pp. 119-148(405).

[14] SANTOS, Maria Amália – "O direito constitucionalmente garantido dos cidadãos à tutela jurisdicional efetiva", *Revista Julgar – Online,* 2019, pp. 1-33(3), disponível em https://julgar.pt/wp-content/uploads/2019/11/20191118-ARTIGO-JULGAR-O-Direito-%C3%A0-tutela-jurisdicional-efetiva-%C3%A0-luz-da-Constiuti%C3%A7%C3%A3o-Maria-Am%C3%A1lia-Santos.pdf (consultado em 23.11.2024).

[15] Na esteira de FREITAS, José Lebre de – *Introdução ao Processo Civil – Conceito e princípios gerais à luz do novo código,* 4.ª edição, Gestlegal, 2017, Coimbra, p. 101, "o alcance do preceito é muito mais vasto, não podendo ser desligado, a não ser para fins de análise, da imposição dum processo equitativo, célere e direcionado para uma tutela efetiva."

[16] BOTELHO, Catarina Santos – "O Tribunal de Estrasburgo…" *cit,* pp. 404-405. Igualmente, MEDEIROS, Rui – "Artigo 20.º", Jorge Miranda e Rui Medeiros (Coord.), *Constituição Portuguesa Anotada Volume I,* 2.ª edição revista e atualizada, Universidade Católica Editora, 2017, Lisboa, pp. 308-333(309).

[17] Assim, como defende MIRANDA, Jorge – *Manual de Direito Constitucional Tomo II,* 5.ª Edição, Coimbra, Coimbra Editora, pp. 270 e ss.

[18] MIRANDA, Jorge – *Manual de... cit.,* pp. 274-276. Todas as normas exequíveis por si mesmas serão precetivas, mas nem todas as normas precetivas são exequíveis por si mesmas.

[19] BOTELHO, Catarina Santos, "O Tribunal de Estrasburgo…" *cit,* p. 405. A saber: o acesso ao direito (n.º 1, 1.ª parte), o acesso aos tribunais (n.º 1, *in fine*), o direito de informação e consulta jurídica (n.º 2), não se tratando – como denota MEDEIROS, Rui – "Artigo 20.º" *cit.,* p. 310 de um direito fundamental sem o mínimo de substância, dado que, embora tenha de haver concretização ordinária, este assume a natureza de direito imediatamente invocável; o direito ao patrocínio judiciário (n.º 2, 2.ª parte), enquanto elemento essencial de acesso aos tribunais e

Torna-se, assim, imperioso assegurar a possibilidade de todos os cidadãos acederem aos tribunais para defender os seus direitos, algo que é densificado na legislação ordinária. De um ponto de vista processual, tal levanta a questão da competência dos tribunais para as diferentes ações.

Antes de analisarmos este problema, importa salientar que o art. 209.º da CRP elenca as categorias de tribunais existentes na ordem jurídica portuguesa, a saber: o Tribunal Constitucional[20], o STJ e os tribunais judiciais da primeira e segunda instância[21], o STA e os demais tribunais administrativos e fiscais[22] e, finalmente, o Tribunal de Contas.[23] Tal como é evidenciado por MÁRIO AROSO DE ALMEIDA, o nosso sistema assenta numa verdadeira "dualidade de jurisdições."[24]

Foi com a Reforma Constitucional de 1989 que tal se sucedeu, passando o legislador constituinte a prever expressamente que compete à jurisdição administrativa e fiscal o julgamento das ações e recursos oficiosos que tenham por objeto dirimir os litígios emergentes das relações administrativas e fiscais[25], conferindo -se ao "juiz administrativo o papel de juiz comum ou ordinário da justiça administrativa, cabendo-lhe sem necessidade de atribuição específica, a competência para julgar os litígios emergentes das relações jurídicas administrativas."[26]

---

garantia dos cidadãos; direito de fazer acompanhar-se por advogado perante qualquer autoridade (n.º 2, *in fine*), direito à proteção do segredo de justiça (n.º 3); direito a uma decisão em prazo razoável (n.º 4, 1.ª parte), direito a um processo equitativo (n.º 4, 2.ª parte) e direito à tutela efetiva (n.º 5). Assim, BOTELHO, Catarina Santos – "O Tribunal de Estrasburgo…" *cit,* p. 405, MEDEIROS, Rui, "Artigo 20.º" *cit,* pp. 310-333 e FREITAS, José Lebre de – "*Introdução ao processo…" cit.,* pp. 102-108.

[20] N.º 1 do art. 200.º da CRP.

[21] Alínea a) do n.º 1 do art. 209.º CRP. *Vide,* igualmente, o art. 210.º e o art. 211.º, ambos da CRP.

[22] Alínea b) do n.º 1 do art. 209.º da CRP. *Vide* art. 212.º da CRP.

[23] Alínea c), do n.º 1 do art. 209.º da CRP.

[24] ALMEIDA, Mário Aroso de – *Manual de Processo Administrativo*, 7.ª Edição, Almedina, 2022, Coimbra, p. 175.

[25] N.º 3 do Art. 212.º CRP e, no plano da legislação ordinária, *vide* o n.º 1.º do art. 1.º do ETAF.

[26] CORREIA, Sérvulo – *Direito do Contencioso Administrativo*, Volume I, Lex, 2005, Lisboa, p. 586. O Autor afirma ainda que "a enunciação constitucional de um âmbito material tendencial para a jurisdição dos tribunais administrativos, assente na figura das relações jurídicas administrativas, integra e completa a garantia institucional da ordem jurídica administrativa".

Inversamente, incumbe aos tribunais judiciais a competência para julgar todas as causas que não sejam atribuídas a outra ordem jurisdicional.[27] Deste modo, não é inócuo refletir sobre qual a jurisdição competente nesta matéria, tendo em consideração que estamos perante um pressuposto processual: a competência dos tribunais. Considerando a sensibilidade do assunto em causa, a falta de clarificação contribuirá, ainda mais, para uma excessiva morosidade na resolução dos diferentes processos.

3. A Tutela Jurisdicional conferida pelo RGPD

O RGPD assumiu uma enorme importância no ordenamento jurídico europeu, sendo que o seu impacto extravasa as nossas fronteiras. Numa era em que os dados pessoais são o novo petróleo[28], é essencial assegurar que existem mecanismos de reação contra a violação das disposições do RGPD. Nesta matéria, FRANCISCO CHILÃO ROCHA considera mesmo que, face à Diretiva 95/46/CE, o regulamento passou "do 8 ao 80"[29], demonstrando-se um esforço adicional no sentido de acautelar os meios de resposta e recurso disponíveis na esfera das pessoas singulares e coletivas.

---

[27] N.º 1 do art. 211.º da CRP e, ainda, o art. 64.º do CPC.

[28] Embora alguns autores chamem à atenção para o facto de esta ser uma expressão algo enganadora. É o caso de POLLICINO, Oreste, BASSINI, Marco e GREGORIO, Giovanni de – *Internet Law and protection of fundamental rights,* Bocconi University Press, Milan, 2022, p. 188. Os autores advogam que, ao contrário do petróleo que constitui um recurso limitado, os dados pessoais estão progressivamente a crescer em qualidade e quantidade, apresentando um caráter inesgotável nesta nova era digital. CORDEIRO, A. Barreto Menezes – *Direito da… cit*., p. 29 postula que a expressão "dados pessoais como novo petróleo" exprime "a convicção, bem enraizada, de que os dados irão representar na Era Digital um papel análogo ao desempenhado pelo petróleo e demais combustíveis fósseis a partir da Revolução Industrial". BARBOSA, Mafalda Miranda – *Inteligência Artificial – Entre a Utopia e a Distopia alguns problemas jurídicos*, 2.ª edição, Gestlegal, 2024, p. 180, advoga que os dados pessoais "são hoje vistos como uma *commodity*, como bens que podem ser transacionados com valor económico".

[29] ROCHA, Francisco Chilão – "Sanções a entidades…" *cit.,* p. 502. Igualmente, COELHO, Cristina Pimenta – "Artigo 78.º – Direito à ação judicial contra uma autoridade de controlo", *in* Alexandre Sousa Pinheiro et al. (Coord.) *Comentário ao Regulamento Geral de Proteção de Dados,* Almedina, 2018, Coimbra, pp. 626-628(627).

Assim, o RGPD prevê diferentes mecanismos de tutela, mormente: o direito a apresentar uma reclamação a uma autoridade de controlo (art. 77.º), o direito à ação judicial contra uma autoridade de controlo (art. 78.º) e o direito à ação judicial contra um responsável pelo tratamento ou subcontratante (art. 79.º).[30]

Saliente-se que, entre os mecanismos de tutela, não existe propriamente uma relação de hierarquia, podendo cada uma das vias de recurso "ser exercida sem prejuízo das outras."[31] Ainda assim, o nosso estudo incidirá, sobretudo, sobre o art. 78.º do RGPD. Parece evidente que se dê a possibilidade de recurso contra as decisões adotadas pelas autoridades de controlo, sendo este preceito uma decorrência do direito basilar à ação, plasmado no art. 47.º da CDFUE.[32] Mais, como relembra WALTRAUT KOTSCHY, isto evidencia que as autoridades de controlo não são tribunais e, como tal, deverá haver a possibilidade de tais decisões serem alvo de escrutínio, sempre que pretendido, por uma instância judicial.[33]

No que concerne à titularidade do direito, o n.º 1 do art. 78.º não se limita a subordinar a possibilidade de reação aos titulares dos dados, pois tal seria demasiado restritivo. Assim, todas as pessoas singulares ou coletivas deverão ter a possibilidade de exercer este direito, estando

---

[30] *Vide* o n.º 7 do art. 4.º para a definição de responsável pelo tratamento e o n.º 8 do art. 4.º (ambos do RGPD) para a definição de subcontratante. SIMÕES, Henrique – "Os tribunais internacionalmente competentes…" *cit.,* pp. 373 e ss. procede à relação entre o n.º 2 do art. 79.º do RGPD e o Regulamento Bruxelas I bis, no contexto da competência internacional em matéria civil e comercial.

[31] TJ, *BE c. Nemzeti Adatvédelmi és Információszabadság Hatóság,* C-132/21, 12 de janeiro de 2023, parágrafo 34.

[32] Onde se lê que "toda a pessoa cujos direitos e liberdades garantidos pelo Direito da União tenham sido violados tem direito a uma ação perante um tribunal nos termos previstos no presente artigo. Toda a pessoa tem direito a que a sua causa seja julgada de forma equitativa, publicamente e num prazo razoável, por um tribunal independente e imparcial, previamente estabelecido por lei. Toda a pessoa tem a possibilidade de se fazer aconselhar, defender e representar em juízo. É concedida assistência judiciária a quem não disponha de recursos suficientes, na medida em que essa assistência seja necessária para garantir a efetividade do acesso à justiça."

[33] KOTSCHY, Waltraut – "Article 78. Right to an effective judicial remedy against a supervisory authority", *in* Christopher Kuner, Lee. A. Bygrave e Christopher Dockey (Ed) *The EU General Data Protection Regulation (GDPR),* Oxford University Press, Oxford, pp. 1125-1132(1127).

aqui incluídos "todos os sujeitos, independentemente da forma ou natureza que assumam"[34].

Adicionalmente, o direito à ação judicial pressupõe que esteja em causa uma decisão juridicamente vinculativa da autoridade de controlo. O considerando 143[35] prevê que não estarão abrangidos os pareceres emitidos ou o aconselhamento prestado pela autoridade de controlo. Inversamente, encontram-se abrangidas as decisões respeitantes ao exercício de poderes de investigação, correção, autorização pelas autoridades de controlo, bem como relativamente à recusa ou rejeição de reclamações.[36] Deveremos, ainda, incluir nesta lista as situações em que a autoridade nacional de controlo não trata a reclamação ou não informa o titular dos dados, no prazo de três meses, sobre o andamento ou o resultado da reclamação que tenha apresentado.[37] A este propósito, a AEPD salientou que, embora exista um dever da autoridade de controlo dar alguma informação nesse prazo sobre o estado da reclamação, tal não pressupõe que a reclamação tenha de ser resolvida no prazo de três meses ou que exista qualquer obrigação de informar o queixoso sobre o estado do processo de três em três meses.[38]

Finalmente, o RGPD prevê, no n.º 3 do art. 78.º que os recursos contra as autoridades de controlo terão de ser interpostos nos tribunais do Estado-Membro em cujo território se encontrem estabelecidos, o que deverá ser aferido através da análise de cada legislação nacional. O

---

[34] CORDEIRO, A. Barreto Menezes – "Art. 78.º (Direito à ação judicial contra uma autoridade de controlo)" – A. Barreto Menezes Cordeiro (Coord.) *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019,* Almedina, 2021, Coimbra, pp. 484-486(484). Igualmente, KELLEHER, Denis e MURRAY, Karen – *EU Data Protection Law,* Bloomsbury, 2018, London, p. 375.

[35] Os considerandos têm como função auxiliar na interpretação do RGPD. Todavia, como assinala CORDEIRO, A. Barreto Menezes – *Direito da… cit.,* p. 49, muitas vezes são invocados erradamente com o mero intuito de "alterar, restringir ou ampliar o sentido, sem que a letra o sustente".

[36] Considerando 143 do RGPD.

[37] N.º 3 do Art. 78.º do RGPD. Sobre o tema, *vide* CORDEIRO, A. Barreto Menezes – "Art. 78.º…" *cit.,* p. 485 e COELHO, Cristina Pimenta – "Artigo 78.º…" *cit*, pp. 627-628.

[38] AEPD, Documento Interno 02/2021 relativo aos deveres das Autoridades de Controlo relativamente às alegadas violações do RGPD, Versão 1.0, adotado a 2 de fevereiro de 2021, pp. 12-13.

problema, no contexto português, encontra-se relacionado com a competência dos tribunais para avaliar estas questões.

4. O ordenamento jurídico português

I. Breve enquadramento histórico

Antes de partirmos para a análise do regime atual consagrado na Lei n.º 58/2019, importa evidenciar a evolução legislativa realizada nesta matéria. A verdade é que, anteriormente à execução da Lei no ordenamento jurídico nacional, várias mudanças foram ocorrendo.[39]

Até 2013, a competência pertencia aos tribunais judiciais comuns, não prevendo a Lei n.º 67/98[40] nada relativamente a esta matéria. Tal competência foi transferida para o Tribunal da Concorrência, Regulação e Supervisão, devido à al. g) do n.º 1 do art. 112.º da LOSJ[41], o qual previa a competência para conhecer as matérias relativas ao recurso, revisão e execução de decisões, despachos e medidas das demais entidades administrativas independentes com funções de regulação e supervisão.

Sucede-se, no entanto, que a LOSJ foi sendo alvo de várias alterações e, com a Lei n.º 23/2018[42], procedeu-se à revogação da alínea mencionada. Assim, e continuando a Lei n.º 67/98 a ser omissa nesta questão, os tribunais judiciais voltaram a "recuperar" a competência.[43] Tal vácuo jurídico viria a mudar com a entrada em vigor da Lei de Execução.

---

[39] CALVÃO, Filipa Urbano – "Novos âmbitos…" *cit.,* p. 39.

[40] Lei n.º 67/98, de 26 de outubro (Lei da Proteção de Dados Pessoais), a qual foi revogada com a entrada em vigor da Lei n.º 58/2019, de 8 de agosto.

[41] Lei n.º 62/2013, de 26 de agosto.

[42] Lei n.º 23/2018, de 5 de junho.

[43] CALVÃO, Filipa Urbano "Novos âmbitos…" *cit.,* p. 39.

II. O Regime sancionatório previsto na Lei n.º 58/2019, de 8 de agosto

O RGPD mudou significativamente o panorama de atuação das autoridades de controlo[44], tendo ocorrido uma "harmonização das funções e dos poderes das autoridades de controlo."[45] Um dos poderes mais importantes consiste, precisamente, no poder sancionatório – agora expressamente previsto no RGPD – seguindo-se uma distinção entre as sanções penais e administrativas.[46] Deste modo, a al. j) do n.º 2 do art. 58.º prevê que as autoridades de controlo têm poder para aplicar coimas havendo lugar a uma violação do RGPD. Por sua vez, o art. 83.º densifica o regime contraordenacional, sendo este uma das principais novidades do diploma, visando-se assegurar uma maior efetividade e dissuasão, à semelhança do que se sucede no Direito Europeu da Concorrência, como denota A. BARRETO MENEZES CORDEIRO.[47]

Embora exista um conjunto de critérios a ter em conta no momento da aplicação da contraordenação, as Autoridades de Controlo dispõem de uma certa margem de discricionariedade.[48] Todavia, a

---

[44] Saliente-se que o Considerando 117 abre a porta à criação de mais do que uma autoridade de controlo, tendo sido isso que se sucedeu, a título de exemplo, na Alemanha. MONIZ, Graça Canto – *Manual de… cit.,* p. 153.

[45] CORDEIRO, A. Barreto Menezes – *Direito da… cit.,* p. 397. ALVES, Joel A. – *O Novo Modelo de Proteção de Dados Pessoais Europeu,* Almedina, 2021, Coimbra, p. 129 salienta que existiu um reforço das autoridades de controlo.

[46] MONIZ, Graça Canto – *Manual de… cit.,* p. 156.

[47] CORDEIRO, A. Barreto Menezes – "Artigo 83.º (Condições Gerais para a aplicação de uma coima)", A. Barreto Menezes Cordeiro (Coord.) *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019,* Almedina, 2021, Coimbra, pp. 498-510(500). A consagração de um regime sancionatório, tal como o expressamente previsto no RGPD, permite reforçar os direitos dos titulares dos dados, tal como é assinalado por CALVÃO, Filipa Urbano – "A Lei n.º 58/2019…" *cit.,* p. 51.

[48] Nos termos do n.º 2 do art. 83.º do RGPD, ao decidir sobre a aplicação de uma coima e sobre o respetivo montante, deverá ser tido em consideração o seguinte: *i)* a natureza, a gravidade e a duração da infração tendo em conta a natureza, o âmbito ou o objetivo do tratamento de dados em causa, bem como o número de titulares de dados afetados e o nível de danos por eles sofridos; *(ii)* o caráter intencional ou negligente da infração; *(iii)* a iniciativa tomada pelo responsável pelo tratamento ou pelo subcontratante para atenuar os danos sofridos pelos titulares; *(iv)* o grau de responsabilidade do responsável pelo tratamento ou do subcontratante tendo em conta as medidas técnicas ou organizativas por eles implementadas nos termos dos artigos

"discricionariedade concedida não se confunde com arbitrariedade"[49]. Prevê-se, assim, um sistema de sanções a dois níveis.

Por um lado, o n.º 4 do art. 83.º do RGPD estipula coimas até 10.000.000€ ou, tratando-se de uma empresa[50], até 2% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que seja mais elevado. Por outro lado, o n.º 5 do art. 83.º do RGPD é aplicável às situações mais graves[51], havendo lugar à aplicação de coimas até 20.000.000€ ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado. Assim, as autoridades devem proceder a duas avaliações distintas, nomeadamente: aferir se deve ser aplicada uma coima e, em caso afirmativo, qual o seu montante.[52]

---

25 e 32.º; *(v)* quaisquer infrações pertinentes anteriormente cometidas pelo responsável pelo tratamento ou pelo subcontratante; *(vi)* o grau de cooperação com a autoridade de controlo, a fim de sanar a infração e atenuar os seus eventuais efeitos negativos; *(vii)* as categorias específicas de dados pessoais afetadas pela infração; *(viii)* a forma como a autoridade de controlo tomou conhecimento da infração, em especial se o responsável pelo tratamento ou o subcontratante a notificaram, e em caso afirmativo, em que medida o fizeram; *(ix)* o cumprimento das medidas a que se refere o artigo n.º 2 do art. 58.º caso as mesmas tenham sido previamente impostas ao responsável pelo tratamento ou ao subcontratante em causa relativamente à mesma matéria; *(x)* o cumprimento de códigos de conduta aprovados nos termos do artigo 40.º ou de procedimento de certificação aprovados nos termos do artigo 42.º; *(xi)* qualquer outro fator agravante ou atenuante aplicável às circunstâncias do caso, como os benefícios financeiros obtidos ou as perdas evitadas, direta ou indiretamente, por intermédio da infração. A este propósito, SIMÕES, Maria Inês – "O regime sancionatório…" *cit.,* p. 152 salienta que o RGPD segue uma "abordagem graduada de sanções, no seu art. 83.º, em função das infrações cometidas e verificadas."

[49] CORDEIRO, A Barreto Menezes – "Artigo 83.º…" *cit.,* p. 500. No mesmo sentido, CALVÃO, Filipa Urbano – "A Lei n.º 58/2019…" *cit.,* p. 52 afirma que "pode interpretar-se o RGPD como atribuindo às autoridades nacionais de controlo um poder discricionário ou de decisão autónoma que as mesmas têm de exercer por referência aos fatores indicados no RGPD e dentro dos limites nele definidos."

[50] Adota-se o mesmo conceito de empresa para efeitos do direito da concorrência.

[51] Nomeadamente quando haja violação dos princípios básicos do tratamento, dos direitos dos titulares de dados e das regras relativas à transferência de dados pessoais para um destinatário num país terceiro ou para uma organização internacional.

[52] Opinião do Advogado Geral Nicholas Emiliou, C-683/21, apresentadas a 4 de maio de 2023, parágrafo 57.

Importa, por agora, analisar o modo como o legislador português deu execução a esta matéria na legislação nacional.[53] A Lei n.º 58/2019, de 8 de agosto, faz uma distinção entre contraordenações muito graves (art. 37.º)[54], cujos montantes mínimos e máximos das coimas variam consoante o infrator da norma[55] e as contraordenações graves (art. 38.º)[56],

---

[53] Para uma análise do regime do direito penal da proteção de dados, tal como consagrado no RGPD, *vide* PALMA, Maria Fernanda – "O Direito Penal da Proteção de Dados", *Anatomia do Crime,* Volume 1, n.º 8, 2018, pp. 9-21.

[54] Elencando um conjunto de situações que poderão caber nesta hipótese, nomeadamente: *(i)* os tratamentos de dados pessoais com inobservância dolosa dos princípios consagrados no artigo 5.º do RGPD; *(ii)* os tratamentos de dados pessoais que não tenham por base o consentimento ou outra condição de legitimidade, nos termos do artigo 6.º do RGPD ou de norma nacional; *(iii)* o incumprimento das regras relativas à prestação do consentimento previstas no artigo 7.º do RGPD; *(iv)* os tratamentos de dados pessoais previstos no n.º 1 do artigo 9.º do RGPD sem que se verifique uma das circunstâncias previstas no n.º 2 do mesmo artigo; (*v)* os tratamentos de dados pessoais previstos no artigo 10.º do RGPD que contrariem as regras aí previstas; *(vi)* a exigência do pagamento de uma quantia em dinheiro fora dos casos previstos no n.º 5 do artigo 12.º do RGPD; *(vii)* a exigência do pagamento de uma quantia em dinheiro, nos casos previstos no n.º 5 do artigo 12.º do RGPD, que exceda os custos necessários para satisfazer o direito do titular dos dados; *(viii)* a não prestação de informação relevante nos termos dos artigos 13.º e 14.º do RGPD, o que pode ocorrer quando haja omissão de informação das finalidades a que se destina o tratamento, omissão de informação acerca dos destinatários ou categorias de destinatários dos dados pessoais ou omissão de informação acerca do direito de retirar o consentimento; *(ix)* não permitir, não assegurar ou dificultar o exercício dos direitos previstos nos artigos 15.º a 22.º do RGPD; *(x)* a transferência internacional de dados pessoais em violação do disposto nos artigos 44.º a 49.º do RGPD; *(xi)* o incumprimento das decisões da autoridade de controlo previstas no n.º 2 do art. 58.º do RGPD, ou recusa da colaboração que lhe seja exigida pela CNPD, no exercício dos seus poderes e *(xii)* a violação das regras previstas no capítulo VI da Lei n.º 58/2019.

[55] Tratando-se de grande empresa, a coima poderá ir de 5000€ a 20.000.000€ ou 4 % do volume de negócios anual, a nível mundial, conforme o que for mais elevado. Sendo uma pequena e média Empresa, terá o valor de 2000€ a 20.000.00€ ou 4 % do volume de negócios anual, a nível mundial, conforme o que for mais elevado. Finalmente, tratando-se de uma pessoa singular, o valor da coima poderá ir de 1000€ a 500.000€.

[56] Constituem contraordenações graves, nos termos do art. 38.º: *(i)* a violação do disposto no art. 8.º do RGPD; *(ii)* a não prestação da restante informação prevista nos art. 13.º e 14.º do RGPD; *(iii)* a violação do disposto nos artigos 24.º e 25.º do RGPD; *(iv)* a violação das obrigações previstas no art. 26.º do RGPD; *(v)* a violação do disposto no art. 27.º do RGPD; *(vi)* a violação das obrigações previstas no art. 28.º do RGPD; *(vii)* a violação do disposto no art. 29.º do RGPD; *(viii)* a ausência de registo dos tratamentos de dados pessoais em violação do disposto no art. 30.º do RGPD; *(ix)* a violação das regras de segurança previstas no art. 32.º do RGPD; *(x)* o incumprimento dos deveres previstos no art. 33.º do RGPD; *(xi)* o incumprimento do dever de informar o titular dos dados pessoais nas situações previstas no artigo 34.º do RGPD; *(xii)* o incumprimento da obrigação de realizar avaliações de impacto nos casos previstos no art. 35.º do RGPD; *(xiii)* o incumprimento da obrigação de consultar a autoridade de controlo

reduzindo o seu montante para metade face às contraordenações muito graves.[57]

Porém, o regime sancionatório português padece de alguns defeitos, sendo que nesta matéria partilhamos inteiramente o entendimento sufragado por FILIPA URBANO CALVÃO. De facto, o legislador português optou, pura e simplesmente, por consagrar montantes de coimas totalmente diversos daqueles que se encontram previstos no RGPD, o que não é de todo desejável[58], sobretudo através da consagração de valores mínimos inferiores ao que foi definido pelo regulamento. Ademais, existe uma certa incongruência, pois o legislador português consagra como critérios de determinação da medida da coima a situação económica do agente, o caráter continuado da infração e a dimensão da entidade.[59] Estes critérios são incongruentes, pois não só o RGPD não estabelece como critério a situação económica do infrator, como não faz sentido ter coimas diferentes em função da dimensão da entidade e, *a posteriori,* usar isso como critério para efeitos de determinação da coima.

Além disso, o Direito da União não faz qualquer distinção quanto à dimensão de empresa, pelo que, uma vez mais, o legislador português,

---

previamente à realização de operações de tratamento de dados nos casos previstos no art. 36.º do RGPD; *(xiv)* o incumprimento dos deveres previstos no art. 37.º do RGPD; *(xiv)* a violação do disposto no art. 38.º do RGPD, nomeadamente no que respeita às garantias de independência do encarregado de proteção de dados;

(xv) o incumprimento dos deveres previstos no art. 39.º do RGPD; (xvi) a prática de atos de supervisão de códigos de conduta por organismos não acreditados pela autoridade de controlo nos termos do artigo 41.º do RGPD; *(xvii)* o incumprimento, por parte dos organismos de supervisão de códigos de conduta, do previsto no n.º 4 do art. 41.º do RGPD; *(xviii)* a utilização de selos ou marcas de proteção de dados que não tinham sido emitidos por organismos de certificação devidamente acreditados nos termos dos artigos 42.º e 43.º do RGPD; *(xix)* o incumprimento, por parte dos organismos de certificação, dos deveres previstos no art. 43.º do RGPD e *(xx)* a violação do disposto no art. 19.º Lei n.º 58/2019.

[57] Tratando-se de grande empresa, a coima poderá ir de 2500 € a 10.000.000€ ou 2 % do volume de negócios anual, a nível mundial, conforme o que for mais elevado. Sendo uma pequena e média empresa, terá o valor de 1000€ a 1.000.000€ ou 2% do volume de negócios anual, a nível mundial, conforme o que for mais elevado. Finalmente, tratando-se de uma pessoa singular, o valor da coima poderá ir de 500€ a 250.000€.

[58] CALVÃO, Filipa Urbano – "A Lei n.º 58/2019…" *cit.,* p. 52.

[59] Art. 39.º, n.º 1, da Lei n.º 58/2019.

ao efetuar a distinção entre pequenas, médias e grandes empresas, está a violar expressamente o RGPD. Fica, assim, comprometida a intenção de salvaguardar uma maior uniformização do quadro regulatório.

Ora, parece-nos, na linha do que defende FILIPA URBANO CALVÃO, que "esta panóplia de normas tem por intenção e efeito reduzir o poder discricionário de atuação conferido pelo Direito da União à autoridade nacional de controlo, em termos que contrariam direta e manifestamente o RGPD."[60] Mais se diga que a opção legislativa vai no sentido de sancionar somente as condutas dolosas, excluindo-se os atos/omissões negligentes, algo que claramente não atende ao espírito do RGPD – contrariando-o, aliás, afirmativamente. Por essa razão, compreendemos a posição da CNPD na Deliberação n.º 2019/494, ao defender que o atual quadro legislativo está em violação do RGPD, não devendo ser aplicável.

Afinal, à luz do princípio do primado, todo o Direito da União prevalece sobre direito nacional contrário, inclusive o de caráter constitucional.[61] Além do quadro sancionatório que, *per se,* já levanta enormes dúvidas de conformidade com o RGPD, o legislador português conseguiu – ainda – criar mais uma ambiguidade jurídica quanto à competência do tribunal, conforme de seguida teremos a oportunidade de demonstrar.

III. A Competência do Tribunal para reagir às decisões sancionatórias da CNPD

Contrariamente à Lei n.º 67/98, de 26 de outubro, o art. 34.º da Lei n.º 58/2019 consagra expressamente um preceito dedicado à tutela jurisdicional. Desde logo, prevê-se que qualquer pessoa, de acordo com as regras gerais de legitimidade processual, pode propor ações contra as decisões, nomeadamente de natureza contraordenacional, e omissões

[60] CALVÃO, Filipa Urbano – "A Lei n.º 58/2019…" *ob cit.,* p. 52.
[61] Afirmado pela primeira vez no caso do TJ, *Costa v. Enel,* C-6/64, 15 de julho de 1964.

da CNPD, bem como ações de responsabilidade pelos danos que tais atos ou omissões possam ter causado.[62]

Consagrou-se, igualmente, que as ações propostas contra a CNPD são competência dos tribunais administrativos. Até aqui não haveria nenhum problema. Porém, de forma a salvaguardar-se a coerência e harmonia do sistema jurídico, é recomendável que se evitem contradições evidentes. Através da análise da Lei n.º 58/2019 fica claro que a competência para conhecer estas questões será dos tribunais administrativos. Todavia, devemos atender às disposições previstas no ETAF quanto a esta matéria.

Sempre foi controvertido a questão de saber se os tribunais administrativos poderiam ter competência para apreciar as ações de impugnação das decisões de coimas pela administração pública, sendo que, numa fase inicial, todas elas encontravam-se sujeitas à competência dos tribunais judiciais. Um dos fatores que a doutrina aponta para isto está relacionada com o reduzido número de tribunais e juízes administrativos, considerando-se que não haveria capacidade para dar resposta a todas as situações.[63] A este propósito, ISABEL CELESTE M. FONSECA e JOSÉ AVINTO FERREIRA DANTAS advogam mesmo que por "razões históricas e programáticas afastaram o contencioso contraordenacional do juiz administrativo, em Portugal"[64]. Somos, assim, confrontados com a principal incoerência do sistema, já que a legislação administrativa nesta matéria é contrária ao disposto na Lei de Execução.

Deste modo, a al. l) do art. 4.º do ETAF, prevê expressamente a competência dos tribunais administrativos somente para as "impugnações judiciais de decisões da Administração Pública que apliquem

---

[62] Art. 34.º, n.º 1, da Lei n.º 58/2019.

[63] CARVALHO, Carlos – "Comentários à Revisão do ETAF e do CPTA", *in* Carla Amado Gomes, Ana Fernanda Neves e Tiago Serrão, *Comentários à revisão do ETAF e do CPTA*, AAFLD, 2016, Lisboa, pp. 51-75(64).

[64] FONSECA, Isabel Celeste M. DANTAS, José Aventino Ferreira – "Sanções (contraordenacionais) administrativas no âmbito da jurisdição administrativa", *Revista do CEJ,* n.º 2, 2015, pp. 237-257(246).

coimas no âmbito do ilícito de mera ordenação social por violação de normas de direito administrativo em matéria de urbanismo e do ilícito de mera ordenação social por violação de normas tributárias."[65]

Ora, o atual regime consagra uma solução de "meio termo"[66], já que a atribuição de competência se cinge às duas situações referidas no preceito: ilícito de mera ordenação social por violação de normas de urbanismo e de normas tributárias.[67] Assim, e não se visando sobrecarregar em demasia a jurisdição administrativa e fiscal, a maior parte das situações não se encontram abrangidas pela norma, devendo essas questões ser analisadas pelos tribunais judiciais. A este propósito, a doutrina evidencia que continuam de fora do âmbito da jurisdição administrativa a generalidade dos litígios relativos a processos de contraordenação.[68]

Encontramos, assim, a principal contradição. Ao passo que a Lei n.º 58/2019, de 8 de agosto, atribui competência aos tribunais administrativos, o ETAF não segue o mesmo caminho. Esta é uma questão que tem sido sempre muito controversa na doutrina, razão pela qual não se compreende o porquê de o legislador português, num ato incoerente, ter

---

[65] ANDRADE, José Carlos Vieira de – *A Justiça Administrativa – Lições,* 16.ª edição, Almedina, 2017, Coimbra, p. 120 advoga que, "no mais puro dos literalismos, apenas se considera competente para conhecer da impugnação, mas já não da execução das decisões administrativas aplicadoras de coimas." Ainda assim, no Acórdão n.º 755/2019, Processo n.º 1093/18, Relatora Conselheira Maria José Rangel de Mesquita, o Tribunal Constitucional não julgou a norma inconstitucional por violação do art. 32.º da CRP, interpretada no sentido de que abrange não só impugnações judiciais de decisões da Administração Pública que apliquem coimas no âmbito do ilícito de mera ordenação social por violação de normas de direito administrativo em matéria de urbanismo, como também das decisões que visem a execução dessas mesmas coimas, ainda que não tenham sido impugnadas diante dos tribunais administrativos.

[66] ALMEIDA, Mário Aroso de – *Manual de… cit.,* p. 194.

[67] A solução adotada não é de todo pacífica. FONSECA, Isabel Celeste M. e DANTAS, José Aventino Ferreira – "Sanções (contraordenacionais) administrativas…" *cit.,* pp. 250-251 advogam que a solução do legislador peca por defeito por ter acolhido "uma pequena parte do todo" quer no que diz respeito à distinção entre direito do urbanismo e direito do ordenamento do território, quer quanto ao conceito de coima em matéria urbanística.

[68] NEVES, Ana Fernanda – "Âmbito de jurisdição e outras alterações ao ETAF", *E-Publica,* Volume 1, n.º 2, 2014, pp. 241-271(254). Houve, por isso, uma "opção intencional e de caráter meramente político" do legislador, tal como afirmam FONSECA, Isabel Celeste M. e DANTAS, José Aventino Ferreira – "Sanções (contraordenacionais) administrativas…" *cit.,* p. 256.

consagrado uma solução que aumenta a incerteza jurídica e, sobretudo, não esclarece de modo harmonioso quais são os tribunais aptos para conhecer estas questões. Assim, e considerando que existiu uma intenção do legislador para diminuir ao máximo, nos processos contraordenacionais, a sobrecarga da jurisdição administrativa e fiscal, não se compreende a opção legislativa que levou ao atual art. 34.º. Estranhamos, ainda, o silêncio recente da CNPD, considerando que, em muitas situações, a indecisão quanto à competência dos tribunais poderá levar à prescrição das coimas aplicáveis, pois estes conflitos negativos atrasam (e muito) todos os processos.

O Conselho Superior de Magistratura emitiu um parecer sobre a necessidade de se proceder a uma alteração quanto à determinação da jurisdição competente para conhecer e julgar da impugnação judicial das decisões da CNPD em processos de contraordenação. No referido parecer alerta-se para o facto de a atual incoerência legislativa ser suscetível de conduzir a "resultados práticos graves, podendo a demora que a decisão de conflito de competência implica conduzir à prescrição da contraordenação."[69] Assinala-se, assim, que o atual enquadramento legislativo, pela sua contrariedade evidente, cria um obstáculo intransponível para todas as partes envolvidas. Desde logo, para a CNPD que, enquanto autoridade de controlo, procede à devida aplicação de coimas no âmbito dos seus processos de contraordenação. Ademais, há um impacto evidente para os visados de tais decisões cujo interesse passa por assegurar uma rápida resolução do litígio.

[69] Parecer do Conselho Superior de Magistratura, Procedimento n.º 2023/GAVPM/2315, 6 de julho de 2023.

5. O Debate no Tribunal dos Conflitos

Nos últimos anos, o debate tem incrementado no Tribunal dos Conflitos[70], havendo interpretações contrárias em diferentes casos. Existindo um conflito de jurisdições[71] (como tem sido o caso) entre os tribunais administrativos e judiciais, o Tribunal de Conflitos será constituído por juízes do Supremo Tribunal Administrativo e do Supremo Tribunal de Justiça.[72] Analisaremos, de seguida, as três principais decisões proferidas até ao momento.

I. Acórdão do Tribunal dos Conflitos n.º 039/2173

Esta foi a primeira grande decisão do Tribunal dos Conflitos. Estava em causa a impugnação judicial de uma decisão da CNPD, no ano de 2021, no âmbito de um processo de contraordenação. Houve lugar à impugnação judicial junto do Tribunal Judicial de Braga, Juízo Local de Guimarães, tendo sido proferida uma decisão a julgar aquele juízo materialmente incompetente. Consequentemente, foi ordenada a remessa para o Tribunal Administrativo e Fiscal de Braga, o qual também se julgou incompetente para conhecer do processo.

Chamado a pronunciar-se sobre este conflito negativo, o Tribunal de Conflitos foi perentório ao defender a incompetência do Tribunal

---

[70] A Lei n.º 91/2019, de 4 de setembro, estabelece o regime da resolução dos conflitos de jurisdição entre os tribunais judiciais e os tribunais administrativos e fiscais, regulando a composição, a competência, o funcionamento e o processo perante o tribunal dos conflitos. Para uma análise da lei, *vide* COIMBRA, José Duarte – "A nova Lei do Tribunal dos Conflitos: a peça que faltava (parte I)", *E-Publica,* Volume 6, n.º 3, 2019, pp. 87-120.

[71] Haverá conflito de jurisdições, nos termos do n.º 1 do art. 9.º da Lei 91/2019, de 4 de setembro, sempre que dois ou mais tribunais, integrados em ordens jurisdicionais diferentes, se arrogam ou declinam o poder de conhecer da mesma questão, dizendo-se o conflito positivo no primeiro caso e negativo na segunda situação.

[72] Sobre a matéria *vide* ALMEIDA, Mário Aroso de – *Manual de… cit.,* p. 229. Ainda sobre a composição tal encontra-se previsto no art.2.º da Lei n.º 91/2019.

[73] Acórdão do Tribunal dos Conflitos n.º 039/21, de 23-02-2022, Relatora Isabel Marques da Silva.

Administrativo e Fiscal, tendo baseado a sua posição nos seguintes argumentos:

i. O escopo de aplicação da al. l) do art. 4.º do ETAF é restrito às situações previstas no seu âmbito normativo, *mutatis mutandis,* às impugnações judiciais de decisões da Administração Pública que apliquem coimas no âmbito de ilícito de mera ordenação social por violação de normas de direito urbanismo ou tributárias;[74]

ii. Deu-se relevância à intenção do legislador, citando-se para este efeito o Preâmbulo do DL n.º 214-G/2015, onde se afirma que "entendeu-se, nesta fase, não incluir no âmbito dessa jurisdição administrativa um conjunto de matérias que envolvem a apreciação de questões várias, tais como as inerentes aos processos que têm por objeto a impugnação das decisões da Administração Pública que apliquem coimas no âmbito do ilícito de mera ordenação social noutros domínios. Pretende-se que estas matérias sejam progressivamente integradas no âmbito da referida jurisdição, à medida que a reforma dos tribunais administrativos for sendo executada".[75]

iii. A violação da norma na origem da aplicação da coima não se integra no conceito de matéria respeitante a urbanismo ou normas tributárias.[76]

iv. Logo, considerou ser aplicável o disposto na al. d) do n.º 2 do art. 130.º da LOSJ, segundo o qual os juízos locais cíveis, locais criminais e de competência genérica serão competentes para julgar os recursos das decisões das autoridades administrativas em processos de contraordenação, salvo os atribuídos expressamente a juízos de competência especializada ou a tribunal de competência territorial alargada.[77]

---

[74] Acórdão do Tribunal dos Conflitos n.º 039/21, de 23-02-2022, Relatora Isabel Marques da Silva.

[75] Acórdão do Tribunal dos Conflitos n.º 039/21, de 23-02-2022, Relatora Isabel Marques da Silva.

[76] Acórdão do Tribunal dos Conflitos n.º 039/21, de 23-02-2022, Relatora Isabel Marques da Silva.

[77] Acórdão do Tribunal dos Conflitos n.º 039/21, de 23-02-2022, Relatora Isabel

Não vemos razões para recusar os argumentos que aqui são apresentados. Parece-nos que o Tribunal dos Conflitos seguiu uma linha coerente, analisando a respetiva competência à luz do al. l) do art. 4.º do ETAF, atribuindo, por isso, à jurisdição comum, mais concretamente ao Tribunal Judicial da Comarca de Braga – Juízo Local Criminal de Guimarães – a competência para conhecer esta questão.

II. Acórdão do Tribunal de Conflitos n.º 013/2278

In casu, o CHBM – Centro Hospital Barreiro Montijo, EPE reagiu igualmente contra a aplicação de uma coima única de €380.000,00 aplicada pela CNPD. Ora, remetidos os autos ao Ministério Público junto do Tribunal Judicial da Comarca de Lisboa – Juízo Local Criminal do Barreiro, este declarou-se incompetente em razão da matéria para conhecer esta questão. O processo foi remetido para o Tribunal Administrativo e Fiscal de Almada, o qual também se declarou incompetente para conhecer o recurso. Perante este conflito negativo, o Tribunal de Conflitos inverteu a posição assumida anteriormente, considerando ser competente para a causa a jurisdição administrativa e fiscal, pelos motivos que se expõem:

i. Uma interpretação do n.º 1 do art. 34.º da Lei n.º 58/2019 permite concluir que é competente a Jurisdição Administrativa e Fiscal, apesar de não estarmos perante situações em que a impugnação é instaurada "contra" a autoridade de controlo. Assim, e mencionando-se o art. 9.º do Código Civil, invoca-se que o legislador terá sabido expressar-se nos termos mais adequados, pelo que a sua intenção terá sido a de efetivamente atribuir aos tribunais administrativos a competência para a apreciação dos recursos de impugnação de decisões de aplicação de coimas.

Marques da Silva.

[78] Acórdão do Tribunal dos Conflitos n.º 13/22, 14-07-2022, Relatora Teresa de Sousa.

ii. Mesmo que tal não resulte expressamente do n.º 1 do art. 4.º do ETAF, a competência para os tribunais administrativos e fiscais poderá resultar do disposto em legislação especial.
iii. Por conseguinte, e estando em causa autoridades reguladoras independentes, admitem que a determinação para a competência deverá ser aferida casuisticamente em função do estabelecido no respetivo estatuto orgânico. Será o caso do art. 34.º da Lei n.º 58/2019.

III. Acórdão do Tribunal dos Conflitos n.º 07/2379

Num acórdão mais recente, o Tribunal de Conflitos voltou a pronunciar-se pela sujeição à jurisdição administrativa. *In casu,* houve lugar à impugnação judicial da Deliberação da CNPD que aplicou uma coima no âmbito de processo de contraordenação. Remetido os autos pela CNPD ao Ministério Público junto do Tribunal Administrativo de Lisboa, este determinou a remessa para o Juízo Criminal Local, o qual, por decisão proferida a 24 de outubro de 2022, declarou a sua incompetência em razão de matéria. O Tribunal de Conflitos invocou os seguintes argumentos, na linha do que já havia sido defendido anteriormente:

i. Em primeiro lugar, atendeu à letra da lei, já que, nos termos do art. 34.º da Lei n.º 58/2019, prevê-se a competência da jurisdição administrativa, tendo tal ocorrido mesmo com sugestão da CNPD em sentido contrário.
ii. Por outro lado, advoga-se que, mesmo não havendo previsão expressa no art. 4.º do ETAF que permita aplicar-se a este tipo de situações, ainda assim o regime aí previsto pode ser alvo de múltiplas derrogações, devendo atender-se ao disposto na legislação especial.[80]

[79] Acórdão do Tribunal dos Conflitos n.º 07/23, 05-07-2023, Relatora Teresa de Sousa.
[80] *Ibid*. Seguindo-se a regra "*lex specialis derogat legi generali*" (a lei especial derroga a lei geral).

iii. Mais, o Tribunal de Conflitos invoca que, tratando-se de coima aplicável por uma autoridade reguladora independente (como é o caso da CNPD), a determinação da competência deve ser analisada casuisticamente, em função do respetivo regime jurídico para ela prevista.

Concluiu, assim, o Tribunal de Conflitos que a competência material pertencerá aos tribunais administrativos, dado ter sido essa a opção legislativa consagrada no art. 34.º da Lei n.º 58/2019.[81]

6. Soluções para a incoerência legislativa

Tivemos a oportunidade de confrontar ambas as posições já defendidas pelo Tribunal de Conflitos em casos diferentes. Esta não é uma mera questão de semântica, já que a opção do legislador português gera incerteza jurídica quanto à definição do tribunal competente, algo que não é de todo desejável. Além disso, este problema poderá comprometer (e muito) a eficácia do regime sancionatório previsto na Lei de Execução. Afinal, não havendo decisão quanto ao tribunal competente, as coimas aplicadas correm o risco sério de prescrever.

Desde logo, a indefinição quanto ao tribunal competente faz com que o litígio se arraste nas instâncias judiciais o que, em processos de maior complexidade, poderá ser altamente prejudicial para a efetividade da aplicação do direito. Ademais, o sucessivo arrastar dos processos poderá comprometer a eficácia das coimas aplicadas, considerando os curtos prazos de prescrição aplicáveis. Deste modo, caso não exista uma decisão dentro do prazo de prescrição estabelecido, a aplicação da

[81] Estes argumentos foram replicados no Acórdão do Tribunal de Conflitos n.º 0218/23.8Y4LSB-A.S1, de 05-07-2023, Relatora Maria dos Prazeres Pizarro Beleza. *In casu,* também estava em causa uma impugnação judicial de uma deliberação da CNPD. Os autos foram remetidos ao Ministério Público junto do Tribunal Administrativo de Círculo de Lisboa – Juízo Administrativo Comum, o qual se declarou incompetente para conhecer a questão, tendo sido os autos remetidos para o Tribunal Judicial da Comarca de Lisboa – Juízo Local Criminal de Lisboa, o qual também se declarou materialmente incompetente para conhecer a questão.

coima extingue-se, tornando ineficaz a atuação sancionatória inicial da CNPD.

Sempre que dois ou mais tribunais se declarem incompetentes, será necessário suscitar oficiosamente a resolução do conflito negativo, junto do Supremo Tribunal a quem caiba a presidência do Tribunal dos Conflitos[82]. Decididas as questões que devam ser apreciadas antes do julgamento do objeto do processo, o relator elaborará o projeto de acórdão no prazo de quinze dias[83]. O processo, acompanhado do projeto de acórdão, irá com vista simultânea, por meios eletrónicos, aos restantes tribunais do Tribunal de Conflitos, no prazo de cinco dias[84].

Podemos, por isso, constatar que esta solução incongruente adotada pelo legislador em nada facilita o papel do intérprete e aplicador do direito, dificultando-se a aplicação do direito da proteção de dados no nosso ordenamento jurídico.

Aliás, tal foi visível no caso "*Russiagate*". A Câmara Municipal de Lisboa, após a aplicação da coima superior de 1,2 milhões de euros pela CNPD, decidiu reagir nos tribunais. Embora a questão tenha acabado por ser decidida pelo Tribunal Administrativo de Lisboa, também neste caso o Juízo Local Criminal de Lisboa declarou-se inicialmente incompetente, algo que gerou, durante algum tempo, um receio quanto ao risco de prescrição da coima.[85] A Câmara Municipal de Lisboa perdeu em primeira instância, tendo o tribunal fixado o valor da coima em 1.027.500 euros, menos 222,5 mil face ao montante inicial. Esta decisão foi um passo muito importante na construção do contencioso do direito da proteção de dados, demonstrando que o RGPD é um instrumento legislativo essencial do ordenamento jurídico, devendo o seu cumprimento ser sempre assegurado.[86] A Câmara Municipal de Lisboa recorreu da

---

[82] Artigo 10.º, n.º 1, da Lei n.º 91/2019, de 4 de setembro.

[83] Artigo 13.º, n.º 1, da Lei n.º 91/2019, de 4 de setembro.

[84] Artigo 13.º, n.º 1, da Lei n.º 91/2019, de 4 de setembro.

[85] Nos termos da al. a) do art. 41.º da Lei n.º 58/2019, de 8 de agosto, o prazo de prescrição é de 3 anos, dado tratar-se de uma coima de montante superior a 100.000 euros.

[86] Rádio Renascença, Russiagate. Câmara de Lisboa condenada a pagar um milhão de euros, https://rr.pt/noticia/pais/2024/08/07/russiagate-camara-de-lisboa-condenada-a-pagar-um-milhao-

decisão, tendo o Tribunal Administrativo Central mantido a decisão da primeira instância. Porém, o montante da coima foi reduzido para 738 mil euros, tendo 46 contraordenações sido extintas por prescrição[87].

Como podemos solucionar este problema? Existem vários cenários:

Em primeiro lugar, poderá tudo manter-se como está. Ora, parece-nos que uma atitude omissiva não será o mais desejável. Não se fazendo qualquer alteração, continuaremos a ter conflitos negativos de jurisdição, sendo necessária a intervenção do Tribunal de Conflitos, o que inevitavelmente atrasará os processos e promoverá o risco de haver lugar à prescrição das coimas. Na nossa ótica, este não é de todo o caminho mais favorável pelos motivos expostos.

Assim, a solução mais natural passará pela alteração legislativa, pois só assim será possível criar a necessária certeza jurídica para a propositura destas ações.

Em primeira linha, tal poderia passar por uma modificação à al. l) do n.º 1 do art. 4.º do ETAF, alargando-se, assim, o escopo de competência dos tribunais administrativos e fiscais relativamente às decisões da Administração Pública que apliquem coimas no âmbito da sua atividade. Conforme já tivemos a oportunidade de referir, aquando da reforma do ETAF, na exposição de motivos afirmou-se a pretensão de vir a incluir as matérias que envolvam a apreciação de coimas aplicadas noutros domínios "à medida que a reforma dos tribunais administrativos for sendo executada."[88] A verdade é que a reforma ainda não foi executada, pelo que não havendo uma modificação expressa ao ETAF, parece-nos difícil, como tem feito o Tribunal de Conflitos em casos recentes, defender que a jurisdição pertence aos tribunais administrativos e fiscais, invocando-se uma vontade ainda não expressa do

-de-euros/389217/ (06.08.2025).

[87] ECO, Russiagate. Câmara de Lisboa perde recurso e arrisca pagar 738 mil euros, https://eco.sapo.pt/2025/08/06/russiagate-camara-de-lisboa-perde-recurso-e-arrisca-pagar-738-mil-euros/ (06.08.2025).

[88] Decreto-Lei n.º 214-G/2015, de 2 de outubro (Exposição de Motivos).

legislador. Estamos, assim, perante uma incoerência legal que se deve "a exercícios tecnicamente menos cuidados por parte do legislador"[89], pelo que em nosso entendimento só sendo levada a cabo a referida alteração ao ETAF é que fará sentido concluir pela competência da jurisdição administrativa.[90]

Saliente-se que a jurisprudência do Tribunal de Conflitos mais recente invoca muito a interpretação literal do art. 34.º, n.º 1 da Lei n.º 58/2019[91]. Ora, rigorosamente falando, nestas situações as ações não são propostas contra a CNPD, antes destinando-se a reagir contra a aplicação da sanção. Por conseguinte, e levando o elemento literal ao seu extremo, também aqui não caberia no teor da norma.

Deste modo, consideramos que a melhor solução passará por proceder a uma reformulação da Lei n.º 58/2019, atribuindo-se a competência aos tribunais judiciais. Tal será a forma de proceder à distinção entre as ações de natureza administrativa (propostas contra a CNPD) e as de natureza contraordenacional.[92] Tal possibilidade foi proposta pela CNPD[93] nos trabalhos preparatórios da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, sendo que o art. 34.º deveria a ter a seguinte formulação:

"Artigo 34.º
Tutela jurisdicional
1- [...]

---

[89] COIMBRA, José Duarte – "A nova lei…" *cit,* p. 92

[90] Nesta matéria, CALVÃO, Filipa Urbano – "Novos âmbitos…" *cit*., p. 39 advoga que a maior parte dos litígios que surjam pertencerão aos tribunais administrativos e fiscais, com exceção dos litígios entre o titular dos dados e o responsável pelo tratamento e litígios relativos à validade, eficácia e execução de um contrato no âmbito de uma relação de subcontratação.

[91] A letra da lei constitui, assim, o ponto de partida e limite da interpretação da lei, dado que, nos termos do n.º 2 do art. 9.º do CC "não pode ser considerado pelo intérprete o pensamento legislativo que não tenha na letra da lei um mínimo de correspondência verbal, ainda que imperfeitamente expresso."

[92] Algo já defendido pela CNPD no Parecer n.º 20/2018.

[93] Devemos salientar que à época em que tal foi proposto, a competência pertencia ao Tribunal da Concorrência, Regulação e Supervisão. Com a alteração de 2019, tal como já tivemos a oportunidade de evidenciar, esta passou a pertencer aos Tribunais Judiciais.

2- A competência para conhecer das ações propostas contra a CNPD é dos tribunais administrativos, com exceção das ações de impugnação das deliberações sancionatórias, cuja competência jurisdicional se afere nos termos da Lei n.º 62/2013, de 26 de agosto.[94]

3- [...]

4- [...]".

Na esteira do que defendeu, em 2018, a CNPD, "a mera remissão para aquela lei será suficiente para que se possa saber, a cada momento e perante questões de índole administrativa ou contraordenacional (ou, até, cível, se for o caso), a que tribunal compete a resolução dos litígios que venham a opor a CNPD a qualquer pessoa singular ou coletiva[95]". Consideramos que esta opção poderá mitigar as dúvidas sentidas na doutrina e na jurisprudência. Será possível fazer a distinção necessária entre as ações propostas contra a CNPD e aquelas que se destinam a reagir contra a aplicação de uma contraordenação, voltando os tribunais judiciais a readquirir a competência para estas questões, por força da al. d) do n.º 2 do art. 130.º da LOSJ.

De qualquer modo, e independentemente da opção que venha a ser adotada, a verdade é que algo deve mudar, em nome da coerência e boa aplicação do Direito.

7. Notas Conclusivas

Em suma, este artigo procurou refletir criticamente sobre o atual estado de arte legislativo em matéria de competência jurisdicional para as ações propostas contra a aplicação de coimas pela CNPD. Assim, vimos como a solução consagrada pelo legislador na Lei n.º 58/2019 gera incerteza jurídica por entrar expressamente em confronto com o disposto no regime jurisdicional do ETAF.

---

[94] Formulação reproduzida do Parecer n.º 40/2018 da CNPD.

[95] CNPD, Parecer 20/2018.

Ora, este não foi um mero lapso legislativo, já que a CNPD propôs uma alteração ao art. 34.º, o que não foi seguido nos trabalhos preparatórios. Num mundo digital onde a proteção dos dados assume um papel fulcral na defesa dos titulares dos dados, os responsáveis pelo tratamento e entidades subcontratantes têm obrigações acrescidas, cujo cumprimento será vital para garantir a plena adequação ao RGPD.

Por essa razão, não pode subsistir a indefinição atual quanto ao tribunal competente para estas questões, motivo pelo qual nos parece que uma atitude omissiva do legislador será prejudicial para os particulares, o intérprete e julgador. Deste modo, existem dois cenários que poderão ser seguidos: *(i)* proceder-se a uma alteração do ETAF alargando aí a competência dos tribunais administrativos e fiscais em matéria de contraordenação ou *(ii)* modificar a Lei n.º 58/2019, realizando a respetiva bifurcação entre as ações propostas contra a CNPD e a impugnação das deliberações sancionatórias. Esta última solução parece-nos a mais coerente, voltando neste cenário os tribunais judiciais a readquirir a competência para analisar estas questões.

Independentemente da solução que venha a ser adotada, não pode o legislador continuar a fechar os olhos a esta temática tão sensível, estando mais do que na hora de reformar a Lei n.º 58/2019, corrigindo os erros e incoerências aí presentes.

O interesse legítimo como fundamento de licitude de tratamento de dados pessoais – Constitui este uma "válvula de escape" ao Regulamento Geral sobre a Protecção de Dados Pessoais[1]?

Elodie Beco[2]

Resumo: A aplicação do fundamento de licitude previsto na alínea f) do n.º 1 do art. 6.º do RGPD – o interesse legítimo do responsável pelo tratamento de dados pessoais ou de terceiro como fundamento de licitude – pode, em determinadas situações, ser utilizado de forma extensiva ou até abusiva, sobretudo quando utilizada como fundamento residual para operações que não se enquadram em nenhum dos outros fundamentos previstos no art. 6.º do RGPD.

Deste modo, pretende-se deixar o nosso contributo para uma melhor interpretação e aplicação deste fundamento de licitude, tendo em consideração as exigências de proporcionalidade e transparência que dele decorrem.

Palavras-Chave: Dados pessoais; Regulamento Geral de Protecção de Dados Pessoais; Tratamento de Dados; Interesses Legítimos; e Protecção de Dados.

---

[1] *De ora em diante, RGPD.*

[2] Advogada inscrita na Ordem dos Advogados Portugueses desde 2018. Data Protection Officer. Formadora em matérias de Direito, de onde se inclui o Direito de Proteção de Dados Pessoais. Licenciada em Direito pela Faculdade de Direito da Universidade de Lisboa. Mestre em Direito das Empresas e do Trabalho, com especialização em Direito do Trabalho, pelo ISCTE – Instituto Universitário de Lisboa. Pós-Graduada em Direito de Proteção de Dados Pessoais pela JURISNOVA – Associação da NOVA School of Law. Membro do Observatório para Proteção de Dados Pessoais – CEDIS – NOVA School of Law.

Abstract: The application of the legal basis provided set out in Article 6(1)(f) of the GDPR – the legitimate interest of the data controller in the processing of personal data of a third party as a ground of lawfulness – may, in certain situations, be used extensively or even abusively, especially when used as a residual ground for operations that do not fall within any of the other legal bases set out in Article 6 of the GDPR. Thus, our aim is to provide a contribution twoards a better interpretation and application of this ground of lawfulness, taking into account the requirements of proportionality and transparency arising therefrom.

Keywords: Personal Data; General Data Protection Regulation; Data Processing; Legitimate Interests; and Data Protection

1. Enquadramento geral

O RGPD rege todo o tratamento de dados pessoais com base em princípios basilares consagrados no art. 5.º do referido diploma, que devem ser tidos em consideração pelo responsável pelo tratamento dos dados pessoais em cada fase desse tratamento. São eles: o princípio da licitude, o princípio da lealdade, o princípio da transparência, o princípio da limitação das finalidades, o princípio da minimização dos dados, o princípio da exactidão, o princípio da limitação da conservação, o princípio da integridade e confidencialidade e o princípio da responsabilidade.

Para efeitos do presente estudo, centremos a nossa atenção no princípio da licitude previsto na alínea a) do n.º 1 do art. 5.º do RGPD: "Os dados pessoais são objeto de um tratamento lícito (…)", ainda que todos eles estejam interligados entre si, como veremos.

Este princípio pressupõe um entendimento em sentido amplo e em sentido estrito[3]. Por um lado, pressupõe o cumprimento do RGPD e

[3] MENEZES CORDEIRO, A. Barreto, *Direito da Protecção de Dados à luz do RGPD e da Lei n.º 58/2019*, Edições Almedina, S.A., 2022, p. 152.

demais legislação aplicável. Por outro lado, assenta o tratamento de dados pessoais realizado pelo responsável por esse tratamento num dos fundamentos de licitude elencados taxativamente no art. 6.º do RGPD.

Em bom rigor, não é uma nova exigência legal. A Carta dos Direitos Fundamentais da União Europeia (CDFUE) há muito que estipula, no n.º 2 do seu art. 8.º, que o tratamento de dados pessoais deverá ter por base "o consentimento da pessoa interessada ou outro fundamento legítimo previsto na lei".

Igualmente, a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, na alínea a) do n.º 1 do seu art. 6.º, continha um teor idêntico.

Por sua vez, o disposto do art. 6.º do RGPD contempla como fundamentos de licitude de tratamento de dados pessoais: o consentimento, a execução de um contrato, o cumprimento de uma obrigação jurídica, a defesa de interesses vitais, o exercício de funções de interesse público ou exercício da autoridade pública e o interesse legítimo.

Sem querermos depreciar os restantes fundamentos de licitude, dedicaremos de ora em diante o nosso estudo exclusivamente ao interesse legítimo enquanto fundamento de licitude. A doutrina tem, contudo, assinalado que este fundamento pode, em determinadas situações, ser utilizado de forma extensiva ou até abusiva, sobretudo quando os responsáveis pelo tratamento de dados não conseguem enquadrar a operação em nenhum dos outros fundamentos previstos no art. 6.º do RGPD[4].

---

[4] Para o efeito, leia-se o estudo desenvolvido por KAMARA, Irene; DHERT, Paul de, "Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach", *Brussels Privacy Hub Working Paper*, Vol. 4, n.º 12, Agosto de 2018: "In the contexto of the Directive, the legitimate interests groud has been criticized as being a potential 'loophole', since it is less precisely framed than the others grounds, which are based on clearer conditions". Igualmente, o estudo apresentado por KYI, Lin; SHIVAKUMAR, Sushil Ammanaghatta; ROESNER, Franziska; SANTOS, Cristiana, ZUFALL, Frederike; SCHAUB, Florian; BIEGA, Asia J.; UR, Blase: "Investigating Deceptive Design in GDPR's Legitimate Interest", CHI Conference on Human Factors in Computing Systems (CHI'23), April 23-28, 2023: "In the context of privacy and data protection, we are interested in deceptive designs that deceive users into making poor privacy decisions, such as making it difficult to object to data collection or using obscure or technical language (…) Exactly how often legitimate interests appear in

2. O interesse legítimo como fundamento de licitude de tratamento de dados pessoais

Nos termos da alínea f) do n.º 1 do art. 6.º do RGPD[5], este fundamento de licitude de tratamento de dados pessoais pressupõe que o aludido tratamento preencha, cumulativamente, os seguintes requisitos:

(i) Prossecução de interesses legítimos pelo responsável pelo tratamento ou terceiro;
(ii) Necessidade desse tratamento para efeito dos interesses legítimos;
(iii) Não prevalência de interesses ou direitos e liberdades fundamentais do titular dos dados que exijam protecção, em especial se o titular for uma criança.

De imediato, depreende-se que este fundamento de licitude se distingue dos demais, uma vez que o enfoque está nos interesses, ainda que legítimos, do responsável pelo tratamento ou de terceiros.

Apesar deste preceito revelar-se bastante útil nas situações em que não é possível obter o consentimento do titular dos dados, este preceito legal tem suscitado dificuldades na sua interpretação e, por sua vez, na sua aplicação, face à forte presença de conceitos indeterminados[6]. Este

privacy notices, what deceptive designs arise in this context, and wether the amalgamation of consent and legitimate interests settings into one notice makes decisions making harder for users, remain open questions, which we investigate in this paper".

[5] Sobre a evolução histórica do aludido preceito legal: MENEZES CORDEIRO, A. Barreto, "O tratamento de dados pessoais fundado em interesses legítimos"*, Revista de Direito e Tecnologia,* Vol. 1, N.º 1, 2019, pp. 1-31.

[6] A este respeito, leia-se as várias decisões do Tribunal de Justiça da União Europeia que têm vindo a ser proferidas sobre esta matéria. A título de exemplo, os *doutos* Acórdãos do Tribunal de Justiça, Processo C-468/10 e C-469/10, ASNEF- FECEMD, 24 de novembro de 2011 (ECLI:EU:C:2011:777); Processo C-582/14, Patrick Breyer, 19 de outubro de 2016 (ECLI:EU:C:2016:779); Processo C-13/16, Rīgas Satiksme, 04 de maio de 2017 (ECLI:EU:C:2017:336); Processo C-708/18, Asociaţia de Proprietari bloc M5A-ScaraA, 11 de dezembro de 2019 (ECLI:EU:C:2019:1064); Processo C-597/19, M.I.C.M, datado de 17 de junho

preceito legal, por um lado, exige um esforço adicional ao responsável pelo tratamento na aplicação deste fundamento de licitude de tratamento de dados pessoais, não abrangendo todo e qualquer interesse daquele ou de terceiro, por outro lado, torna imprevisível algumas das situações de tratamento de dados pessoais pela errónea aplicação da alínea f) do n.º 1 do art. 6.º do RGPD[7] com consequências nefastas para os titulares dos dados pessoais.

Este é, assim, um fundamento de licitude de tratamento de dados pessoais marcado pela falta de rigidez do legislador, assumindo, neste caso, as autoridades de controlo e os tribunais um papel fulcral na concretização dos conceitos indeterminados aqui presentes, atendendo que o legislador não atribuiu quaisquer competências à União Europeia ou aos Estados-Membros para o efeito.

Pelo que, revela-se imperativo decifrar, individualmente, cada um dos elementos que compõem a alínea f) do n.º 1 do art. 6.º do RGPD, com vista a, pelo menos, amenizar as dificuldades de aplicação deste fundamento de licitude e, por conseguinte, evitar os efeitos-surpresa na esfera dos titulares dos referidos dados pessoais.

2.1. Prossecução de interesse legítimo pelo responsável pelo tratamento ou terceiro

No disposto na alínea f) do n.º 1 do art. 6.º do RGPD, o legislador exige, desde logo, que o tratamento dos dados pessoais se revele necessário "para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros". O mesmo é dizer que pressupõe, *ab*

---

de 2021 (ECLI:EU:C:2021:492); Processo C-439/19, Latvijas Republikas Saeima, 22 de junho de 2021 (ECLI:EU:C:2021:504); Processo C-252/21, Meta v. Bundeskartellamt, 04 de julho de 2023 (ECLI:EU:C:2023:537); Processo C-26/22 e C-64/22, SCHUFA Holding AG, 07 de dezembro de 2023 (ECLI:EU:C:2023:958).

[7] A este propósito, leia-se, por exemplo, o *douto* Acórdão do Tribunal de Justiça, Processo C-26/22 e C-64/22, SCHUFA Holding AG, 07 de dezembro de 2023 (ECLI:EU:C:2023:958), que conduziu ao apagamento, sem demora injustificada, dos dados pessoais em causa, por não se verificarem os requisitos cumulativos previstos na alínea f) do n.º 1 do art. 6.º do RGPD.

initio, a prossecução de um interesse por parte do responsável pelo tratamento ou de terceiro a quem esses dados sejam comunicados, devendo este interesse ser, consequentemente, legítimo.

Este preceito legal afasta, assim, do seu âmbito de aplicação a prossecução de interesses das autoridades públicas[8], os subcontratantes e as pessoas que, sob a autoridade directa deste, estão autorizadas a tratar os dados pessoais, por força da conjugação da alínea f) do n.º 1 do art. 6.º e n.º 10 do art. 4.º, ambos do RGPD.

A par disto, pressupõe a existência de um interesse concreto, que seja efectivamente prosseguido e não meramente abstracto e hipotético, no momento da tomada de decisão do tratamento de dados pessoais[9].

Aqui chegados, deparamo-nos com os primeiros conceitos indeterminados presentes nesta disposição legal – interesses legítimos –, o qual o legislador não arriscou a delimitar o seu âmbito, no nosso entender, propositadamente.

A concretização destes conceitos indeterminados, requer uma avaliação casuística, uma vez que o interesse aqui corresponde a uma vantagem concreta que o responsável pelo tratamento dos dados pessoais ou terceiro irão beneficiar através do tratamento desses dados pessoais[10], o que se distingue da finalidade mencionada na alínea b) do n.º 1 do art. 5.º do RGPD. Ao contrário do interesse, a finalidade corresponde ao propósito ou intenção que está por detrás do tratamento

---

[8] O que não quer dizer que o interesse legítimo prosseguido pelo responsável pelo tratamento ou por terceiro não possa coincidir com um interesse público, como veremos.

[9] Leia-se o *douto* Acórdão do Tribunal de Justiça, Processo C-708/18, *Asociația de Proprietari bloc M5A-ScaraA*, 11 de dezembro de 2019 (ECLI:EU:C:2019:1064), para. 44: "(…) o responsável pelo tratamento dos dados pessoais ou o terceiro a quem os dados são comunicados deve prosseguir um interesse legítimo que justifique esse tratamento, esse interesse deve ser existente e efectivo no momento do tratamento, e não de natureza hipotética".

Veja-se, também, os exemplos expostos pelo European Data Protection Board, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, 08 October 2024, p. 9.

[10] Neste sentido, MENEZES CORDEIRO, A. Barreto, *Direito da Protecção de Dados…,* p. 226; e CANTO MONIZ, Graça, *Manual de Introdução à Protecção de Dados Pessoais*, Edições Almedina, S.A., 2024, p. 93.

dos dados pessoais[11]. Por outras palavras, e seguindo o raciocínio da Professora Graça Canto Moniz, a finalidade corresponderá, por exemplo, à implementação de procedimentos de controlo de acessos, e o interesse corresponderá, por exemplo, em garantir a segurança de uma organização[12].

O que, inevitavelmente, exigirá uma análise detalhada do caso concreto, ainda que consigamos reconduzir, no imediato, algumas situações ao conceito de "interesse legítimo". Pense-se, por exemplo, na comercialização directa de bens ou serviços. Também a autoridade de controlo nacional tem ilustrado esta necessidade de concretização. A Comissão Nacional de Protecção de Dados, na Deliberação n.º 1039/2017, reconheceu que a gravação de chamadas para efeitos de prova da celebração de contratos pode fundar-se em interesse legítimo do responsável pelo tratamento. Contudo, delimitou esse interesse impondo prazos máximos de conservação diferenciados consoante o sector (telecomunicações, seguros, banca), reforçando o princípio da proporcionalidade e evitando que tal fundamento seja invocado de forma ilimitada[13]. Situação idêntica já se tinha verificado na Deliberação n.º 61/2004, onde a Comissão Nacional de Protecção de Dados, a propósito da videovigilância, reconhecendo a possibilidade de existir um interesse legítimo para protecção de pessoas e bens, mas com algumas restrições, como a proibição de gravação em zonas de descanso e convívio[14]. Este entendimento foi igualmente seguido

---

[11] European Data Protection Board, *Guidelines 1/2024…,* p. 7: "For example, a controller may have an interest in promoting its products, whereas this interest may be advanced by processing personal data for direct marketing purposes".

[12] CANTO MONIZ, Graça, Manual de Introdução à Protecção…, Edições Almedina, S.A., 2024, p. 92-93.

[13] Comissão Nacional de Protecção de Dados, Deliberação n.º 1039/2017, de 27 de Julho de 2017, *relativa à conservação de gravações de chamadas telefónicas para prova da celebração de contratos à distância*.

[14] Comissão Nacional de Protecção de Dados, Deliberação n.º 61/2004, de 21 de Janeiro de 2004, relativa ao tratamento de dados pessoais por sistemas de videovigilância. Também a jurisprudência nacional tem acompanhado este entendimento. O *douto* Acórdão do Tribunal da Relação de Lisboa, de 16 de Novembro de 2011, proc. 17/10.7TTBRR.L1-4, disponível para consulta em www.dgsi.pt, considerou lícito o uso de imagens captadas por videovigilância autorizada pela Comissão Nacional de Protecção de Dados, desde que destinadas à protecção de bens e não ao controlo do desempenho profissional do trabalhador.

pela jurisprudência nacional, que tem vindo a reforçar os limites à invocação do interesse legítimo como fundamento de licitude[15].

Com efeito, o interesse pode assumir qualquer natureza, com mais ou menos impacto positivo na sociedade, desde que o mesmo não seja ilegítimo e, como se verá adiante, não colida com outros interesses ou direitos e liberdades fundamentais do titular dos dados pessoais preponderantes.

Destarte, espera-se que, a todo o momento, o interesse seja lícito, isto é, admissível de acordo com a legislação em matéria de protecção de dados pessoais e a demais legislação aplicável.

É nesta óptica, que, no nosso entender, o legislador fê-lo, nos Considerandos 47 a 50 do RGPD, ao enumerar algumas situações concretas passíveis de serem subsumidas no âmbito da disposição legal em análise, como a existência de uma relação relevante e apropriada entre o titular dos dados pessoais e o responsável pelo tratamento desses dados; a prevenção e controlo da fraude; a comercialização directa[16]; a existência de uma relação de grupo empresarial ou de uma instituição associada a um organismo central; segurança da rede e das informações e dos serviços conexos; transmissão de dados a autoridades competentes.

---

[15] O *douto* Acórdão do Tribunal Constitucional n.º 268/2022, proc. n.º 828/19, declarou a insconstitucionalidade da conservação generalizada e indiferenciada de metadados de comunicações, entendendo que o interesse público ou estatal genérico não basta para justificar ingerências tão extensas na privacidade. Também o *douto* Acórdão do Supremo Tribunal de Justiça, proc. 2335/06.0TMPRT-D.P1.S1, 23 de Fevereiro de 2021, reafirmou que o acesso de terceiros a processos judicias exige sempre a demonstração de um interesse legítimo concreto, sujeito a autorização judicial.

[16] Denote-se, porém, que em algumas situações não é possível fundamentar o tratamento de dados pessoais a propósito de marketing directo mediante aplicação da alínea f) do n.º 1 do art. 6.º do RGPD, mas sim através, por exemplo, do consentimento previsto na alínea a) do n.º 1 do mesmo artigo. Sobre isto: European Data Protection Board, *Guidelines 1/2024…,* pp. 29-33.

O Grupo de Trabalho do art. 29.º[17] também já se tinha debruçado sobre esta matéria, tendo sugerido um conjunto de interesses que poderiam caber no âmbito do preceito legal em estudo, tais como o exercício do direito à liberdade de expressão ou de informação, nomeadamente nos meios de comunicação social e nas artes; mensagens não comerciais não solicitadas, nomeadamente relativas a campanhas políticas ou a actividades de angariação de fundos para fins de beneficência; execução de créditos, incluindo cobrança de dívidas através de processos não judiciais; prevenção da fraude, utilização abusiva de serviços ou branqueamento de capitais[18]; monitorização da actividade dos trabalhadores para fins de segurança ou de gestão; sistemas de denúncia; segurança física, tecnologias de informação e segurança das redes; tratamento para fins históricos, científicos, estatísticos e de investigação (nomeadamente pesquisas de mercado). No que respeita a interesses de terceiros, o Grupo de Trabalho do artigo 29.º, igualmente, enunciou alguns exemplos susceptíveis de aplicação da alínea f) do n.º 1 do art. 6.º do RGPD[19], como a publicação de dados para fins de transparência e de responsabilidade (por exemplo, os salários dos quadros superiores de uma sociedade); a investigação histórica ou outros tipos de investigação científica, em especial quando seja necessário o acesso a determinadas

---

[17] O Grupo de Trabalho do art. 29.º para a protecção de dados pessoais foi instituído ao abrigo do art. 29.º da Directiva 95/46/CE e correspondia a um órgão consultivo europeu independente em matéria de protecção de dados e privacidade, motivo pelo qual os seus textos assumiam unicamente a forma de pareceres e recomendações, sem qualquer vinculação jurídica, conforme previa o disposto no art. 30.º da referida Directiva. Posteriormente, com o início da aplicação do RGPD, em 25 de Maio de 2018, este órgão foi substituído pelo actual European Data Protection Board. Veja-se, Grupo de Trabalho do art. 29.º para a Protecção de Dados, *Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na acepção do art. 7.º da Diretiva 95/46/CE*, 09 de abril de 2014, p. 39.

[18] A este respeito, o *douto* Acórdão do Tribunal de Justiça, Processo C-252/21, *Meta v. Bundeskartellamt*, 04 de julho de 2023 (ECLI:EU:C:2023:537), para 124, assume uma posição particular: "Com efeito, um operador privado como a Meta Platforms Ireland não pode invocar esse interesse legítimo, alheio à sua actividade económica e comercial. Em contrapartida, o referido objectivo pode justificar o tratamento efectuado por esse operador quando for objectivamente necessário para o cumprimento de uma obrigação jurídica à qual esse operador está submetido".

[19] Grupo de Trabalho do artigo 29.º para a Protecção de Dados, *Parecer 06/2014 sobre o conceito de interesses legítimos…*, p. 39.

bases de dados; e prossecução de um interesse público geral ou de terceiros[20], mormente, combate a actividades ilícitas (por exemplo, branqueamento de capitais, o tráfico de crianças, ou a partilha ilícita de ficheiros em linha). Acrescente-se também a esta lista não exaustiva, o exercício de um direito de terceiro ou a sua defesa (por exemplo, quando se verifica a necessidade de identificar determinada pessoa, no seguimento de ter causado danos, com vista a intentar a competente acção judicial)[21].

Não obstante, subsiste a presença de um conceito indeterminado, o que dificulta, em muito, a correcta subsunção de uma situação concreta ao disposto na alínea f) do n.º 1 do art. 6.º do RGPD, mesmo nos casos em que houve uma avaliação cuidada como sugerida pelo legislador no Considerando 47 do mesmo diploma.

2.2. Necessidade de tratamento de dados pessoais para efeito do interesse legítimo

Para além da observância de um interesse legítimo prosseguido pelo responsável pelo tratamento dos dados pessoais ou por terceiro, o legislador exige, para aplicação do disposto na alínea f) do n.º 1 do art. 6.º do RGPD, que o aludido tratamento de dados pessoais se revele como necessário na prossecução do interesse legítimo e, por sua vez, a demonstração dessa necessidade, por alusão ao disposto no n.º 2 do art. 5.º do RGPD.

---

[20] Veja-se o *douto* Acórdão do Tribunal de Justiça, Processo C-708/18, Asociaţia de Proprietari bloc M5A-ScaraA, 11 de dezembro de 2019 (ECLI:EU:C:2019:1064), em que se considerou a instalação de um sistema de videovigilância, nas partes comuns de um imóvel para habitação, como proporcional e adequado para prosseguir interesses legítimos de garantia da segurança e da protecção das pessoas e dos bens, sem o consentimento das pessoas em causa, se o tratamento dos dados pessoais recolhidos através desse sistema de videovigilância cumprir os requisitos previstos na alínea f) do n.º 1 do art. 6.º do RGPD.

[21] A propósito, *douto* Acórdão do Tribunal de Justiça, Processo C-13/16, *Rīgas Satiksme*, 04 de maio de 2017 (ECLI:EU:C:2017:336), para. 29: "(…) não há dúvida de que o interesse de um terceiro em obter uma informação de ordem pessoal sobre uma pessoa que danificou os seus bens para instaurar uma acção contra essa pessoa constitui um interesse legítimo (…)"

O conceito de necessidade aqui abordado deverá ser interpretado à luz do RGPD e dos seus princípios basilares, com especial destaque para o princípio da minimização dos dados, previsto na alínea c) do n.º 1 do art. 5.º do RGPD[22].

Os dados pessoais que são objecto de tratamento deverão limitar-se ao adequado, pertinente e estritamente necessário, *in casu*, para efeito de prossecução do interesse legítimo identificado, sendo certo que a existir uma alternativa menos intrusiva na esfera do titular dos dados pessoais deverá antes ser adoptada esta última. Neste caso, os requisitos legais da alínea f) do n.º 1 do art. 6.º do RGPD não estarão totalmente preenchidos, porquanto faltará, desde logo, o critério de necessidade do aludido tratamento de dados pessoais para efeito de prossecução do interesse legítimo em causa[23].

Assim, a avaliação da necessidade do tratamento dos dados pessoais requer uma análise cuidada da situação em concreto e, sobretudo, comparativa de todas as alternativas disponíveis, a fim de apurar a menos intrusiva para a esfera do titular dos dados pessoais e passível de cumprir o mesmo propósito.

2.3. Não prevalência de interesses ou direitos e liberdades fundamentais do titular dos dados

Por último, e não menos importante, a aplicação do disposto na alínea f) do n.º 1 do art. 6.º do RGPD pressupõe a não prevalência de interesses ou direitos e liberdades fundamentais do titular dos dados pessoais na tomada de decisão de tratamento desses dados pessoais pelo

---

[22] A este respeito, MENEZES CORDEIRO, A. Barreto, in *Direito da Protecção de Dados…,* p. 225, defende que "o conceito de necessidade não só não é passível de ser reconduzido ao princípio da proporcionalidade, como assume um conteúdo distinto dos preenchimentos preconizados para as demais alíneas do artigo 6.º/1. (…) A assunção desta posição não impossibilita, pelo contrário, que na decomposição desenvolvida o intérprete-aplicador recorra aos desenvolvimentos prosseguidos no âmbito do princípio da proporcionalidade (…)".

[23] A este propósito, o *douto* Acórdão do Tribunal de Justiça, Processo C-252/21, Meta v. Bundeskartellamt, 04 de julho de 2023 (ECLI:EU:C:2023:537), para. 108 e 109.

responsável pelo tratamento, em relação ao interesse legítimo que este último visa prosseguir.

Este requisito legal assume um papel fulcral no momento de ponderação pelo tratamento ou não dos dados pessoais pelo responsável pelo tratamento, na medida em que o legislador não visa uma protecção dos interesses, direitos e liberdades do titular dos dados pessoais idêntica à que confere aos interesses legítimos do responsável pelo tratamento ou terceiro. Pelo contrário, os interesses, direitos e liberdades fundamentais do titular dos dados assumem-se como determinantes na caracterização de um tratamento de dados pessoais como lícito ou não.

Sucede que, facilmente, se compreenderá a posição adoptada pelo legislador se tivermos por presente o direito à auto-determinação informacional do titular dos dados pessoais e o tendente desequilíbrio entre o responsável pelo tratamento e o titular dos dados pessoais[24].

Deste modo, os conceitos "interesses, direitos e liberdades fundamentais" aqui expostos deverão ser tidos em consideração no seu sentido amplo[25], à semelhança do conceito "interesses legítimos" já abordado, com vista a assegurar uma protecção íntegra do titular dos dados pessoais.

Tanto assim é que o legislador incluiu os direitos e liberdades, mas também os interesses do titular dos dados pessoais, o que torna esta protecção mais abrangente.

---

[24] A este propósito, enfatiza o Grupo de Trabalho do artigo 29.º para a Protecção de Dados, in *Parecer 06/2014 sobre o conceito de interesses legítimos…*, p. 47, o seguinte: "Numa época em que existe um crescente desequilíbrio na capacidade de informação, em que quer governos quer organizações empresariais vêm acumulando volumes sem precedentes de dados sobre as pessoas e têm cada vez mais condições para elaborar perfis pormenorizados que permitirão prever os seus comportamentos (reforçando o desequilíbrio de informação e reduzindo a sua autonomia), é mais importante do que nunca assegurar que o interesse das pessoas em preservar a sua privacidade e a sua autonomia seja protegido".

[25] Face à amplitude dos conceitos em estudo, MENEZES CORDEIRO, A. Barreto, in *Direito da Protecção de Dados…*, p. 229, inclui neste elenco os direitos de base patrimonial ou económica, reputação do titular dos dados pessoais e os eventuais efeitos discriminatórios associados. Igualmente, European Data Protection Board, *Guidelines 1/2024…,* pp. 13: "(…) include any interest that may be affected by the processing at stake, including, but not limited to, financial interests, social interests or personal interests".

Todavia, o legislador vai mais longe – os interesses, direitos, liberdades em causa não têm que ser necessariamente legítimos. Caso tivesse sido essa a intenção do legislador, este tê-lo-ia previsto, tal como o fez na primeira parte da disposição legal em estudo para o responsável pelo tratamento e terceiro. Por aqui, conseguimos compreender a amplitude que esta protecção poderá assumir na esfera do titular dos dados pessoais[26].

Destarte, caberão aqui todas as situações que, de alguma forma, asseguram a posição do titular dos dados pessoais, sejam elas legítimas ou não.

3. Teste de ponderação

Conhecidos os requisitos que determinam uma correcta aplicação do fundamento de licitude acolhido na alínea f) do n.º 1 do art. 6.º do RGPD, fica uma questão por responder: Como poderá o responsável pelo tratamento dos dados pessoais garantir que a sua análise casuística foi realizada conforme a avaliação cuidada sugerida pelo legislador no Considerando 47 do aludido diploma?

A resposta acertada a esta pergunta por cada um dos responsáveis pelo tratamento de dados pessoais resolveria o problema central desta disposição legal[27] – os abusos constantes praticados por aqueles na subsunção de todas as situações concretas a este preceito legal sempre que não se aplique um dos restantes fundamentos de licitude, previstos no n.º 1 do art. 6.º do RGPD, uns por ignorância, outros com plena

[26] A este propósito, afirma o Grupo de Trabalho do artigo 29.º para a Protecção de Dados, in *Parecer 06/2014 sobre o conceito de interesses legítimos…*, p. 47, o seguinte: "Mesmo as pessoas que estejam envolvidas em actividades ilegais não devem estar sujeitas a uma ingerência desproporcionada nos seus direitos e interesses. Por exemplo, os interesses de uma pessoa suspeita de ter praticado um furto num supermercado podem, ainda assim, prevalecer sobre a publicação da sua fotografia e da sua morada particular nas paredes do supermercado e/ou na Internet pelo proprietário da loja".

[27] Neste sentido, European Data Protection Board, *Guidelines 1/2024…,* pp. 5-6.

consciência do seu acto. Este preceito legal também não assume um carácter mais geral em comparação com as restantes alíneas aí previstas, em que todas as situações concretas possam, de alguma forma, ser reconduzidas à aplicação do fundamento de licitude em estudo.

Sucede, porém, que o legislador não faz qualquer distinção deste fundamento de licitude em relação aos restantes fundamentos de licitude consagrados no aludido art. 6.º do RGPD. Pelo contrário, coloca-os em pé de igualdade. Aliás, o legislador assume a possibilidade de um determinado tratamento de dados pessoais estar justificado por mais do que um fundamento de licitude previsto no n.º 1 do art. 6.º do RGPD: "O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:". Importa, contudo, sublinhar que desta formulação não decorre que os responsáveis pelo tratamento possam escolher livremente o fundamento de licitude a posteriori, como se se tratasse de um mecanismo de substituição (cherry picking)[28].

Ainda assim, a nosso ver, é suficiente a subsunção da situação concreta apenas a uma das alíneas do aludido preceito legal para admitir-se que o tratamento de dados pessoais em causa está justificado[29].

Deste modo, a alínea f) do n.º 1 do art. 6.º do RGPD não tem uma aplicação residual, ainda que se sugira uma análise prévia de subsunção

---

[28] European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679*, Version 1.1, 04 May 2020, p. 25: "the controller cannot swap from consent to other lawful bases. For example, it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent. Because of the requirement to disclose the lawful basis, which the controller is relying upon at the time of collection of personal data, controllers must have decided in advance of collection what the applicable lawful basis is".

[29] A este respeito, Conclusões do Advogado-Geral Maciej Szpunar, Processo C-394/23, Association Mousse, 11 de julho de 2024 (ECLI:EU:C:2024:610), para. 30: "(…) o Tribunal de Justiça especificou o caráter não cumulativo das justificações previstas no artigo 6.º, n.º 1, do RGPD. Indicou assim que «quando seja possível constatar que um tratamento de dados pessoais é necessário à luz de uma das justificações previstas no artigo 6.º, n.º 1, […] alíneas b) a f), do RGPD, não há que determinar se esse tratamento está igualmente abrangido por outra dessas justificações». Por outras palavras, como eu já havia mencionado, o tratamento de dados pessoais é lícito quando é justificado por um único motivo, sem que um motivo seja considerado subsidiário de outro".

a um dos outros fundamentos de licitude aí previstos[30]. Conforme vimos, este fundamento de licitude é fortemente marcado pela presença de conceitos indeterminados, o que só por si dificulta a sua interpretação. Pelo que, é fulcral a adopção de uma abordagem pragmática, isto é, se for possível, por exemplo, numa situação concreta reconduzir o tratamento de dados pessoais à necessidade do mesmo para a execução de um contrato no qual o titular de dados pessoais é parte [alínea b) do n.º 1 do art. 6.º do RGPD], a nosso ver, deverá ser considerado antes este fundamento de licitude, porquanto o responsável pelo tratamento de dados pessoais terá, em princípio, mais facilidade em justificar o aludido tratamento dos dados pessoais. O mesmo se dirá relativamente a uma situação em que o titular dos dados pessoais consentiu com o tratamento desses dados pessoais [alínea a) do n.º 1 do art. 6.º do RGPD].

Posto isto, a nosso ver, o Grupo de Trabalho do artigo 29.º[31] dá-nos uma possível resposta bastante completa à questão levantada –, mediante um teste de ponderação, baseado em quatro factores[32]:

(i) Avaliação do interesse legítimo do responsável pelo tratamento ou de terceiro – natureza e origem;
(ii) Impacto que esse tratamento assume na esfera do titular dos dados pessoais;
(iii) Equilíbrio provisório entre o interesse legítimo do responsável pelo tratamento e o impacto do tratamento dos dados pessoais na pessoa em causa;
(iv) Caso o resultado da avaliação ainda suscite dúvidas, aplicação de garantias complementares pelo responsável pelo tratamento para evitar qualquer impacto indevido nas pessoas em causa.

---

[30] Assumindo uma posição similar, European Data Protection Board, *Guidelines 1/2024…*, p. 6: "(…) processing relying on Article 6(1)(f) GDPR should not encompass several purposes without assessing the validity of the legal basis for each of them".

[31] Sobre este assunto, Grupo de Trabalho do artigo 29.º para a Protecção de Dados, *Parecer 06/2014 sobre o conceito de interesses legítimos…,* p. 52 e ss. Na mesma linha de raciocínio, CANTO MONIZ, Graça, *Manual de Introdução à Protecção…,* Edições Almedina, S.A., 2024, pp. 95 e ss.

[32] Em sentido diverso, MENEZES CORDEIRO, A. Barreto, *Direito da Protecção de Dados…*, pp. 231 e ss., defendendo uma divisão tripartida: dados pessoais, partes e tratamento.

3.1. Avaliação do interesse legítimo do responsável pelo tratamento ou de terceiro

Perante um interesse legítimo, o responsável pelo tratamento dos dados pessoais deverá ponderar o impacto que o tratamento de dados pessoais irá repercutir no titular desses dados pessoais e acautelar que a prossecução do interesse ou o exercício do direito ou liberdade deste último não prevalece em relação àquele.

Como já vimos *supra*, o conceito de "interesse legítimo" pode, por vezes, revelar-se de difícil concretização face à amplitude do seu conteúdo.

Contudo, existe um conjunto de situações que conduz, em princípio, à prevalência do interesse legítimo do responsável pelo tratamento de dados pessoais, legitimando, assim, o tratamento desses dados pessoais.

É o que sucede quando estamos perante o exercício de um direito fundamental daquele[33]ou a presença de um interesse público ou um interesse da comunidade em geral[34], que pode coincidir ou não com um interesse privado do responsável pelo tratamento dos dados pessoais[35]. A sociedade em geral espera que numa situação concreta em que um interesse legítimo coincida com um interesse público ou da comunidade em geral, este interesse seja mais preponderante. O contrário já não acontece.

---

[33] Grupo de Trabalho do artigo 29.º para a Protecção de Dados, *Parecer 06/2014…,* pp. 53-54, dá o seguinte exemplo: "pode muito bem ser necessário e proporcionado um jornal publicar determinados pormenores comprometedores sobre os hábitos de consumo de um alto funcionário governamental envolvido num alegado escândalo de corrupção".

[34] Grupo de Trabalho do artigo 29.º para a Protecção de Dados, *Parecer 06/2014…,* p. 54, dá o exemplo de "uma organização sem fins lucrativos pode fazê-lo com o objectivo de alertar para a corrupção governamental".

[35] A título de exemplo, Grupo de Trabalho do artigo 29.º para a Protecção de Dados*, Parecer 06/2014…,* p. 55: "Um prestador de serviços pode ter um interesse comercial legítimo em assegurar que os seus clientes não utilizem o serviço de forma abusiva (ou não consigam obter serviços sem pagar) e, ao mesmo tempo, os clientes da empresa, os contribuintes e o público em geral têm igualmente um interesse legítimo em assegurar que as actividades fraudulentas, quando ocorram, sejam desencorajadas e detetadas".

Na mesma linha de raciocínio, incluir-se-á as situações em que o interesse legítimo do responsável pelo tratamento tem reconhecimento jurídico, cultural ou social[36]. Também aqui o referido interesse será mais preponderante.

A par disto, o interesse legítimo pode manifestar-se no contexto de outros fundamentos jurídicos aplicáveis, nomeadamente, os previstos nas alíneas b) e c) do n.º 1 do art. 6.º do RGPD, na medida em que o tratamento de dados pessoais pode não ser estritamente necessário, mas ser, ainda assim, relevante para a execução de um contrato ou uma lei que o permita, sem, todavia, o impor[37]. Importa, contudo, ressalvar que tal possibilidade não significa que o responsável pelo tratamento possa recorrer ao interesse letígitimo de forma residual ou como fundamento de recuso quando outro, como o consentimento, não se mostra adequado ou válido.

Sucede, porém, que não é suficiente a avaliação concreta do interesse legítimo do responsável pelo tratamento ou de terceiro. Requer-se também uma apreciação do impacto que o tratamento desses dados pessoais repercutirá nos interesses, direitos ou liberdades fundamentais do titular dos dados pessoais.

3.2. Impacto do tratamento de dados pessoais na esfera do titular desses dados pessoais

Para efeito do teste de ponderação, o impacto deverá ser entendido no sentido amplo, abrangendo as consequências, tanto potenciais[38]

---

[36] A título de exemplo, Grupo de Trabalho do artigo 29.º para a Protecção de Dados, *Parecer 06/2014…,* p. 56: "quaisquer orientações validamente adotadas e não vinculativas, emitidas pelos organismos competentes, por exemplo, por entidades reguladoras, que incentivem os responsáveis pelo tratamento a tratar os dados na prossecução do interesse em causa".

[37] Neste sentido, Grupo de Trabalho do artigo 29.º para a Protecção de Dados, *Parecer 06/2014…,* p. 55.

[38] A este respeito, Grupo de Trabalho do artigo 29.º para a Protecção de Dados, *Parecer 06/2014 sobre o conceito de interesses legítimos…,* p. 59 identifica dois elementos-chave: "a probabilidade de o risco se realizar, por um lado, e a gravidade das consequências, por outro lado – contribuem para a avaliação global do potencial impacto".

como reais, do tratamento de dados, sejam elas positivas ou negativas, tendo por base que a sua probabilidade e gravidade variará caso a caso[39].

Sucede que elementos como a natureza dos dados pessoais, a forma como estes são tratados, as expectativas razoáveis do titular dos dados pessoais e a relação entre este e o responsável pelo tratamento dos dados pessoais podem, efectivamente, revelar-se determinantes na apreciação do impacto do aludido tratamento. Vejamos.

A natureza dos dados pessoais está intrinsecamente relacionada com a presença ou não de categorias especiais de dados pessoais, contempladas no art. 9.º do RGPD, porquanto, o seu tratamento trará, em princípio, maiores consequências na esfera do titular desses dados pessoais, ainda assim tal não descura a necessidade de uma análise casuística. Igualmente, existem outros factores que poderão assumir-se como relevantes na ponderação, mormente, a origem dos dados, isto é, se os dados pessoais em causa foram recolhidos directamente junto do titular dos mesmos ou, porventura, se já foram tornados públicos pelo titular desses dados pessoais ou por terceiros e se foi gerada uma expectativa razoável daqueles dados serem reutilizados para finalidades específicas[40].

Relativamente à forma como os dados pessoais são tratados[41], e dissecada a natureza dos mesmos, é necessário avaliar o modo de tratamento, a dimensão do número de pessoas com acesso a esses dados

---

[39] Para o efeito, leia-se o Considerando 75 do RGPD.

[40] Grupo de Trabalho do artigo 29.º para a Protecção de Dados, *Parecer 06/2014 sobre o conceito de interesses legítimos…,* p. 61: "(…) por exemplo, para fins de investigação ou para fins relacionados com a transparência e a responsabilidade".

[41] Veja-se o *douto* Acórdão do Tribunal de Justiça, Processo C-708/18, Asociaţia de Proprietari bloc M5A-ScaraA, 11 de dezembro de 2019 (ECLI:EU:C:2019:1064), para. 57: "(…) deve nomeadamente ser tida em conta a natureza dos dados pessoais em questão, em especial a natureza potencialmente sensível desses dados, bem como a natureza e as modalidades concretas do tratamento dos dados em questão, sobretudo o número de pessoas que têm acesso a esses dados e as modalidades de acesso aos mesmos"; e *douto* Acórdão do Tribunal de Justiça, Processo C-252/21, Meta v. Bundeskartellamt, 04 de julho de 2023 (ECLI:EU:C:2023:537), para. 118: "(…) incide sobre dados potencialmente ilimitados e tem um impacto importante no utilizador, cujas atividades em linha são, em grande parte ou mesmo quase na sua totalidade, monitorizadas pela Meta Platforms Ireland, o que pode suscitar no utilizador a sensação de uma vigilância contínua da sua vida privada".

como o número de pessoas envolvidas no seu tratamento, o número de titulares de dados afectados pelo tratamento[42], a duração do tratamento dos dados pessoais, o volume de dados pessoais em causa e a existência de uma eventual combinação com outros dados[43], uma vez que pode conduzir ao tratamento de categorias especiais de dados pessoais como dar azo a previsões incertas ou incorrectas[44] e, por conseguinte, gerar um impacto maior na esfera do titular dos dados pessoais. Significa isto que quanto mais invasivo for o tratamento, mais difícil será para o responsável pelo tratamento dos dados pessoais justificar o mesmo.

Quanto às expectativas razoáveis do titular dos dados pessoais[45], importa compreender o contexto em que surge o tratamento dos dados pessoais deste último e como esse tratamento lhe foi comunicado e o que lhe foi dito em específico, a sua relação com o responsável pelo tratamento dos dados pessoais e ainda natureza da relação ou do serviço prestado ou as obrigações jurídicas ou contratuais aplicáveis[46]. Por

---

[42] European Data Protection Board, Guidelines 1/2024…, p. 16, realça para o seguinte: "(…) the controller should not base its assessment of the interests at stake on an assumption that all of the affected data subjects share the same interests when it has – or should have – concrete indications of the existence of particular individual interests or when, from an objective perspective, it is simply not likely that all data subjects will have the same interest(s) the controller has assumed. This is especially true in the context of an employer-employee relationship".

[43] Grupo de Trabalho do artigo 29.º para a Protecção de Dados, *Parecer 06/2014 sobre o conceito de interesses legítimos…*, p. 62: "(…) por exemplo, no caso da elaboração de perfis, para fins comerciais, de aplicação da lei ou outros".

[44] Grupo de Trabalho do artigo 29.º para a Protecção de Dados, *Parecer 06/2014 sobre o conceito de interesses legítimos…,* p. 62: "(…) por exemplo, a respeito do comportamento ou da personalidade das pessoas em causa".

[45] A este respeito, *douto* Acórdão do Tribunal de Justiça, Processo C-708/18, Asociaţia de Proprietari bloc M5A-ScaraA, 11 de dezembro de 2019 (ECLI:EU:C:2019:1064), para. 58; e *douto* Acórdão do Tribunal de Justiça, Processo C-252/21, Meta v. Bundeskartellamt, 04 de julho de 2023 (ECLI:EU:C:2023:537), para. 117: (…) apesar da gratuitidade dos serviços de uma rede social em linha como o Facebook, o utilizador desta não pode razoavelmente esperar que, sem o seu consentimento, o operador dessa rede social trate os dados pessoais desse utilizador para efeitos de personalização da publicidade (…)".

[46] CANTO MONIZ, Graça, *Manual de Introdução à Protecção…*, Edições Almedina, S.A., 2024, p. 96 dá os seguintes exemplos: "(…) não é de esperar videovigilância em instalações sanitárias ou saunas, em espaços habitados ou em gabinetes de exame e de tratamento. Por outro lado, o cliente típico de um banco esperará ser vigiado no interior do banco ou enquanto levanta dinheiro de uma caixa de multibanco". Outros exemplos, *European Data Protection Board, Guidelines* 1/2024…, p. 18.

exemplo, quanto mais próxima for a relação entre aqueles, maior relevância deverá ser atribuída aos interesses dos titulares dos dados pessoais. Com efeito, todo o contexto factual é relevante para aferir a razoabilidade das expectativas criadas pelo titular dos dados pessoais quanto ao tratamento dos seus dados pessoais numa situação concreta. Por outras palavras, cumpre apurar se, na mesma situação concreta, um terceiro "médio" criaria, igualmente, expectativas quanto ao aludido tratamento[47].

Por fim, a relação entre o titular dos dados pessoais e o responsável pelo tratamento desses dados pessoais será influenciada, por um lado, pela posição mais ou menos dominante deste último em relação ao primeiro, isto é, se estamos perante uma pessoa singular ou pessoa colectiva e, quanto a esta última, qual a sua dimensão[48], o posicionamento daquele no mercado ou na sociedade em geral. Por outro lado, e ao contrário do que pode indiciar o legislador ao consagrar no art. 8.º do RGPD um regime especial aplicável às crianças, a vulnerabilidade aqui abordada não se circunscreve apenas a estas. O titular dos dados pessoais pode necessitar de uma protecção especial, por exemplo, em virtude da capacidade jurídica diminuída ou da idade[49].

---

[47] A este respeito, European Data Protection Board, *Guidelines 1/2024…*, p. 17: "The fact that certain types of personal data are commonly processed in a given sector does not necessarily mean that the data subject can reasonably expect such processing".

[48] Grupo de Trabalho do artigo 29.º para a Protecção de Dados, *Parecer 06/2014 sobre o conceito de interesses legítimos…*, p. 63: "Uma grande empresa multinacional pode, por exemplo, ter mais recursos e poder de negociação do que a pessoa singular em causa, pelo que pode estar em melhores condições de impor à pessoa em causa o que acredita ser o seu «interesse legítimo»".

[49] Para o efeito, leia-se os Considerandos 38 e 75 do RGPD. Igualmente, dando enfâse à protecção em caso de comercialização, de criação de perfis de personalidade ou de utilizador, e de proposta de serviços, o *douto* Acórdão do Tribunal de Justiça, Processo C-252/21, Meta v. Bundeskartellamt, para. 111 e 123: "(…) o objetivo de melhoria do produto possa, tendo em conta a amplitude desse tratamento e o seu impacto significativo no utilizador, bem como a circunstância de este último não poder razoavelmente esperar que esses dados sejam tratados pela Meta Platforms Ireland, prevalecer sobre os interesses e os direitos fundamentais desse utilizador, tanto mais na hipótese de este ser uma criança".

Com uma visão diversa da vulnerabilidade da criança, o douto Acórdão do Tribunal de Justiça, Processo C-13/16, Rīgas Satiksme, 04 de maio de 2017 (ECLI:EU:C:2017:336), para. 33: "(…) não se afigura justificado, em condições como as que estão em causa no processo

Concluindo, a apreciação do impacto do tratamento não visa evitar a repercussão de quaisquer consequências negativas na esfera do titular dos dados pessoais, mas sim evitar que o seu impacto seja desajustado e desproporcional[50], por consonância com os princípios basilares que regem o RGPD (art. 5.º) e as próprias obrigações adjacentes à figura do responsável pelo tratamento dos dados pessoais, resultantes do disposto no art. 25.º do mesmo diploma. O teste de ponderação apresenta-se, assim, como uma mais-valia no momento de avaliar cada dessas consequências potenciais e reais, negativas e positivas, na medida em que auxilia o responsável pelo tratamento dos dados pessoais a discriminar cada uma dessas consequências e, por conseguinte, a medir o peso que cada uma delas assume no caso concreto.

3.3. Equilíbrio provisório

Realizada a ponderação entre o interesse legítimo do responsável pelo tratamento ou de terceiro e o impacto que esse tratamento assume na esfera do titular dos dados pessoais, o responsável pelo tratamento dos dados pessoais adopta as medidas técnicas e organizativas adequadas e em conformidade com os princípios basilares, previstos no artigo 5.º do RGPD conjugado com os art. 24.º e 32.º do mesmo diploma, como com os deveres de informação a que este está incumbido, previstos nos art. 12.º, 13.º e 14.º do RGPD.

Porém, nem sempre poderá ser linear que o impacto desse tratamento na esfera do titular dos dados pessoais seja reduzido, desajustado e desproporcional[51]. Pelo que, a realização de uma nova ponderação

principal, recusar a uma parte lesada a comunicação dos dados pessoais necessária à propositura de uma ação de indemnização contra o autor do dano ou, se for o caso, contra as pessoas que exerçam o poder parental, por esse autor ser menor".

[50] Neste sentido, European Data Protection Board, *Guidelines 1/2024…,* p. 13.

[51] Grupo de Trabalho do artigo 29.º para a Protecção de Dados, *Parecer 06/2014 sobre o conceito de interesses legítimos…*, p. 64: "O cumprimento integral deve implicar que o impacto nas pessoas seja reduzido, que seja menos provável que os interesses ou os direitos e liberdades fundamentais das pessoas em causa sejam afectados e que, por isso, seja mais provável que o responsável pelo tratamento dos dados possa invocar o artigo 7.º, alínea f)".

entre aqueles dois elementos, com base na ponderação já realizada, terá um papel crucial no processo de equilíbrio entre aqueles dois elementos.

Adicionalmente, neste processo de equilíbrio, o responsável pelo tratamento dos dados pessoais pode equacionar a introdução de medidas complementares, tendo em vista a reduzir o impacto indevido desse tratamento na esfera do titular dos dados pessoais, que não se conseguiu atingir numa primeira ponderação.

3.4. Garantias complementares

No processo de equilíbrio entre o interesse legítimo do responsável pelo tratamento ou de terceiro e o impacto que esse tratamento assume na esfera do titular dos dados pessoais, a adopção de medidas complementares/atenuantes poderá ser determinante na redução do impacto indevido desse tratamento na esfera do titular dos dados pessoais.

Contudo, na eventualidade da adopção dessas medidas atenuantes não se revelar suficiente para determinar a prevalência do interesse legítimo do responsável pelo tratamento ou de terceiro em relação aos interesses, direitos e liberdades fundamentais do titular dos dados pessoais, o responsável pelo tratamento dos dados pessoais deverá abster-se da realização de qualquer tratamento, sob pena do mesmo ser considerado ilícito.

A adopção de medidas complementares[52] pelo responsável pelo tratamento dos dados pessoais pode passar pela disponibilização de um mecanismo viável e acessível para assegurar que os titulares dos dados pessoais possam optar, de forma incondicional, por não permitir o tratamento; limitação rigorosa do volume de dados recolhidos; eliminação imediata de dados após utilização; implementação de medidas técnicas

[52] A este propósito, Grupo de Trabalho do artigo 29.º para a Protecção de Dados, *Parecer 06/2014 sobre o conceito de interesses legítimos…*, pp. 65-67.

e organizativas para assegurar que os dados não possam ser utilizados para tomar decisões ou outras medidas em relação às pessoas (a chamada "separação funcional"); utilização ampla de técnicas de anonimização, de agregação de dados, de pseudónimos, a encriptação de dados armazenados ou em trânsito; realização de avaliações de impacto; criação de uma maior transparência na sua relação com o titular dos dados pessoais; e portabilidade dos dados e medidas afins para capacitar as pessoas em causa.

Em face do exposto, facilmente, se depreende que muitas dessas garantias complementares aproximam-se de direitos conferidos aos titulares pelo RGPD, destinados a assegurar transparência, controlo e protecção efectiva relativamente ao tratamento dos seus dados pessoais. Outras medidas, por sua vez, coincidem, em larga medida, com obrigações já impostas pelo próprio RGPD ao responsável pelo tratamento dos dados pessoais. A diferença está em que, uma vez accionadas, tais garantias podem conferir ao titular dos dados um mível de acrescido de salvaguarda, atenuando de forma mais eficaz os efeitos do tratamento na esfera do titular dos dados pessoais do que aquele que resultaria da aplicação estrita das disposições do RGPD[53].

Adoptada uma medida atenuante, o responsável pelo tratamento dos dados pessoais deverá respeitar a decisão tomada pelo titular desses dados, sem que lhe seja possível alterar ou eliminar a garantia anteriormente conferida e/ou proceder a uma nova ponderação.

---

[53] Vejamos exemplos: Uma plataforma de comércio eletrónico que obtenha dados de terceiros pode, além de cumprir o dever de informação previsto no art. 14.º do RGPD, disponibilizar ao titular dos dados um painel digital interactivo que lhe permita verificar a origem dos dados, os destinatários e exercer de imediato os direitos de apagamento ou oposição; Uma instituição bancária, para além de prestar as informações obrigatórias no âmbito dos arts. 13.º e 14.º, pode fornecer relatórios periódicos sobre todas as operações de tratamento efectuadas, reforçando a transparência e permitindo ao cliente detectar eventuais abusos; Um hospital, além de implementar medidas de segurança para dados sensíveis (art. 9.º do RGPD), pode oferecer aos pacientes alertas automáticos sempre que os seus dados clínicos sejam acedidos, reforçando o direito de acesso e a transparência; Já uma empresa de telecomunicações, no exercício do direito à portabilidade previsto no art. 20.º do RGPD, pode simplificar o processo mediante a criação de mecanismos automáticos de migração de conta, atenuando os impactos burocráticos e técnicos para o titular.

4. A transparência e informação como pedra angular

Feito o estudo sobre o teste de ponderação que deverá ser realizado antes da subsunção de um caso concreto ao disposto na alínea f) do n.º 1 do art. 6.º do RGPD, facilmente, se compreende como a transparência e o cumprimento dos deveres de informação previstos nos art. 12.º, 13.º e 14.º, todos do RGPD pelo responsável pelo tratamento dos dados pessoais poderão revelar-se fulcrais para evitar males maiores, como a ruptura da relação entre o responsável pelo tratamento dos dados pessoais e o titular dos dados pessoais e/ou impactos indevidos na esfera jurídica das Partes envolvidas, com consequências nefastas que, bem geridas, teriam sido acauteladas. Vejamos.

Quanto maior for a transparência no tratamento de dados pessoais com base na aplicação da alínea f) do n.º 1 do art. 6.º do RGPD, menor será, em princípio, o impacto daquele na esfera das Partes envolvidas. Tanto assim é que o legislador condiciona o responsável pelo tratamento dos dados pessoais a um cuidado redobrado na informação a prestar ao titular dos dados pessoais quando estamos perante um tratamento de dados pessoais com fundamento num interesse legítimo daquele ou de terceiro, conforme o disposto na alínea d) do n.º 1 do art. 13.º e alínea b) do n.º 1 do art. 14.º do RGPD, sem prejuízo naturalmente do direito de acesso que assiste, a todo o momento, ao titular dos dados pessoais, nos termos do disposto no art. 15.º do RGPD.

Primeiramente, esta transparência permitirá ao titular tomar conhecimento integral do tratamento dos dados pessoais, mais concretamente, os dados objecto de tratamento, a forma de tratamento, a finalidade de tratamento e ainda o fundamento jurídico que está na base desse tratamento.

Por conseguinte, a expectativa criada pelo titular dos dados pessoais relativamente ao tratamento realizado será, em princípio, a mais próxima da realidade.

Por outro lado, garantirá o exercício efectivo dos direitos do titular dos dados pessoais, bem como das próprias medidas atenuantes que tenham sido implementadas, fruto do teste de ponderação entre o

interesse legítimo do responsável pelo tratamento dos dados pessoais ou de terceiro e o impacto deste nos interesses, direitos e liberdades fundamentais do titular dos dados pessoais em causa.

Por último, e não menos importante, o envolvimento do titular dos dados pessoais no tratamento de dados pessoais em causa, contribuirá para que se verifique menos consequências nefastas para ambas as Partes, reduzindo, assim, a probabilidade do aludido tratamento vir a ser considerado ilícito.

Em face do exposto, e ainda que o legislador não o exija expressamente, nos casos em que o fundamento jurídico seja o previsto na alínea f) do n.º 1 do art. 6.º do RGPD, somos do entendimento que o responsável pelo tratamento de dados pessoais deverá informar o titular dos dados pessoais da realização do teste de ponderação, bem como de todo o seu processo, a fim do titular dos dados pessoais dispor de uma informação completa e, em consequência, o tratamento dos seus dados ser caracterizado como justo e transparente[54]. Até porque, como vimos, decorre do disposto no n.º 2 do art. 5.º do RGPD, que cabe ao responsável pelo tratamento dos dados pessoais demonstrar a conformidade do tratamento com o RGPD.

Pelo que, só por força do princípio da responsabilidade entende-se que recai sobre o responsável pelo tratamento de dados pessoais um dever de prestar informação relativamente ao teste de ponderação previamente realizado e que determinou a aplicação do fundamento jurídico previsto na alínea f) do n.º 1 do art. 6.º do RGPD.

Por esta razão, consideramos que a transparência e o cumprimento pelo responsável pelo tratamento dos dados pessoais do seu dever de informação são a âncora na relação entre este e o titular dos dados pessoais, uma vez que a discordância entre estes resulta, geralmente, pela falta de transparência no tratamento dos dados pessoais pelo responsável pelo tratamento.

---

[54] O mesmo se dirá relativamente ao direito de acesso previsto no art. 15.º do RGPD. Neste sentido, European Data Protection Board, *Guidelines 1/2024…,* p. 21

5. Evolução da Jurisprudência do Tribunal de Justiça da União Europeia

Analisados todos os requisitos legais que compõem o disposto na alínea f) n.º 1 do art. 6.º do RGPD, cumpre-nos elucidar qual tem vindo a ser a posição adoptada pelo Tribunal de Justiça da União Europeia nas suas decisões.

Primeiramente, tal como resulta dos *doutos* Acórdãos do Tribunal de Justiça, Processo C-13/16, Rīgas Satiksme, 04 de maio de 2017 (ECLI:EU:C:2017:336), para. 99; Processo C-252/21, Meta v. Bundeskartellamt, 04 de julho de 2023 (ECLI:EU:C:2023:537), para. 90; Processo C-582/14, Patrick Breyer, 19 de outubro de 2016 (ECLI:EU:C:2016:779); Processo C-439/19, Latvijas Republikas Saeima, 22 de junho de 2021 (ECLI:EU:C:2021:504); e Processo C-26/22 e C-64/22, SCHUFA Holding AG, 07 de dezembro de 2023 (ECLI:EU:C:2023:958), é unânime que o art. 6.º do RGPD prevê uma lista exaustiva e taxativa dos casos em que um tratamento de dados pessoais ser considerado lícito. Assim, para ser considerado legítimo, um tratamento deve ser abrangido por um dos casos previstos nesta disposição.

Por conseguinte, o Tribunal de Justiça também já declarou, no *douto* Acórdão datado de 04 de julho de 2023, Processo C-252/21, Meta v. Bundeskartellamt (ECLI:EU:C:2023:537), para. 94, que, quando seja possível constatar que um tratamento de dados pessoais é necessário à luz de uma das justificações previstas nas alíneas b) a f) do n.º 1 do art. 6.º do RGPD, não há que determinar se esse tratamento está igualmente abrangido por outra dessas justificações.

Igualmente, no *douto* Acórdão datado de 04 de julho de 2023, Processo C-252/21, Meta v. Bundeskartellamt (ECLI:EU:C:2023:537), para. 106; no *douto* Acórdão datado de 17 de junho de 2021, Processo C-597/19, M.I.C.M. (ECLI:EU:C:2021:492), para. 106; e no *douto* Acórdão datado de 07 de dezembro de 2023, Processo C-26/22 e C-64/22, SCHUFA Holding AG (ECLI:EU:C:2023:958), é pacífico para

o Tribunal de Justiça que a alínea f) do n.º 1 do art.º 6 do RGPD, prevês três requisitos cumulativos para que um tratamento de dados pessoais seja lícito, a saber: a prossecução de interesses legítimos pelo responsável pelo tratamento ou por terceiros; a necessidade do tratamento dos dados pessoais para a realização do interesse legítimo prosseguido; e o requisito de os interesses ou direitos e liberdades fundamentais da pessoa a quem a protecção de dados diz respeito não prevalecerem.

Com efeito, o que tem gerado controvérsia é, precisamente, a verificação de cada um desses requisitos num determinado caso concreto. Vejamos:

5.1. Caso Rīgas Satiksme – Processo C-13/16

No seguimento de um acidente, Rīgas Satiksme necessitava de informações sobre a pessoa que já tinha sido sancionada administrativamente pelo mesmo, mais concretamente o endereço e/ou número de identificação dessa pessoa, com vista a intentar a competente acção cível, uma vez que à luz do Direito Letão o demandante deve, pelo menos, ter conhecimento do local de residência do demandado. Pelo que, discutiu-se se a polícia nacional estava obrigada a revelar os dados pessoais solicitados a Rīgas Satiksme.

O Tribunal de Justiça considerou, e bem, que não havia dúvidas que o interesse de um terceiro em obter uma informação de ordem pessoal sobre uma pessoa que danificou os seus bens para instaurar uma acção contra essa pessoa constituía um interesse legítimo.

Igualmente, o Tribunal de Justiça entendeu verificado o requisito da necessidade do tratamento desses dados, na medida em que "a comunicação meramente do nome e do apelido da pessoa que é autora do dano não permite identificá-la com precisão suficiente para poder instaurar contra ela uma acção. Assim, afigura-se necessário para esse efeito obter igualmente o endereço e/ou o número de identificação dessa pessoa". A este respeito, recordemos sobre a essência que está neste

requisito – o interesse legítimo em estudo não podia ser razoavelmente alcançado de modo igualmente eficaz através de outros meios menos lesivos das liberdades e dos direitos fundamentais dos titulares dos dados, revelando-se, como vimos, os referidos dados como estritamente necessários para a finalidade de tratamento que se visava prosseguir, *in casu,* a instauração de uma acção cível.

Por último, e não menos importante, no que respeita à ponderação dos direitos e interesses opostos, teve-se em consideração a idade do titular dos dados que, *in casu*, era menor. Contudo, ainda assim, o Tribunal de Justiça entendeu que "não se afigura justificado, em condições como as que estão em causa no processo principal, recusar a uma parte lesada a comunicação dos dados pessoais necessária à propositura de uma acção de indemnização contra o autor do dano ou, se for o caso, contra as pessoas que exerçam o poder paternal, por esse autor menor".

Concluindo-se que, sempre que o direito nacional o exija, pode revelar-se imperioso comunicar dados pessoais a um terceiro a fim de lhe permitir instaurar uma acção de indemnização num tribunal cível por um dano causado pela pessoa interessada na protecção desses dados, à luz da alínea f) do n.º 1 do art. 6.º do RGPD.

5.2. Caso SCHUFA Holding AG – Processo C-26/22 e C-64/22

SCHUFA é uma sociedade privada que fornece informações comerciais que regista e conserva, nas suas próprias bases de dados, informações provenientes de registos públicos, nomeadamente relativas às remissões de dívida remanescente. Esta sociedade procede à supressão destas informações decorrido um prazo de três anos do seu registo, em conformidade com o código de conduta elaborado, na Alemanha, pela associação que agrupa sociedades que fornecem informações comerciais e aprovado pela autoridade de controlo competente.

Quanto à observância de um interesse legítimo, o Tribunal de Justiça entendeu que "embora o tratamento de dados pessoais como o que está em causa nos processos principais sirva os interesses

económicos da SCHUFA, esse tratamento também serve para prosseguir o interesse legítimo dos parceiros contratuais da SCHUFA, que pretendem celebrar contratos relativos a um crédito com pessoas, de poder avaliar a solvabilidade destas e, portanto, os interesses do sector de crédito num plano socioeconómico".

Contudo, não verificou a existência de necessidade desse tratamento, atendendo que esse tratamento implicaria, por um lado, uma conservação desses dados num registo público na Internet por um período de seis meses, a contar da data das decisões judiciais de remissão antecipada da dívida remanescente proferidas nos respectivos processos de insolvência, à luz da legislação alemã. Por outro lado, uma conservação desses dados nas bases de dados das sociedades que fornecem informações comerciais, não procedendo a essa conservação por ocasião do caso concreto, mas na eventualidade de os seus parceiros contratuais virem a pedir-lhe tais informações no futuro, com base num código de conduta na acepção do art. 40.º RGPD. A isto, acresce ainda o facto destas sociedades conservarem esses dados durante três anos, ao passo que a legislação alemã prevê, no que respeita ao registo público, um prazo de conservação de apenas seis meses.

A par disto, na ponderação dos direitos e interesses opostos, o Tribunal de Justiça também verificou que tal tratamento de dados pessoais pela SCHUFA, nas suas próprias bases de dados, por período superior aos seis meses implicaria uma ingerência grave nos direitos fundamentais dos titulares dos dados em causa. O legislador alemão considerou que, depois de expirado o aludido prazo seis meses, os direitos e interesses do titular dos dados prevalecem sobre os do público em dispor dessa informação, na medida em que "esses dados servem como um factor negativo na avaliação da solvabilidade da pessoa em questão e constituem, portanto, informações sensíveis sobre a sua vida privada", o que dificultaria, de alguma forma, o exercício das suas liberdades, como participar novamente na vida económica.

Assim, um código de conduta que conduza a uma apreciação diferente da obtida em aplicação da alínea f) do n.º 1 do art. 6.º do RGPD

não poderá ser tomada em consideração na ponderação efectuada ao abrigo desta disposição legal.

Concluindo, o Tribunal de Justiça determinou que o prazo de conservação e a natureza dos dados pessoais foram determinantes na ponderação dos direitos e interesses opostos. A este propósito, nós acrescentaríamos um outro critério – expectativa do titular dos dados pessoais, no sentido em que existindo um registo público oficial dos referidos dados pessoais, que os conserva pelo período de seis meses, à luz da legislação nacional, não é expectável para os titulares desses dados pessoais que, esses dados pessoais, sejam tratados por outras pessoas, por período superior ao legalmente fixado.

Em consonância com o *supra* exposto, SCHUFA foi obrigada a apagar, sem demora injustificada, os referidos dados pessoais, no seguimento do exercício do direito de apagamento pelo titular dos dados pessoais, previsto na alínea d) do n.º 1 do art. 17.º do mesmo diploma.

6. Consequências da violação do princípio da licitude

Nos termos do disposto no n.º 2 do art. 5.º do RGPD, cabe ao responsável pelo tratamento demonstrar o preenchimento de todos os pressupostos previstos na alínea f) do n.º 1 do art. 6.º do RGPD.

Por outras palavras, é da responsabilidade daquele certificar que o tratamento de dados pessoais realizado ao abrigo daquela disposição legal visa a prossecução de um interesse legítimo, que existe a necessidade do aludido tratamento de dados pessoais para efeito de prossecução desse interesse legítimo e, por sua vez, que, na situação em concreto, os interesses ou direitos e liberdades fundamentais do titular dos dados não prevaleçam em relação ao interesse legítimo a ser prosseguido pelo responsável pelo tratamento.

Pelo que, aconselha-se ao responsável pelo tratamento dos dados pessoais a documentar, sempre que possível, de forma pormenorizada o raciocínio desenvolvido em todo o teste de ponderação realizado antes

de iniciar qualquer tratamento de dados pessoais, a fim de demonstrar e comprovar a subsunção do caso concreto ao disposto na alínea f) do n.º 1 do art. 6.º do RGPD[55]. Uma mais-valia será, também, o responsável pelo tratamento dos dados pessoais auxiliar-se do conhecimento especializado do Encarregado de Protecção de Dados, nas situações em que tenha sido designado, garantindo o envolvimento deste em todo o processo, em cumprimento do disposto no n.º 1 do art. 38.º do RGPD.

A falta de um destes requisitos origina, como vimos, na ilicitude do tratamento de dados pessoais efectuado, o que poderá acarretar a responsabilidade civil do responsável pelo tratamento dos dados pessoais, aplicando-se, neste caso, o Direito interno do Estado-Membro competente, nos termos do disposto no art. 82.º conjugado com o art. 79.º, ambos do RGPD. Igualmente, tal conduta materializa-se numa contra-ordenação muito grave, por força do disposto na alínea a) do n.º 5 do art. 83.º do RGPD, o que acarreta também na responsabilidade contra-ordenacional do responsável pelo tratamento dos dados pessoais, mediante a aplicação de uma coima nos termos do aludido art. 83.º do RGPD. Por último, não menos importante, ao abrigo da Lei n.º 58/2019, de 08 de agosto, o responsável pelo tratamento pode ainda ser responsabilizado criminalmente, por acesso indevido a dados pessoais, previsto no seu art. 47.º.

Destarte, facilmente, se compreende a importância que a realização de um teste de ponderação cuidado e focado no caso concreto pode aqui assumir, atendendo que, por um lado, evita impactos indevidos na esfera dos interesses, direitos e/ou liberdades fundamentais do titular dos dados pessoais, por outro lado, acautela eventuais responsabilidades civil, contra-ordenacional e/ou criminal do responsável pelo tratamento de dados pessoais.

---

[55] Neste sentido, Grupo de Trabalho do artigo 29.º para a Protecção de Dados, in *Parecer 06/2014 sobre o conceito de interesses legítimos…*, p. 68. Igualmente, European Data Protection Board, *Guidelines 1/2024…*, p. 2

6.1. Em especial os direitos do titular dos dados pessoais ao abrigo do RGPD

Sem prejuízo do *supra* exposto, o RGPD oferece ao titular dos dados pessoais um conjunto de direitos passíveis de serem exercidos por este último como reacção a um tratamento ilícito de dados pessoais.

Primeiramente, o titular dos dados pessoais pode exercer o seu direito a apresentar uma reclamação junto da autoridade de controlo competente, ao abrigo e nos termos do n.º 1 do art. 77.º do RGPD.

Perante o tratamento ilícito dos seus dados pessoais, o titular pode ainda exercer, a qualquer momento, o seu direito de oposição ao referido tratamento, devendo, nesse caso, o responsável pelo tratamento cessar imediatamente o tratamento desses dados pessoais, ao abrigo do n.º 1 do art. 21.º do RGPD. E, por conseguinte, o titular pode exigir o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, igualmente, sem demora injustificada, conforme o disposto na alínea c) do n.º 1 do art. 17.º do mesmo diploma.

Em alternativa ao direito de oposição e direito ao apagamento, o titular pode apenas limitar o tratamento desses dados pessoais por recurso ao disposto na alínea b) do n.º 1 do art. 18.º do aludido diploma.

Contudo, com uma particularidade, o exercício tanto dos direitos de oposição, de apagamento, como de limitação do tratamento, pressupõe a demonstração pelo titular dos dados pessoais da prevalência dos seus interesses, direitos e/ou liberdades sobre as razões que conduziram ao tratamento dos seus dados pessoais pelo responsável pelo tratamento.

Esta condição não afasta a responsabilidade que recai sobre este último – de demonstrar o preenchimento de todos os pressupostos previstos na alínea f) do n.º 1 do art. 6.º do RGPD. Tanto assim é que o disposto na alínea d) do n.º 1 do art. 18.º do RGPD estipula que em caso do titular dos dados pessoais tiver oposto ao tratamento dos seus dados nos termos do n.º 1 do art. 21.º do mesmo diploma, este observará, de

facto, uma limitação do tratamento dos seus dados pessoais, porém, "até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados". O que sucede é que, nestes casos, o interesse legítimo invocado pelo responsável pelo tratamento e os interesses, direitos e liberdades fundamentais do titular dos dados pessoais serão objecto de uma nova ponderação, desta vez, realizada pela autoridade de controlo competente e/ou tribunal competente[56].

7. Conclusões

O presente estudo centrou-se num dos fundamentos jurídicos que poderão justificar determinado tratamento de dados pessoais pelo responsável pelo tratamento de dados pessoais e taxativamente previstos no art. 6.º do RGPD, mais concretamente, no interesse legítimo do responsável pelo tratamento de dados pessoais ou de terceiro como fundamento de licitude. Tal deveu-se à nossa preocupação com os frequentes abusos por parte dos responsáveis pelo tratamento de dados pessoais na subsunção arbitrária do referido tratamento à alínea f) do n.º 1 art. 6.º do RGPD a qualquer situação concreta e, sobretudo, quando não conseguem subsumir a nenhum dos outros fundamentos de licitude previstos no aludido art. 6.º do RGPD.

Nos termos da alínea f) do n.º 1 do art. 6.º do RGPD, este fundamento de licitude de tratamento de dados pessoais pressupõe que o aludido tratamento preencha, cumulativamente, os seguintes requisitos: prossecução de interesses legítimos pelo responsável pelo tratamento ou terceiro; necessidade desse tratamento para efeito dos interesses legítimos; e não prevalência de interesses ou direitos e liberdades fundamentais do titular dos dados que exijam protecção, em especial se o titular for uma criança.

---

[56] Seguindo uma posição semelhante, Grupo de Trabalho do artigo 29.º para a Protecção de Dados*, in Parecer 06/2014 sobre o conceito de interesses legítimos…,* p. 70.

A presença de conceitos indeterminados tem gerado algumas dificuldades de interpretação e, por sua vez, de aplicação deste fundamento de licitude. Pelo que, as autoridades de controlo e os tribunais assumem aqui um papel fulcral na concretização dos conceitos indeterminados aqui presentes, através de uma avaliação cuidada e casuística, uma vez que o legislador não atribuiu quaisquer competências à União Europeia ou aos Estados-Membros para o efeito. A este respeito, os *doutos* Acórdãos proferidos, por exemplo, nos casos Rīgas Satiksme, Asociaţia de Proprietari bloc M5A-ScaraA e Meta v. Bundeskartellamt, Patrick Breyer, M.I.C.M, Latvijas Republikas Saeima e SCHUFA Holding AG, poderão, efectivamente, ajudar na análise do caso concreto. Igualmente, o Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na acepção do art. 7.º da Directiva 95/46/CE, 09 de abril de 2014 elaborado pelo Grupo de Trabalho do artigo 29.º para a Protecção de Dados e, mais recentemente, a Directrizes 1/2024 sobre o processamento de dados pessoais com base na alínea f) do n.º 1 do art. 6.º do RGPD, elaborado pelo European Data Protection Board. Em Portugal, a Comissão Nacional de Protecção de Dados também tem desempenhado essa função de concretização, como se verifica na Deliberação n.º 1039/2017, onde balizou o tratamento de dados resultante da gravação de chamadas com fundamento no interesse legítimo. O mesmo já se tinha verificado na Deliberação n.º 61/2004, a respeito da utilização de sistemas de videovigilância para protecção de pessoas e bens como interesse legítimo. Igualmente, a jurisprudência portuguesa tem dado o seu contributo – veja-se, por exemplo, os já citados *doutos* Acórdão do Tribunal da Relação de Lisboa, proc. 17/10.7TTBRR.L1-4, 16 de Novembro de 2011; Acórdão do Tribunal Constitucional n.º 268/2022, proc. n.º 828/19; Acórdão do Supremo Tribunal de Justiça, proc. 2335/06.0TMPRT-D.P1.S1, 23 de Fevereiro de 2021.

De todo o modo, podemos definir o interesse legítimo do responsável pelo tratamento dos dados pessoais ou de terceiro a quem esses dados tenham sido comunicados como uma vantagem concreta, de qualquer natureza, que o responsável pelo tratamento dos dados pessoais ou terceiro irão beneficiar através do tratamento desses dados pessoais,

devendo, por isso, o interesse aqui em estudo ser lícito, concreto, efectivamente prosseguido e não meramente abstracto e hipotético, no momento da tomada de decisão do tratamento de dados pessoais.

Por sua vez, o tratamento de dados pessoais em causa deverá revelar-se como necessário na prossecução do interesse legítimo identificado, não se observando uma alternativa menos intrusiva na esfera do titular dos dados pessoais.

Sucede, porém, que esta disposição legal está subordinada a um teste de ponderação, na medida em que exige ao responsável pelo tratamento uma ponderação entre um determinado interesse legítimo e o impacto que o tratamento de dados pessoais irá repercutir no titular desses dados pessoais, devendo ainda acautelar, a todo o momento, que a prossecução do interesse ou o exercício do direito ou liberdade deste último não prevalece em relação àquele.

Neste sentido, o teste de ponderação apresenta-se como uma mais-valia no momento de avaliar cada uma dessas consequências potenciais e reais, negativas e positivas, na medida em que auxilia o responsável pelo tratamento dos dados pessoais a discriminar cada uma dessas consequências e, por conseguinte, a medir o peso que cada uma delas assume no caso concreto.

Concluído o teste de ponderação, o responsável pelo tratamento dos dados pessoais deverá abster-se de iniciar qualquer tratamento dos dados pessoais, sempre que falhe um dos pressupostos previstos na alínea f) do n.º 1 do art. 6.º do RGPD, atendendo que a falta de um desses pressupostos poderá acarretar na responsabilidade civil, contra-ordenacional e até penal do responsável pelo tratamento dos dados pessoais, porquanto recai neste a responsabilidade de demonstrar a observância de todos aludidos pressupostos legais, por força do disposto no n.º 2 do artigo 5.º do RGPD.

Pelo que, a participação do Encarregado de Protecção de Dados em todo o processo de ponderação, nas situações em que tenha sido designado, será uma mais-valia, face ao seu conhecimento especializado em Direito da Protecção dos Dados Pessoais.

A par disto, o envolvimento do titular dos dados pessoais no tratamento de dados pessoais, contribuirá, decisivamente, para um menor número de consequências nefastas para todas as Partes, incluindo o responsável pelo tratamento dos dados pessoais, bem como para a diminuição da probabilidade de o tratamento vir a ser considerado ilícito. Quanto maior for a transparência no tratamento de dados pessoais com base na aplicação na alínea f) do n.º 1 do art. 6.º do RGPD menor será, em princípio, o impacto daquele na esfera das Partes envolvidas.

Concluindo, o legislador não faz qualquer distinção entre o fundamento de licitude previsto da alínea f) do n.º 1 do art. 6.º do RGPD em relação aos restantes fundamentos de licitude consagrados no aludido preceito. Pelo contrário, coloca-os em pé de igualdade.

Com efeito, o legislador assume a possibilidade de um determinado tratamento de dados pessoais estar justificado por mais do que um fundamento de licitude previsto no n.º 1 do art. 6.º do RGPD. Importa, contudo, sublinhar que desta formulação não decorre que os responsáveis pelo tratamento possam escolher livremente o fundamento de licitude a posteriori, como se se tratasse de um mecanismo de substituição (cherry picking). Ainda assim, a nosso ver, é suficiente a subsunção da situação concreta apenas a uma das alíneas do aludido preceito legal para admitir-se que o tratamento de dados pessoais em causa está justificado.

Em suma, o fundamento de licitude previsto na alínea f) do n.º 1 do art. 6.º do RGPD não contém, por um lado, um carácter mais geral em comparação com os restantes fundamentos de licitude previstos no aludido art. 6.º do RGPD. Por outro lado, não contem um âmbito de aplicação residual, ainda que se sugira uma análise prévia de subsunção a um dos outros fundamentos de licitude aí previstos. Na verdade, apenas contém uma particularidade em relação aos restantes fundamentos de licitude previstos no RGPD, requer uma avaliação cuidada e casuística, auxiliada por um teste de ponderação antes da tomada de decisão de qualquer tratamento de dados pessoais pelo responsável pelo tratamento com fundamento num interesse legítimo deste ou de terceiro,

e com um reforço nos deveres de informação que recaem sobre estes e previstos nos art. 12.º, 13.º e 14.º do RGPD.

Bibliografia

Acórdão do Tribunal Constitucional n.º 268/2022, proc. n.º 828/19

Acórdão do Tribunal da Relação de Lisboa, proc. 17/10.7TTBRR.L1-4, 16 de Novembro de 2011

Acórdão do Tribunal de Justiça da União Europeia, Processo C-468/10 e C-469/10, ASNEF- FECEMD, 24 de novembro de 2011 (ECLI:EU:C:2011:777)

Acórdão do Tribunal de Justiça da União Europeia, Processo C-582/14, Patrick Breyer, 19 de outubro de 2016 (ECLI:EU:C:2016:779)

Acórdão do Tribunal de Justiça da União Europeia, Processo C-13/16, Rīgas Satiksme, 04 de maio de 2017 (ECLI:EU:C:2017:336)

Acórdão do Tribunal de Justiça da União Europeia, Processo C-708/18, Asociaţia de Proprietari bloc M5A-ScaraA, 11 de dezembro de 2019 (ECLI:EU:C:2019:1064)

Acórdão do Tribunal de Justiça da União Europeia, Processo C-597/19, M.I.C.M, datado de 17 de junho de 2021 (ECLI:EU:C:2021:492)

Acórdão do Tribunal de Justiça da União Europeia, Processo C-439/19, Latvijas Republikas Saeima, 22 de junho de 2021 (ECLI:EU:C:2021:504)

Acórdão do Tribunal de Justiça da União Europeia, Processo C-252/21, Meta v. Bundeskartellamt, 04 de julho de 2023 (ECLI:EU:C:2023:537)

Acórdão do Tribunal de Justiça da União Europeia, Processo C-26/22 e C-64/22, SCHUFA Holding AG, 07 de dezembro de 2023 (ECLI:EU:C:2023:958)

CANTO MONIZ, Graça, *Manual de Introdução à Protecção de Dados Pessoais*, Edições Almedina, S.A., 2024

Acórdão do Supremo Tribunal de Justiça, proc. 2335/06.0TMPRT-D.P1.S1, 23 de Fevereiro de 2021

Comissão Nacional de Protecção de Dados, Deliberação n.º 61/2004, relativa ao tratamento de dados pessoais por sistemas de videovigilância, 21 de Janeiro de 2004

Comissão Nacional de Protecção de Dados, Deliberação n.º 1039/2017, relativa à conservação de gravações de chamadas telefónicas para prova da celebração de contratos à distância, 27 de Julho de 2017

Conclusões do Advogado-Geral Maciej Szpunar, Processo C-394/23, *Association Mousse*, 11 de julho de 2024 (ECLI:EU:C:2024:610)

European Data Protection Board, Endorsement 1/2018, 25 de Maio de 2018

European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, 04 May 2020

European Data Protection Board, *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR*, Version 1.0, 08 October 2024

Grupo de Trabalho do artigo 29.º para a Protecção de Dados, *Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na acepção do art. 7.º da Diretiva 95/46/CE*, 09 de abril de 2014

KAMARA, Irene & HERT, Paul de, "Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach", Brussels Privacy Hub Working Paper, Vol. 4, n.º 12, Agosto de 2018

KYI, Lin; SHIVAKUMAR, Sushil Ammanaghatta; ROESNER, Franziska; SANTOS, Cristiana, ZUFALL, Frederike; SCHAUB, Florian; BIEGA, Asia J.; UR, Blase, In proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI'23), April 23-28, 2023

MENEZES CORDEIRO, A., *Direito da Protecção de Dados à luz do RGPD e da Lei n.º 58/2019*, Edições Almedina, S.A., 2022

MENEZES CORDEIRO, A. Barreto, "O tratamento de dados pessoais fundado em interesses legítimos", *Revista de Direito e Tecnologia*, Vol. 1, N.º 1, 2019, pp. 1-31

Watching the watchers: Mass Surveillance in the United States, United Kingdom, and France

Jacob Bourgault

Introduction

"We need a better way to handle our emotional responses to terrorism than by giving our government carte blanche to violate our freedoms, in some desperate attempt to feel safe again. If we don't find one, then, as they say, the terrorists will truly have won."[1]
– Bruce Schneier, American Cryptographer

Dr. Rahinah Ibrahim, a Muslim woman, is a Professor of Architecture at the Putra University of Malaysia.[2] Dr. Ibrahim lived in the United States for thirteen years pursuing higher education.[3] During that time, she received a Bachelor of Arts in Architecture from the University of Washington,[4] a Master of Architecture from the Southern California Institute of Architecture,[5] and was accepted into a Ph.D. program at Stanford University.[6] In early January 2005, during Ibrahim's studies at Standford, she had booked a flight to present her doctoral research.[7] While she was checking in, the airline staff found that she

---

[1] Bruce Schneier, Data and Goliath 228 (2016).

[2] *See* Rahinah Ibrahim, LinkedIn, https://my.linkedin.com/in/rahinah-ibrahim-1b1225b8 (last visited Feb. 17, 2025).

[3] Ibrahim v. U.S. Dep't of Homeland Sec., 912 F.3d 1147, 1154 (9th Cir. 2019) ("Dr. Ibrahim is a Muslim woman, scholar, wife, and mother of four children. She lived in the United States for thirteen years pursuing undergraduate and post-graduate studies.").

[4] *See* Ibrahim, *supra* note 2.

[5] *See id.*

[6] *See id.*

[7] *Ibrahim*, 912 F.3d at 1154 (noting that Dr. Ibrahim had "planned to fly from San Francisco to Hawaii" to "present the results of her doctoral research").

was on a No-Fly List.[8] The authorities were called and Ibrahim was arrested.[9] She was arrested in front of her fourteen year old daughter and in a wheelchair due to a previous operation.[10] She was then held for two hours and received no explanation from authorities for her detainment.[11]

Although Ibrahim was released and later permitted to fly back to Malaysia, she was unable to fly back to the United States when it came time to finish her doctoral degree: she was still on the No-Fly List.[12] Later that year, while still outside the U.S., her student visa was revoked.[13] The letter notifying Ibrahim of this decision cited a provision of the United States Code barring entry for those "reasonably believed to be engaged in or likely to be engaged in terrorist activity, or who has incited terrorist activity."[14] Dr. Ibrahim spent the next *eight years* trapped in a Kafkaesque set of proceedings that lacked clarity or a resolution to the issue.[15] In 2013, after "the government engaged in years of scorched earth litigation,"[16] it was later revealed that Ibrahim landed on the No-Fly List solely because an FBI agent misread a form.[17]

---

[8] *Id.* ("When Dr. Ibrahim arrived at the United Airlines counter, the airline staff discovered her name on the No Fly list and called the police.").

[9] *Id.* ("Dr. Ibrahim was handcuffed and arrested.").

[10] *See, e.g.*, *id.* ("Dr. Ibrahim arrived at SFO with her daughter, Rafeah, then fourteen. At the time, Dr. Ibrahim was still recovering from a hysterectomy performed three months earlier and required wheelchair assistance.").

[11] *Id.* ("[Ibrahim] was escorted to a police car (while handcuffed) and transported to a holding cell by male police officers, where she was searched for weapons and held for approximately two hours.... No one explained to Dr. Ibrahim the reasons for her arrest and detention.").

[12] *Id.* ("The next day [Ibrahim] returned to SFO where an unspecified person told her that she was again–or still–on the No Fly list. She was nonetheless allowed to fly.... [W]hen she arrived at the Kuala Lumpur International Airport, she was not permitted to board the flight to the United States.").

[13] *Id.* ("[O]n April 14, 2005, the U.S. Embassy in Kuala Lumpur wrote to inform Dr. Ibrahim that the Department of State had revoked her F-1 student visa on January 31, 2005....").

[14] *Id.* at 1155.

[15] *See generally id.* (discussing the prolonged immigration litigation against Ibrahim).

[16] *Id.* at 1171.

[17] Id. at 1157 ("Agent Kelley misunderstood the directions on the form and erroneously nominated Dr. Ibrahim to the TSA's No Fly list and DHS's IBIS. He did not intend to do so."); *see also* Maura Dolan, *Appeals Court Rebukes Federal Government in 'No-fly' Case, Ruling It Owes Millions in Legal Fees*, L.A. Times (Jan. 2, 2019), https://www.latimes.com/local/lanow/

All of this–the unjust arrest, eight-year litigation, and accompanying eight-year delay in her education–was due to a single agent misreading a single document. What happened to Dr. Ibrahim was likely driven, at least part, by U.S. law enforcement's mass surveillance of Muslims post-911. This widespread practice was engaged in by entities like the FBI,[18] New York Police Department,[19] and Los Angeles Police Department.[20] Yet, Muslims are not the only victims of mass surveillance in the United States. Nor is the practice of mass surveillance limited to the United States; places like the United Kingdom and France have also gone to great lengths to establish Orwellian surveillance states in the name of national security. The practices that led to Ibrahim's unfair treatment span across demographics, the United States, and the world.

This paper examines these government mass surveillance programs, focusing on the United States, the United Kingdom ("UK"), and France. This analysis includes *de jure* foreign intelligence surveillance practices (e.g., the legal basis for government surveillance in each jurisdiction) and *de facto* foreign intelligence surveillance practices (e.g., the surveillance systems that have actually been enacted, regardless of legality). The analysis reveals that these three countries have historically developed mass surveillance states. Civil unrest, foreign conflict, and public fear have driven the rise of mass surveillance infrastructure. Mass surveillance programs have often been conducted in secret, without appropriate oversight, and tend to be weaponized against minority groups. This analysis showed

---

la-me-ln-no-fly-terrorist-9thcircuit-20190102-story.html ("Ibrahim ended up on the no-fly list in 2004 because an FBI agent misread a form....").

[18] *See generally* Sabrina Alimahomed-Wilson, *When the FBI Knocks: Racialized State Surveillance of Muslims*, 45 Critical Socio. 871 (2019).

[19] *See* Saher Khan & Vignesh Ramachandran, *Post-9/11 Surveillance Has Left a Generation of Muslim Americans in a Shadow of Distrust and Fear*, PBS News (Sept. 16, 2021), https://www.pbs.org/newshour/nation/post-9-11-surveillance-has-left-a-generation-of-muslim-americans-in-a-shadow-of-distrust-and-fear (discussing NYPD and FBI surveillance of Muslims post-9/11).

[20] *See generally* Richard Winton et al., *LAPD Defends Muslim Mapping Effort*, L.A. Times (Nov. 10, 2007), https://www.latimes.com/local/la-me-lapd10nov10-story.html.

that, based on public knowledge, the U.S. has rolled back its mass surveillance efforts. However, mass surveillance in the UK and France is currently expanding. The history of these nation's mass surveillance efforts informs the papers' ultimate recommendations.

Part I defines mass surveillance for the purposes of this paper and the accompanying negative effects. Part II discusses the foreign intelligence surveillance practices of the United States, United Kingdom, and France. This includes a historical and contemporary analysis accompanied by constitutional provisions, legislation, case law, and surveillance infrastructure. Part III compares the historical and contemporary surveillance practices in each jurisdiction. Part IV briefly analyzes the costs and benefits of mass surveillance for foreign intelligence. Part V reconciles these values by making four proposals to maximize the benefits of foreign intelligence surveillance while minimizing the drawbacks. Part V calls for (1) three branch oversight of foreign intelligence surveillance with independent government watchdogs, (2) guaranteed privacy rights in each nation, (3) citizens to stand up for their privacy rights and civil liberties, even in times of fear, and (4) the tailored and safeguarded use of AI in surveillance efforts. The mass surveillance cycle must end and be replaced by targeted surveillance based on individualized suspicion.

People, generally, tend to exaggerate a sense of risk and focus on the worst-case scenario.[21] This susceptibility to fear can lead people to give up their civil liberties for a feeling of temporary security.[22] But this susceptibility to fear, and the accompanying consequences, are misguided. Sacrificing one's civil liberties–in the case of mass surveillance, the privacy rights of millions–leads to an abridgement of those individuals' fundamental needs, gives unfettered discretion and power to the government, and risks the possibility of unjust results, particularly against marginalized groups. While the negative effects of mass

[21] See generally Cass R. Sunstein, Fear and Liberty, 71 Soc. Rsch. 967 (2004).

[22] *See id.* at 967 ("In the midst of external threats, public overreactions are predictable. Simply because of fear, the public and its leaders will favor measures that do little to protect security but that compromise important forms of freedom.").

surveillance are *salient* and *recurring*, they are nonetheless allowed to fester so that *nebulous* national security interests can be protected. Namely, the governments' national security interest in attempting to prevent speculative attacks that may never happen and, even if it were to happen, may not have been caught through mass surveillance.[23] To break this wheel in the early age of Artificial Intelligence ("AI"), which has the possibility to exasperate this surveillance, it is critical to first examine where mass surveillance has been–and where it is headed.

I. DEFINING "MASS SURVEILLANCE" AND NEGATIVE EFFECTS

Although mass surveillance can be defined a number of ways, this paper adopts the definition posed by Amnesty International: "Indiscriminate mass surveillance is the monitoring of internet and phone communications of large numbers of people – sometimes entire countries – without sufficient evidence of wrongdoing."[24] This definition excludes things like the Lantern Laws in the United States (which predated the constitution, and required slaves to carry lit lanterns if unaccompanied by a white person) and recording of information in the national census.[25] This definition was chosen because of its contemporary relevance. Under this definition, things like wiretapping a single individual–or small group of individuals–under investigation for a specific crime is excluded. Instead, this paper focuses on country or demographic wide surveillance practices focused on intercepting

[23] This argument is expanded upon *infra* Part IV.

[24] *Easy Guide to Mass Surveillance*, Amnesty Int'l, https://www.amnesty.org/en/latest/campaigns/2015/03/easy-guide-to-mass-surveillance (last visited Feb. 17, 2025).

[25] *See History of Surveillance Timeline*, Univ. Mich.: Info. & Tech. Servs. [hereinafter *U.S. Surveillance Timeline*], https://safecomputing.umich.edu/protect-privacy/history-of-surveillance-timeline (last visited Feb. 17, 2025) ("Lantern Laws in New York City in the 1700s require Black, mixed-race, and Indigenous enslaved people to carry lit lanterns when in the city after sundown and unaccompanied by a white person.").

foreign intelligence. Several countries, including the three in this analysis, have aimed to surveil broad swaths of their populations.

Dr. Ibrahim's story, and those like it, help to show why the mantra "I have nothing to hide" is an insufficient resolution to surveillance states. Nor is surveillance, in and of itself, harmless. The right to privacy is something that, like other civil liberties, shields citizens from abuses of power and is a fundamental need for individuals.[26] Individuals need community and socialization, but they similarly need to be able to withdraw from others and not have their personal space or correspondence invaded.[27] This need for privacy is found in other non-human animals.[28] Biologist and author Peter Watts notes that "Mammals don't respond well to surveillance. We consider it a threat. It makes us paranoid, and aggressive and vengeful.... The link between surveillance and fear is a lot deeper than the average privacy advocate is willing to admit."[29] Humans have long recognized this need, as "practices designed to protect privacy are found in almost all societies, across time and geographies."[30] The right to privacy is important enough that it is codified in both the United Nations' Universal Declaration of Human Rights[31] and European Convention on Human Rights ("ECHR").[32]

---

[26] *See* Carissa Véliz, *The Ethics of Privacy and Surveillance*, Inst. for Ethics in AI (Jan. 23, 2024), https://www.oxford-aiethics.ox.ac.uk/blog/new-book-ethics-privacy-and-surveillance ("Privacy matters because it shields us from possible abuses of power. Human beings need privacy just as much as they need community.").

[27] *See id.* ("Our need for socialization brings with it risks and burdens which in turn give rise to the need for spaces and time away from others.").

[28] *See id.* (noting that things like "the need to withdraw from others, the ability to deceive, the desire to save face, and the tendency to feel uncomfortable when others stare" are privacy traits found in "human beings and some non-human animals alike").

[29] *Peter Watts on the Harms of Surveillance*, Schneier on Sec. (May 23, 2014), https://www.schneier.com/blog/archives/2014/05/alan_watts_on_t.html.

[30] Véliz, *supra* note 26.

[31] G.A. Res. 217 (III) A, Universal Declaration of Human Rights Art. 12 (Dec. 10, 1948) ("No one shall be subjected to *arbitrary interference with his privacy, family, home or correspondence*, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." (emphasis added)).

[32] European Convention on Human Rights art. 8 ("Everyone has the *right to respect for his private and family life*, his home and his correspondence." (emphasis added)).

Still, some scholars have posed that mass surveillance is harmless. These scholars take the position that if you have nothing to hide, then it does not affect you while simultaneously keeping people safe.[33] However, this argument has three underlying faults: (1) it neglects to consider that privacy violations are inherently harmful to individuals; (2) surveillance often leads to mistakes and perpetuates oppression against marginalized groups, as seen in Dr. Ibrahim's previously delineated story; and (3) mass surveillance has proven ineffective for protecting national security, undermining national interests by diverting resources from more effective programs.[34] Neil Richards, a law professor at Washington University in St. Louis, takes a different tack. Richards argues that surveillance is inherently harmful because it threatens "intellectual privacy."[35]

Richards takes the position "that people should be able to make up their minds at times and places of their own choosing; and that a meaningful guarantee of privacy – protection from surveillance or interference – is necessary to promote this kind of intellectual freedom."[36] He presents a (1) normative and (2) empirical basis for the argument. The normative basis is that civil liberties should protect the right to form beliefs through reading, thinking, and having private conversations.[37] This is undermined when people have to worry about the government snooping on their private correspondence and activities. The empirical basis examines empirical studies and popular media to conclude that

---

[33] *See, e.g.*, Dr. Gabriel Schoenfeld, *In Defense of the American Surveillance State*, 63 Drake L. Rev. 1121, 1134 (2015) ("The measures taken to interdict terrorist communication deserve applause, not condemnation. The American surveillance state is working pretty well.... There has not been a reprise of 9/11.").

[34] For a more detailed discussion of the ineffectiveness of mass surveillance, see *infra* Part IV.

[35] Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934, 1945 (2013) ("The most salient harm of surveillance is that it threatens a value I have elsewhere called 'intellectual privacy.'").

[36] *Id.* at 1496.

[37] Id. ("The normative claim is that the foundation of Anglo-American civil liberties is our commitment to free and unfettered thought and belief – that free citizens should be able to make up their own minds about ideas big and small, political and trivial. This claim requires at a minimum protecting individuals' rights to think and read, as well as the social practice of private consultation with confidantes.").

surveillance undermines "our society's foundational commitments to intellectual diversity and eccentric individuality" by preventing people from engaging in actions or thoughts that are outside the norm.[38] Richards also notes that surveillance in the U.S has led to blackmail (e.g., the FBI admitting to attempting to blackmail Martin Luther King Jr. in an effort to silence his civil rights activism), government persuasion, and discrimination.[39]

Others have also studied empirical data showing the harms of mass surveillance. Daragh Murray et al. recently examined the effects of AI-empowered mass surveillance in Uganda and Zimbabwe.[40] The empirical analysis found that mass surveillance increased self--censorship, led to intimidation-induced chilling effects on speech, and undermined the freedom of assembly.[41] This study found that mass surveillance had tangible negative effects (e.g., fear and distrust among the population) as well as the intangible negative effects (e.g., loss of public discourse and engagement between different groups).[42] Similarly, a poll in the United States found that 88% of those surveyed felt "it is important that they not have someone watch or listen to them without their permission."[43] Further, just 6% felt confident that government agencies could keep their records secure.[44] After the Snowden leaks, the Parliamentary Assembly of the Council of Europe cited a study concluding that 85% of U.S. writers feared government surveillance, leading many to self-censor.[45]

---

[38] *Id.* at 1948.

[39] *Id.* at 1953–58 (discussing "Blackmail," "Persuasion," and "Sorting/Discrimination" as negative effects of mass surveillance).

[40] Daragh Murray et al., *The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe*, 16 J. Hum. Rts. Prac. 397 (July 31, 2023).

[41] *Id.* at 403 –09 (delineating the effect of mass surveillance on the examined communities).

[42] *Id.* (same).

[43] Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Rsch. Ctr. (May 20, 2015), https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance.

[44] *Id.* ("Just 6% of adults say they are 'very confident' that government agencies can keep their records private and secure....").

[45] Eur. Parl. Ass., Comm. On Legal Affs. & Hum. Rts., *Mass Surveillance* at 25 (2015), https://

Based on Western norms regarding civil liberties and empirical data, mass surveillance has proven harmful. Of course, many people are likely to be cognizant of this fact. Privacy, as previously mentioned, is fundamental to humans. However, so is safety and a feeling of comfort. Striking this balance is part of the reason that mass surveillance has been allowed to continue. In 2014, the world's oldest defense think-tank went as far as concluding that "[t]here seems to be a political consensus on the need for surveillance of digital data that is proportionate to the danger faced by UK citizens."[46] However, the think tank did not cite any empirical evidence to support this, instead pointing to two speeches by UK politicians.[47] Still, this balance between national security, privacy rights, and other civil liberties has underpinned every argument for and against mass surveillance throughout history.

II. THE RIGHT TO PRIVACY AND MASS SURVEILLANCE

This section examines the evolution of mass surveillance practices in the U.S., UK, and France. It is worth noting preliminarily that the United States is considerably younger than either the UK or France. Detailing the full evolution of the UK and France's surveillance practices throughout their history would take the balance of the paper to reproduce. For example, the earliest attempt at mass surveillance among these countries may have been William the Conqueror's Domesday Book in 1086.[48] The Domesday Book served as a pseudo-census and is

www.scribd.com/document/253848295/Mass-Surveillance-Report ("85% of the 520 American writers who responded to the survey said they are worried about government surveillance.").

[46] Commentary, *The Politics of Surveillance*, Royal United Servs. Inst. for Def. & Sec. Stud. (Mar. 7, 2014), https://rusi.org/explore-our-research/publications/commentary/politics-surveillance.

[47] *See generally id.*

[48] *See* Dr. Gary Girod, *Mass Surveillance in France & Britain: The Aristocratic Age*, Fr. Hist. Podcast (May 31, 2024), https://www.thefrenchhistorypodcast.com/mass-surveillance-in-france--britain-the-aristocratic-age ("The earliest attempt at widespread intelligence-gathering by the central state as a means of controlling the population in England was the Domesday Book 1086....").

considered the "earliest attempt at widespread intelligence-gathering by the central state as a means of controlling the population in England."[49] Since synthesizing the entire history of each countries surveillance practices is impracticable, this paper focuses on government mass surveillance of foreign intelligence conducted by these three countries since the late 18th century. This coincides with the founding of the United States. It is important to note that discussions on the Five Eyes program, which includes both the U.S. and UK, are saved for the UK section.

Each country's section is divided into three parts: Pre-World War I, World War I to the 21st Century, and the Contemporary Era. As this paper shows, the implementation of mass surveillance and foreign intelligence programs are often the result of domestic unrest or international conflict. Both World Wars and 21st-century terrorism catalyzed the development of mass surveillance infrastructure. It is because of these developments that these three periods were chosen. The first section focuses on the youngest country in this analysis, the United States.

A. United States

Modern understandings of foreign intelligence surveillance in the U.S. are closely tied to the National Security Agency's ("NSA") mass surveillance, the post-911 Patriot Act, and Edward Snowden's leaks. However, in order to understand how this contemporary framework came about, it is important to examine the evolution of U.S. government surveillance practices. Part II.A.1 examines foreign intelligence surveillance from America's founding to WWI. Foreign intelligence played a key role in the Revolutionary War, Civil War, and George Washington's presidency, but lagged behind the practices of the UK and France at the time. Part II.A.2 examines WWI to the 21st century. During that time, several government operations sought to spy on domestic Americans and foreigners. This period also saw the development of increased surveillance capabilities during WWII, as well as a

[49] *Id.*

combination of bills and an executive order that established the framework underpinning modern mass surveillance. Finally, Part II.A.3 examines the contemporary framework.

1. Pre-WWI

While the capabilities accompanying contemporary mass surveillance are relatively recent developments, tracking and monitoring people is not. Indeed, surveillance in its earliest form was enacted through the 1700's New York Lantern Laws, preventing slaves from walking at night unaccompanied unless they had a lantern.[50] Foreign intelligence also played a key role in the Revolutionary War against the British. George Washington developed spy rings to report on British troop movements.[51] The Continental Congress established the Committee of Secret Correspondence in 1775 to gather information from Europeans to help the war effort.[52] During George Washington's presidency, he continued to focus on the importance of intelligence and requested intelligence funding from Congress.[53] By the third year of his presidency intelligence funding accounted for approximately "12% of the Government's budget."[54]

Although federal foreign intelligence surveillance would falter after Washington' presidency, states and private parties occasionally

---

[50] *See, e.g.*, Zain Murdock, *These Lantern Laws Laid The Groundwork For Modern-Day Surveillance And Stop-And-Frisk*, PushBlack (June 28, 2023), https://www.pushblack.us/news/these-lantern-laws-laid-groundwork-modern-day-surveillance-and-stop-and-frisk (noting that the New York law forbade any "Negro or Indian Slave... to be... in any of the streets... without a lanthorn.").

[51] *See The Evolution of the U.S. Intelligence Community-An Historical Overview*, GovInfo, https://www.govinfo.gov/content/pkg/GPO-INTELLIGENCE/html/int022.html (last visited Feb. 27, 2025) ("Washington recruited and ran a number of agents, set up spy rings, devised secret methods of reporting, analyzed the raw intelligence gathered by his agents, and mounted an extensive campaign to deceive the British armies.")

[52] *See id.* ("In November of 1775, the Continental Congress created the Committee of Secret Correspondence to gather foreign intelligence from people in England, Ireland, and elsewhere on the European continent to help in the prosecution of the war.").

[53] *See id.* ("Washington's keen interest in intelligence carried over to his presidency.... Washington asked the Congress for funds to finance intelligence operations.").

[54] *Id.*

formed their own surveillance programs. In 1819, South Carolina enacted legislation requiring all white men over 18 to track and regulate the activity of slaves.[55] One of the first private surveillance practices came from Pinkerton's National Detective Agency ("Pinkerton's"), which still exists today under the name Pinkerton Consulting & Investigations, Inc.[56] In the mid-1800s Pinkerton's conducted surveillance on criminal and labor organizers on behalf of the U.S. government, with Allan Pinkerton becoming the "the first to form an intelligence service for the federal government."[57] Foreign intelligence surveillance would later see a federal revitalization during the Civil War.

During the Civil War, from 1861-1865, the Union intercepted telegraphs and mail from the Confederacy.[58] Both sides established intelligence surveillance systems, as well as spy networks.[59] The Union's surveillance efforts allowed them to track Confederate troop movements and decode confederate message over telegraph.[60] These surveillance efforts greatly assisted the Union in winning the war.[61] Approximately 20 years later, in the 1880s, the Office of Naval Intelligence and the Military Intelligence Division were formed to monitor foreign and domestic military intelligence.[62] From the 1880s until WWI, U.S.

---

[55] *U.S. Surveillance Timeline*, *supra* note 25 (noting that in 1819 "[t]he South Carolina General Assembly enact[ed] a law requiring all white men over the age of 18 to participate in slave patrols").

[56] *See generally Our History*, Pinkerton Consulting & Investigations, Inc., https://pinkerton.com/our-story/history.

[57] Alan Bilansky, *Pinkerton's National Detective Agency and the Information Work of the Nineteenth-Century Surveillance State*, 53 Info. & Culture 67, 79 (2018).

[58] *See, e.g.*, *19th Century – The Origins of Surveillance*, Stan. Univ., https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/history_19century.html (last visited Feb. 17, 2025) ("Wiretapping was perhaps the earliest form of surveillance and began during the Civil War when both the Union and the Confederacy tapped into each other's telegraph lines and copied down the messages.").

[59] *See* GovInfo, *supra* note 51 ("Both the Union and Confederate leadership valued intelligence information, established their own spy networks, and often railed at the press for providing intelligence to the other side.").

[60] *See id.* (noting that Union surveillance efforts led to successfully "detecting a large concentration of Confederate troops preparing to attack at Fair Oaks, Virginia").

[61] *See generally id.*

[62] *See id.* (noting that the Office of Naval Intelligence was created in March 1882, and the Military Intelligence Division was created three years later).

surveillance activities were primarily focused on domestic intelligence.[63] This included the Justice Department's Bureau of Investigation, the predecessor to the Federal Bureau of Investigations ("FBI"), being formed in 1908 due to concerns that the federal government was spying on members of Congress.[64]

However, prior to the breakout of WWI, the United States lacked comprehensive and coordinated intelligence efforts.[65] This was likely in part due to President Woodrow Wilson's (1913-1921) disdain for spies and surveillance, instead preferring open diplomacy.[66] However, British intelligence services would contribute to the U.S. entering the war and, eventually, the development of U.S. intelligence infrastructure. The British intercepted German intelligence revealing that the Germans were attempting to prevent the U.S. from contributing finance or goods to the British war effort.[67] A catalyst for the U.S. entering WWI was the British interception of the "Zimmerman Telegram," which promised Mexico land from the U.S. if they joined the Germans.[68] This "wake-up" call for President Wilson led the U.S. into WWI and, as an accompanying result, the development of increased U.S. surveillance infrastructure.

---

[63] *See id.* ("For the most part, however, the early part of the twentieth century was marked not by an expanded use of intelligence for foreign policy purposes, but by an expansion of domestic intelligence capabilities.").

[64] *See id.* ("The Justice Department's Bureau of Investigation (the forerunner of the FBI) was established in 1908 out of concern that Secret Service agents were spying on members of Congress.").

[65] *See id.* ("At the time the United States entered [World War I], it lacked a coordinated intelligence effort.").

[66] *See id.* ("As a champion of open diplomacy, President Woodrow Wilson had disdained the use of spies and was generally suspicious of intelligence.").

[67] *See id.* ("British intelligence played a major role in bringing the United States into World War I. Public revelations of German intelligence attempts to prevent U.S. industry and the financial sector from assisting Great Britain greatly angered the American public.").

[68] *The Zimmermann Telegram*, Nat'l Archives (June 2, 2021), https://www.archives.gov/education/lessons/zimmermann ("In January 1917, British cryptographers deciphered a telegram from German Foreign Minister Arthur Zimmermann to the German Minister to Mexico, Heinrich von Eckhardt, offering United States territory to Mexico in return for joining the German cause. This message helped draw the United States into the war and thus changed the course of history.").

2. WWI to 21st Century

WWI led to the formation of MI-8 in 1917. MI-8 was mandated to decode military communications and ensure the security of the army's correspondence.[69] This data was transferred to the state department and would later becoming known as the "Black Chamber."[70] The Black Chamber monitored intelligence even after the war ended, including from Japanese officials in the early 1920's.[71] MI-8 and the Black Chambers surveillance efforts would be derailed by President Herbert Hoover (1929-1933), who shared President Wilson's distaste for snooping on private correspondence.

Domestically, wiretapping was the primary surveillance mechanism, but would not be widely used by U.S. law enforcement until Prohibition in the 1920s-30s.[72] Even still, the NYPD had a national scandal in 1916 when they were caught wiretapping "hundreds of phones a year to track criminals and suppress labor activism."[73] These developments did not lead to any major policy changes and the 1928 Supreme Court, in a narrow 5-4 vote, held that wiretapping without a warrant was not a constitutional violation.[74] Further, The Espionage Act of 1917 and Palmer Raids accompanying the Red Scare both led to government monitoring of private actors based on potential political affiliations.[75] The former targeted disloyalty in the First World War, and

---

[69] *See* GovInfo, *supra* note 51 ("In June of 1917, the first U.S. signals intelligence agency was formed within the Army. Known as 'MI-8,' the agency was charged with decoding military communications and providing codes for use by the U.S. military.").

[70] *See id.*

[71] *See id.* ("In 1921, the Black Chamber celebrated perhaps its most significant success by decrypting certain Japanese diplomatic traffic.").

[72] *See* April White, *A Brief History of Surveillance in America*, Smithsonian Mag. (Apr. 2018), https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399 ("Until the 1920s, wiretapping was most often used by private detectives and corporations. It wasn't until Prohibition that it became a common law enforcement tool.").

[73] *U.S. Surveillance Timeline*, *supra* note 25.

[74] Olmstead v. United States, 277 U.S. 438 (1928).

[75] *U.S. Surveillance Timeline*, *supra* note 25 ("Following World War I and the Russian Revolution of 1917, the first Red Scare period in the United States was marked by fear of leftist movements and influence. The U.S. Department of Justice conducted raids led by Attorney General A. Mitchell Palmer, known as Palmer Raids in an attempt to arrest foreign anarchists, commu-

the latter targeted potential communist sympathizers (surveillance that would be reprised during the Cold War).[76] In the late years of WWI, Congress enacted the Sedition Act of 1918, which made it a crime to "willfully utter, print, write, or publish any disloyal, profane, scurrilous, or abusive language about the form of Government of the United States."[77] Interestingly, by the 1960s U.S. citizens supported wiretapping for national security purposes, but opposed its use in criminal matters (a perspective that has now largely flipped).[78]

It was during World War II that the U.S. began to enact much of its mass surveillance, generally focusing on communist sympathizers. In 1938, the House Un-American Activities Committee ("HUAC") was created to investigate and track communist sympathizers.[79] In 1945 the United States began Project SHAMROCK out of the ashes of, and largely because of, WWII.[80] Project SHAMROCK monitored domestic radio and wire communications with foreign entities, collecting "approximately 150,000 messages per month" at its peak.[81] This program lasted

---

nists, and radical leftists.").

[76] History.com Editors, *Red Scare*, History (Apr. 21, 2023), https://www.history.com/topics/cold-war/red-scare#cold-war-concerns-about-communism (delineating the first Red Scare (1917--1920) and subsequent Red Scare during the Cold War).

[77] *The Sedition Act of 1918*, Digit. Hist. (2021), https://www.digitalhistory.uh.edu/disp_textbook.cfm?smtID=3&psid=3903.

[78] White, *supra* note 72 ("By 1965, the normative political position in the United States was that wiretapping for national security was a necessary evil, whereas wiretapping in the service of the enforcement of criminal law–in, say, tax evasion cases or even in Mafia prosecutions, which was a big priority among American law enforcement starting in the 1960s–was outrageous and an abuse of power. Today, it's the opposite. Most people are worried about wiretapping by the government.").

[79] *See House Un-American Activities Committee*, Harry S. Truman Libr., https://www.trumanlibrary.gov/education/presidential-inquiries/house-un-american-activities-committee (last visited Feb. 17, 2025) ("HUAC was created in 1938 to investigate alleged disloyalty and rebel activities on the part of private citizens, public employees and organizations suspected of having Communist ties.").

[80] Major Dave Owen, A Review of Intelligence Oversight Failure: NSA Programs that Affected Americans 33 (2012), https://irp.fas.org/agency/army/mipb/2012_04-owen.pdf ("Project SHAMROCK began in August 1945, shortly before the end of World War II and over seven years prior to the establishment of the NSA.").

[81] *Id.* at 34; *see also U.S. Surveillance Timeline*, *supra* note 25 ("Operation SHAMROCK was tasked with monitoring radio and wire communications targeting agents of foreign governments or agents of foreign commercial enterprises.").

until the 1970s,[82] and is an early example of the U.S. government conducting a large-scale collection and analyzation of American citizens private correspondence.[83]

The 1947 National Security Act led to the development of the National Security Council ("NSC") and Central Intelligence Agency ("CIA").[84] Just five years later, and what is now a household name after Edward Snowden's leaks, the National Security Agency ("NSA") was formed as an agency largely unknown to the public.[85] Contemporaneously, the FBI began its Counterintelligence Program ("COINTELPRO") which "expanded its domestic surveillance programs" and tracked communists, socialists, and black civil rights groups.[86] The NSA's first major mass surveillance program came around this time and was called Project MINARET.[87] Integrating data from Project SHAMROCK, Project MINARET cataloged the actions of American citizens and put certain people on a "watch list."[88] This list targeted "individuals and

---

[82] *See, e.g.*, Owen, *supra* note 80, at 34 ("The Director of the NSA terminated Project SHAMROCK in 1975....")

[83] *Cf.* ("Though Project SHAMROCK undoubtedly collected and analyzed American citizens' private communications on a large scale, this effort still focused on foreign intelligence.").

[84] *National Security Act of 1947*, U.S. Dep't State: Off. Hist., https://history.state.gov/milestones/

1945-1952/national-security-act (noting that the National Security Act of 1947 created both the NSC and CIA).

[85] *See, e.g.*, Owen, *supra* note 80, at 33 ("President Truman created NSA in 1952.... [S]ince both the memorandum and directive which led to its creation were classified, the NSA was generally unknown to the public.").

[86] JK Davis, *Spying on America: The FBI's Domestic Counter-Intelligence Program*, U.S. Dep't Just., https://www.ojp.gov/ncjrs/virtual-library/abstracts/spying-america-fbis-domestic--counter-intelligence-program (last visited Feb. 17, 2025) ("COINTELPRO was aimed at five major social and political protest groups: The Communist party, the Socialist Workers party, the Ku Klux Klan, black nationalist hate groups, and the New Left movement. Under COINTELPRO policies, the FBI expanded its domestic surveillance programs and increasingly used questionable, even unlawful, methods in an effort to disrupt virtually the entire social and political protest process.").

[87] *See, e.g.*, Owen, *supra* note 80, at 34–35 (discussing the origins and transformation of Project MINARET).

[88] *See id.* ("Project MINARET was essentially the NSA's watch list. It used existing SIGINT accesses (to include information from Project SHAMROCK), and searched for terms, names, and references associated with certain American citizens.... [S]tarting in 1967, the NSA started

organizations active in the antiwar and civil rights movements."[89] Alongside the NSA and FBI, the CIA also had their own surveillance program. The CIA's Operation CHAOS maintained a computer index of over 300,000 people and organizations, the majority of them U.S. citizens.[90]

Project SHAMROCK, Project MINARET, Operation CHAOS, and COINTELPRO all ended in the early- to mid-1970s. By this point, these programs were likely illegal under U.S. law. In 1967, the U.S. Supreme Court decided both *Berger v. New York* and *Katz v. United States*.[91] Both cases found that wiretapping without a warrant was unconstitutional, with the *Katz* ruling providing for a "reasonable expectation of privacy" in correspondence that cannot be violated without adhering the necessary procedural safeguards (i.e., a warrant and individualized suspicion).[92] *Katz* remains good law, and under *Katz* the NSA's mass surveillance is likely unconstitutional. But it was not these cases that necessarily led to the downfall of Project SHAMROCK, Project MINARET, Operation CHAOS, and COINTELPRO.

Instead, a flurry of different events contributed to the demise of these programs: (1) a 1971 FBI break-in leaked the details of COINTELPRO; (2) the Watergate Scandal led to increased government scrutiny; (3) the Supreme Court decided *United States v. United States District Court* (*Keith Case*); and (4) the U.S. Senate's Church Committee began investigating the surveillance practices of the FBI, CIA, NSA,

---

adding selectors associated with American citizens to the watch list, establishing a 'civil disturbance' watch list.").

[89] *See id.*

[90] New York Times Archive, *'Operation Chaos'...*, N.Y. Times (June 11, 1975), https://www.nytimes.com/1975/06/11/archives/operation-chaos.html (noting that the Operation CHAOS had a computer database "containing an index of over 300,000 names and organizations, almost all of them of United States citizens and organizations unconnected with espionage").

[91] These cases overruled the previously mentioned *Olmstead* case. Berger v. New York, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967).

[92] It is worth noting that the "reasonable expectation of privacy" test came from Judge Harlan's concurrence, not the main opinion, and therefore was not binding. However, it has since become the applicable and universally accepted standard. *Katz*, 389 U.S. at 360–62 (Harlan, J., concurring).

and Internal Revenue Services ("IRS"). The 1971 leak triggered the Church Committee investigation,[93] and the *Keith Case* held that a warrant is required for domestic surveillance.[94] However, the *Keith* court left open whether foreign intelligence surveillance requires a warrant.[95] The nail in the coffin was the Church Committees final report. The report found that these surveillance practices (specifically naming SHAMROCK, COINTELPRO, and MINARET) were civil rights abuses that had "undermined the constitutional rights of citizens."[96] This all contributed to the passing of the Foreign Intelligence Surveillance Act ("FISA") in 1978.

If FISA is considered a win for privacy rights, it was only in form, not in substance. Although FISA was posited as increasing oversight of foreign intelligence surveillance in the U.S.,[97] it had little effect on the permissible bounds of mass surveillance. FISA created the Foreign Intelligence Surveillance Court ("FISC") and requires the Department of Justice ("DOJ") to obtain a warrant from FISC before conducting

---

[93] Tom Jackman, *The FBI Break-in That Exposed J. Edgar Hoover's Misdeeds to Be Honored With Historical Marker*, Wash. Post (Sept. 1, 2021), https://www.washingtonpost.com/history/2021/09/01/fbi-burglary-hoover-cointelpro ("The revelations about COINTELPRO, a program begun by Hoover in 1956, led to congressional hearings by the Church Committee....").

[94] United States v. U.S. District Court, 407 U.S. 297, 323–24 (*Keith Case*) (1972) ("We do hold, however, that prior judicial approval is required for the type of domestic security surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.").

[95] *Id.* at 308 ("[T]he instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country.").

[96] *Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, U.S. Senate, https://www.senate.gov/about/powers-procedures/investigations/church-committee.htm (last visited Feb. 17, 2025).

[97] *The Foreign Intelligence Surveillance Act of 1978 (FISA)*, U.S. Dep't of Just. [hereinafter *DOJ FISA*], https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286 (last visited Feb. 17, 2025) ("Congress sought to provide judicial and congressional oversight of foreign intelligence surveillance activities while maintaining the secrecy necessary to effectively monitor national security threats."); *see also U.S. Surveillance Timeline*, *supra* note 25 ("The Foreign Intelligence Surveillance Act (FISA) sought to provide judicial and congressional oversight of foreign intelligence surveillance activities in response to the exposure of abuses of U.S. persons' privacy rights by certain components of the United States government.").

foreign intelligence surveillance.[98] FISC is a specialized court in Washington, D.C. that reviews warrant application for foreign intelligence.[99] FISC judges are picked from existing District Court Judges by the U.S. Supreme Court Chief Justice for a temporary and part time assignment.[100] In theory, this provided three branch oversight of foreign intelligence surveillance–the DOJ (executive) must request a warrant from FISC (judiciary) through the parameters set by FISA (legislature).

However, in practice, this was not the case. FISC rejected only 11 out of 34,000 warrant requests from 1979 to 2013.[101] This indicates the warrant process was more of a rubber stamp than a meaningful review. During this time the review process had a lower burden than traditional warrants, its rulings were secret (providing no congressional oversight), and adverse parties were not permitted to present evidence in it.[102] Only in 2022 did the government release a set of classified rulings from FISC, with much of it redacted.[103] Further, FISC has been criticized for serving as a rule-maker instead of its intended role as gatekeeper.[104]

---

[98] *DOJ FISA*, *supra* note 97 ("Subchapter I of FISA established procedures for the conduct of foreign intelligence surveillance and created the Foreign Intelligence Surveillance Court (FISC). The Department of Justice must apply to the FISC to obtain a warrant authorizing electronic surveillance of foreign agents.").

[99] *See generally About the Foreign Intelligence Surveillance Court*, U.S. Foreign Intel. Surveillance Ct., https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court (last visited Feb. 27, 2025).

[100] *Id.* ("The FISC is composed of 11 experienced federal district judges who are designated by the Chief Justice of the United States for this part-time assignment.").

[101] Schneier, *supra* note 1, at 175 (noting that FISC "rejected a mere 11 out of 34,000 warrant requests between its formation in 1979 and 2013").

[102] *See id.* at 177 ("[T]he FISA Court has a much lower standard of evidence before it issues a warrant. Its cases are secret, its rulings are secret, and no one from the other side ever presents in front of it.").

[103] *See* Matthew Guariglia & Aaron Mackey, *Victory: Government Finally Releases Secretive Court Rulings Sought By EFF*, Elec. Frontier Found. (Aug. 22, 2022), https://www.eff.org/deeplinks/2022/08/victory-government-finally-releases-secretive-court-rulings-sought-eff ("[T]he government released seven heavily-redacted but previously classified rulings from the Foreign Intelligence Surveillance Court that shed new light on how the secret court interprets key provisions of the laws that authorize mass surveillance.").

[104] *See generally* Emily Berman, *The Two Faces of the Foreign Intelligence Surveillance Court*, 91 Ind. L.J. 1191 (2016).

Essentially, while FISC *should* ensure that the government has met the necessary warrant requirements (i.e. gatekeeper), the court has instead been asked to determine whether mass surveillance is in line with existing law (i.e. rule-maker), all while operating in secret.[105]

Further, even with FISA's rubber-stamping warrant process, the court was often entirely bypassed. For example, in 2012 US Cellular received two wiretap orders approved by the judiciary.[106] That same year, the company received 10,801 subpoenas without appropriate judicial oversight.[107] Sometimes the NSA went further still, as seen in Snowden's leaks, by hacking directly into corporate infrastructure.[108] FISA failed to add meaningful safeguards against government mass surveillance, and FISA has even been weaponized against domestic citizens (even though FISA provided no justification for monitoring domestic information).[109] Further, FISA was amended in 2008 to add Section 702, which authorizes the warrantless collection of "foreign intelligence information."[110] This dismantled some of the very little protections that FISA afforded and allowed domestic citizens to be spied on if they have

---

[105] *See id.* at 1192 –93 (arguing that the FISC has become a "rule maker" post-911 as opposed to its original charge of "gatekeeper").

[106] *See* Schneier, *supra* note 1, at 177 ("US Cellular received only two judicially approved wiretap orders in 2012....").

[107] *See id.* (noting that in 2012 US Cellular additionally received "another 10,801 subpoenas for the same types of information without any judicial oversight whatsoever").

[108] *See, e.g.*, *id.* at 85 ("[N]ot satisfied with the amount of data it receives from Google and Yahoo via PRISM, the NSA hacked into the trunk connections between both companies' data centers....").

[109] *See* Berman, *supra* note 104, at 1198 ("The FISA Court has authorized at least three bulk--collection programs since 9/11, some more controversial than others. The most controversial is the bulk collection of all domestic telephony metadata....").

[110] *See Warrantless Surveillance Under Section 702 of FISA*, Am. C.L. Union, https://www.aclu.org/warrantless-surveillance-under-section-702-of-fisa (last visited Feb. 27, 2025) ("Under Section 702 of the Foreign Intelligence Surveillance Act (FISA), the U.S. government engages in mass, warrantless surveillance of Americans' and foreigners' phone calls, text messages, emails, and other electronic communications."); Noah Chauvin, *Why Congress Must Reform FISA Section 702–and How It Can*, Brennan Ctr. for Just. (Apr. 9, 2024), https://www.brennancenter.org/our-work/analysis-opinion/why-congress-must-reform-fisa-section-702-and-how--it-can ("Enacted shortly after 9/11, Section 702 allows intelligence agencies to collect the phone calls, emails, text messages, and other communications of almost any non-American located outside of the United States without a warrant.").

interactions with anyone outside of America, a practice that increased significantly in the wake of 9/11.

Returning to the chronology of U.S. mass surveillance, in 1981 President Reagan signed Executive Order 12333, which gave the government a legal basis (notwithstanding nor acknowledging *Katz*, *Berger*, or *Keith*) for this surveillance.[111] The NSA still relies on this executive order while conducting surveillance activities for foreign intelligence.[112] The executive order ambiguously permits the collection of "[i]nformation constituting foreign intelligence or counterintelligence."[113] A glimmer of hope again came from the United States Supreme Court in the 2001 *Kyllo v. United States* case.[114] In *Kyllo*, the court held that using thermal imaging to see inside someone's home without a warrant is a violation of *Katz*'s reasonable expectation of privacy and, hence, the Fourth Amendment.[115] Although it did not address foreign intelligence surveillance, it appeared to be another win for privacy rights. However, later that year, privacy rights would be all but eviscerated in the wake of 9/11.

3. Contemporary Era

Six weeks after terrorists flew three planes into the World Trade Center and Pentagon, President Bush signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("Patriot Act").[116] This bill was pushed to the Senate floor for a vote with "no discussion, debate, or hearings."[117] Many senators did not even have a chance to

---

[111] *Executive Order 12333*, Nat'l Sec. Agency, https://www.nsa.gov/Signals-Intelligence/EO-12333 (last visited Feb. 27, 2025) ("Executive Order (EO) 12333 is the foundational authority by which NSA collects, retains, analyzes, and disseminates foreign signals intelligence information.").

[112] *See id.*

[113] Exec. Order No. 12,333, 46 F.R. 59941 (1981).

[114] Kyllo v. United States, 533 U.S. 27 (2001).

[115] *Id.*

[116] Pub. L. No. 107-56, 115 Stat. 272 (2001).

[117] *Surveillance Under the USA/PATRIOT Act*, Am. C.L. Union (Oct. 23, 2001), https://www.aclu.org/documents/surveillance-under-usapatriot-act.

read it.[118] In the House, there was a debate, and from those debates the Judiciary Committee put forth a watered down version of the bill.[119] This compromise bill was tossed by House leadership and a bill mirroring the Senate version was moved to floor, both without debate, and the Bush administration sent a clear message: if you vote this down, the next attack will be your fault.[120]

Most relevant to mass surveillance, Section 215 of the Patriot Act permitted the FBI to force anyone (i.e. everyone) to turn over information nebulously related to "clandestine intelligence activities."[121] It was under Section 215 that tens of millions of ordinary Americans had their communications secretly recorded by the government since 2001.[122] Often, the U.S. government worked in willing cooperation with cell phone companies like AT&T.[123] In fact, "AT&T shared billions of emails and phone records from its domestic networks" with the NSA.[124] So did other companies like Verizon.[125] Overall, there was effectively nothing stopping the NSA in their surveillance. Many companies holding

---

[118] *See id.* ("Many Senators complained that they had little chance to read it, much less analyze it, before having to vote.").

[119] *See id.* ("In the House, hearings were held, and a carefully constructed compromise bill emerged from the Judiciary Committee.").

[120] *See id.* ("But then, with no debate or consultation with rank-and-file members, the House leadership threw out the compromise bill and replaced it with legislation that mirrored the Senate version.... The Bush Administration implied that members who voted against it would be blamed for any further attacks....").

[121] 50 U.S.C. § 1801(e)(1)(C).

[122] *See, e.g.*, *NSA Spying*, Elec. Frontier Found., https://www.eff.org/nsa-spying (last visited Feb. 27, 2025) ("The US government, with assistance from major telecommunications carriers including AT&T, has engaged in massive, illegal dragnet surveillance of the domestic communications and communications records of millions of ordinary Americans since at least 2001.").

[123] *See id.*

[124] Daniel Costa-Roberts, *AT&T Cooperated Extensively With NSA, Snowden Documents Reveal*, PBS News (Aug. 15, 2015), https://www.pbs.org/newshour/politics/report-att-cooperated-extensively-nsa-sharing-billions-phone-email-records.

[125] *See* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA Today (Sept. 15, 2022), https://eu.usatoday.com/story/money/2022/09/13/nsa-secretly-collecting--americans-phone-call-records/7940563001 ("The National Security Agency has been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon and BellSouth....").

private citizen data willingly gave it over to the NSA. If not, the NSA would get a rubber stamp warrant from FISC (recall that only 0.03% of warrant applications were denied by FISC).[126] Occasionally this oversight was sidestepped entirely by the government hacking into corporate databases.[127] The Patriot Act had a sundown provision, but many of the bills salient provisions were permanently codified in 2005.[128]

Of course, it is likely that this surveillance went well beyond the scope of the bill. Many were shocked in 2013 when Edward Snowden, an NSA intelligence contractor, revealed the extent of this surveillance.[129] Even the author of the Patriot Act was disturbed to learn that it led to mass surveillance, contending that the bill never intended mass surveillance.[130] Among the most startling revelations were derived from the NSA's Prism and XKeyscore programs. The NSA's Prism program provided backdoor access to companies like "Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple," processing and storing vast amounts of information.[131] This allowed the NSA to log every correspondence and access those logs without a warrant.[132] Since much of the world uses American internet companies for their correspondence, Prism included vast amounts of international and domestic information.[133] It is still unclear which companies willingly complied,

---

[126] *See supra* note 101 and accompanying text.

[127] *See supra* note 108 and accompanying text.

[128] USA PATRIOT Act Improvement and Reauthorization Act, Pub. L. No. 109-177, 120 Stat. 192 (2005).

[129] *See, e.g.*, Network of Eur. Union, The NSA Leaks and Transatlantic Relations (2014) (discussing European reactions to the leaks).

[130] See *End Mass Surveillance Under the Patriot Act*, Am. C.L. Union, https://www.aclu.org/end-mass-surveillance-under-the-patriot-act (last visited Feb. 27, 2025) ("The author of the [PATRIOT Act] has publicly stated that it was never intended to facilitate mass, suspicionless surveillance.").

[131] Zoe Kleinman, *What Does Prism Tell Us About Privacy Protection?*, BBC News (June 10, 2013), https://www.bbc.com/news/technology-22839609.

[132] *See* Samuel Chapman, *Edward Snowden & the NSA PRISM Program*, Priv. J. (Nov. 21, 2024), https://www.privacyjournal.net/edward-snowden-nsa-prism ('Through the PRISM program, the NSA and other agencies can 'obtain targeted communications without having to request them from the service providers and without having to obtain individual court orders.'").

[133] *See, e.g.*, *id.* ("Because much of the world uses communication channels run by American internet firms, PRISM's back door gives U.S. intelligence direct access to a global data stream.").

which were forced to comply by court order, and which were hacked directly by the government.[134] Yahoo, for example, was threatened with a $250,000 per-day fine if they denied the NSA access.[135]

XKeyscore is potentially more intrusive than Prism. NSA described XKeyscore as its "widest reaching" data gathering mechanism.[136] XKeyscore allows for NSA agents to monitor web traffic–specifically "at least 41 billion total records" in a 30 day period–with the data being compiled to let analysts "search by name, telephone number, IP address, keywords, the language in which the Internet activity was conducted or the type of browser used."[137] However, this data is only kept for a short period of time.[138]

Even prior to these mass surveillance revelations, there were legal challenges to the statutory basis underpinning U.S. mass surveillance. A collection of people that engaged in sensitive correspondence filed a lawsuit against James Clapper, the Director of National Intelligence. Although the Supreme Court finally had the chance to declare this surveillance unconstitutional in *Clapper v. Amnesty International*, they failed to do so.[139] Instead of reaching the merits of the case, the court tossed the case due to a lack of standing, finding that the plaintiffs (which included groups that conduct sensitive and privileged correspondence such as "attorneys and human rights, labor, legal, and media

---

[134] *See id.* (noting that some telecommunications companies willingly complied, others were threatened, and the "MUSCULAR" program was focused purely on hacking directly into telecommunication infrastructure).

[135] *See, e.g.*, Kim Zetter, *Feds Threatened to Fine Yahoo $250K Daily for Not Complying With PRISM*, Wired (Sept. 11, 2014), https://www.wired.com/2014/09/feds-yahoo-fine-prism ("[T]he Feds threatened [Yahoo] the internet giant with a massive $250,000 a day fine if it didn't comply and a court ruled that Yahoo's arguments for resisting had no merit.").

[136] *See* Yannick LeJacq, *How the NSA's XKeyscore Program Works*, NBC News (Aug. 1, 2013), https://www.nbcnews.com/technolog/how-nsas-xkeyscore-program-works-6c10812168 (noting that NSA described XKeyscore as its "'widest reaching' means of gathering data from across the Internet.").

[137] *See id.*

[138] *See id.* ("Content remains on the system for only three to five days....").

[139] Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).

organizations")[140] did not suffer any harm.[141] The standing doctrine in the United States requires that plaintiffs have: (1) an injury in fact that is (a) concrete and particularized and (b) actual or imminent; (2) a causal connection between the injury and the conduct before the court; and (3) likeliness of redressability if the court grants a favorable decision.[142] The plaintiffs in *Clapper* failed on the first prong, being unable to show they suffered an injury in fact.[143] This doctrine is convoluted and contested at best, while potentially allowing the Supreme Court to dodge meaningful questions at the worst.

Things did not go according to plan for Snowden personally. When it became public that he was the source of the leaks, he was charged with theft and violations of the 1917 Espionage Act.[144] In route to Ecuador for asylum, he landed in Moscow, where his passport was canceled.[145] He spent forty days in the Moscow airport seeking asylum but was refused at every turn.[146] Snowden eventually decided to stay in Russia, where he remains today after getting married and having two sons.[147]

On a broader level, however, there have been some minor improvements since *Amnesty International.* Two of the most important

---

[140] *Id.* at 406.

[141] *See generally id.*

[142] *See generally Standing*, Legal Info. Inst., https://www.law.cornell.edu/wex/standing (last visited Feb. 27, 2025).

[143] *Clapper*, 568 U.S. at 410 ("[R]espondents' theory of standing, which relies on a highly attenuated chain of possibilities, does not satisfy the requirement that threatened injury must be certainly impending.").

[144] *See Edward Snowden: A Timeline*, NBC News (May 26, 2014), https://www.nbcnews.com/feature/edward-snowden-interview/edward-snowden-timeline-n114871 (noting that Snowden was charged with two counts of violating the 1917 Espionage Act).

[145] *See* Dave Davies, *Edward Snowden Speaks Out: 'I Haven't And I Won't' Cooperate With Russia*, Nat'l Pub. Radio (Sept. 19, 2019), https://www.npr.org/2019/09/19/761918152/exiled--nsa-contractor-edward-snowden-i-haven-t-and-i-won-t-cooperate-with-russia (discussing the cancelation of Snowden's passport in Russia).

[146] *See id.* ("Snowden spent 40 days in the Moscow airport, trying to negotiate asylum in various countries.").

[147] *See* Greg Myre, *A Decade on, Edward Snowden Remains in Russia, Though U.S. Laws Have Changed*, Nat'l Pub. Radio (June 4, 2023), https://www.npr.org/2023/06/04/1176747650/a-decade-on-edward-snowden-remains-in-russia-though-u-s-laws-have-changed (discussing Snowden's life in Russia as of 2023).

developments came in 2015. First, the Second Circuit (a federal court just beneath the Supreme Court) ruled in *ACLU v. Clapper* that the NSA's bulk collection of data went beyond the scope of Section 215 of the Patriot Act.[148] Second, the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act ("USA Freedom Act") was subsequently signed into law by President Obama.[149] Legislators touted that the USA Freedom Act prohibited the "bulk collection of ALL records under Section 215 of the PATRIOT Act, the FISA pen register authority, and national security letter statutes."[150] It also mandated the disclosure of certain opinions by FISC and imposed new reporting requirements for government surveillance activities.[151] However, it also made *ACLU* moot before it could reach the Supreme Court.[152]

While mass surveillance has purportedly been rolled back (by the same government that secretly did it in the first place), the fight is far from over. It is unclear if there has been meaningful change at the federal level. In 2017, the NSA stated that it had 40 surveillance targets but collected over 543 million call records.[153] Section 702 of the FISA program was recently extended past its deadline with bipartisan support.[154] It also expanded the definition of "Electronic Communications Service

---

[148] Am. C.L. Union v. Clapper, 785 F.3d 787 (2nd Cir. 2015).

[149] Pub. L. No. 114-23, 129 Stat. 268 (2015).

[150] *USA Freedom Act*, House Judiciary Comm., https://judiciary.house.gov/usa-freedom-act (last visited Feb. 27, 2025).

[151] *See generally id.*

[152] *Cf.* Clapper, 785 F.3d at 826 ("[T]he statutory issues on which we rest our decision could become moot....").

[153] *See ACLU v. ODNI – FOIA Lawsuit Seeking Records About Government Surveillance Under the USA Freedom Act*, Am. C.L. Union (Sept. 14, 2023), https://www.aclu.org/cases/aclu-v-odni-foia-lawsuit-seeking-records-about-government-surveillance-under-usa-freedom-act ("[I]n 2017, the NSA asserted it had 40 surveillance targets–and collected more than 534 million call records.").

[154] *See* The Associated Press, *Biden Signs Reauthorization of Surveillance Program Into Law Despite Privacy Concerns*, Nat'l Pub. Radio (Apr. 20, 2024), https://www.npr.org/2024/04/20/1246076114/senate-passes-reauthorization-surveillance-program-fisa ("[T]he Senate had approved the bill by a 60-34 vote hours earlier with bipartisan support, extending for two years the program known as Section 702 of the Foreign Intelligence Surveillance Act.").

Provider," to include "anyone who oversees the storage or transmission of electronic communications" such as emails, texts, or other online data, and requires them to "cooperate with the federal government's requests to hand over data."[155] Under Section 702 and Executive Order 12333, it is possible that little has changed regarding the NSA's surveillance practices today.[156]

If meaningful change is going to happen in the U.S., its best chance is derived from public sentiment. Democratically elected legislators are subject to the desires of their voters. Americans need to demand more transparency in government surveillance practices and an end to mass surveillance. The Supreme Court is unlikely to step in. In theory, a future mass surveillance challenge like *Amnesty International* could survive a standing challenge if the courts take the position that privacy violations are inherently harmful and injurious.[157] However, this is a long shot. Further, even if mass surveillance plaintiffs are given standing, U.S. courts often refuse to hear cases presenting political question, which mass surveillance and national security would likely fall under.[158] Better whistleblower protections–sufficient to encourage and protect those like Snowden–would be a great start alongside the recommendations in Part V.

B. United Kingdom

Snowden's leaks exposed considerable information about mass surveillance in the UK. In contrast to the United States, the United

---

[155] *See* Matthew Guariglia, *NSA Surveillance and Section 702 of FISA: 2024 in Review*, Elec. Frontier Found. (Dec. 28, 2024), https://www.eff.org/deeplinks/2024/11/nsa-surveillance-and-section-702-fisa-2024-year-review

[156] *See generally* Sarah Taitz, *Five Things to Know About NSA Mass Surveillance and the Coming Fight in Congress*, Am. C.L. Union (Apr. 11, 2023), https://www.aclu.org/news/national-security/five-things-to-know-about-nsa-mass-surveillance-and-the-coming-fight-in-congress.

[157] *See supra* notes 97–110 and accompanying text.

[158] *See, e.g.*, *Political Question Doctrine*, Legal Info. Inst., https://www.law.cornell.edu/wex/political_question_doctrine (last visited Feb. 27, 2025) ("Political Question doctrine is the rule that Federal courts will refuse to hear a case if they find that it presents a political question.").

Kingdom has steadily expanded its surveillance powers after the Snowden leaks. The UK now has one of the most expansive surveillance regimes in Europe, and almost certainly surpasses the U.S. in scope. Snowden, in 2016, claimed that "the US' National Security Agency could only dream of having the same power that the UK's GCHQ exercised."[159] Ironically, Britain has historically sought to avoid the centralized state power that was a French hallmark. As this paper shows, the UK consistently caught up to France's surveillance capabilities and may now claim the title for most surveilled country in Europe.

Part II.B.1 examines foreign intelligence surveillance from the late 18th century to WWI. During that time foreign intelligence surveillance played a key role in British colonialism and monitoring Irish terrorists. The lead up to WWI also saw drastic increases in UK surveillance capabilities. Part II.B.2 examines WWI to the 21st century. During this time, the UK continued to expand its intelligence capabilities, targeting both citizens and foreign diplomats. This period also gave rise to the Five Eyes Alliance. Finally, Part II.A.3 examines the contemporary framework, where it becomes apparent that the UK continues to conduct extensive surveillance domestically and internationally.

1. Pre-WWI

The UK (used interchangeably with Great Britian and its progeny) has a foreign intelligence wrinkle; their widespread colonization differentiates it from the U.S. This can be seen in Ireland–one of Britain's oldest colonies–near the turn of the 18th century. After the Irish Rebellion of 1798, the British collected statistics and census data on the Irish.[160] This surveillance paired with spies allowed the British "to control the Irish population more robustly... [and] play nationalist and

[159] Girod, *supra* note 48.

[160] *See* Eliza Egret & Tom Anderson, Mass Surveillance and Control of European Dissidence: The UK Surveillance State 4 (2021) ("Following the Irish rebellion of 1798, the British

[state] undertook mass surveillance of the Irish population, including the collection of statistics and census data.").

unionist populations off against each other."[161] A similar strategy was employed in India, where the British undertook scientific population classifications to use community and caste differences against the local population.[162] This colonial tactic would be expanded upon by the British in the Middle East after WWI, dispersing ID cards and developing "control systems such as security fences, watchtowers, permit systems and checkpoints."[163]

A domestic surveillance mechanism came from the Aliens Act of 1793.[164] This has been called Britain's "first large-scale statutory effort to control and curb immigration to the British Isles" and required immigrants to register with government officials on arrival.[165] In the early-19th century, Britain built up its police force, and from the "late 1820s-onward... engaged in unprecedented mass data collection as they sought to know and control their population[]."[166] Another early example of British surveillance came in the 1840's. In 1840 the British government made postage costs (up to a pound in weight and irrespective of distance) a penny.[167] This quintupled the volume of letters sent in Britian and solidified the governments monopoly on postage.[168] However, it was later

---

[161] *Id.*

[162] See id. at 4–5 ("After the 1858 Indian rebellion against the British East India Company, efforts

gathered apace to develop a new system of 'scientific' population classification in order to enable the famous British 'divide and rule' strategy, which consolidated British rule by weaponising the divisions between India's different religious communities and castes.").

[163] *Id.* at 5.

[164] Aliens Act 1793, 33 Geo. 3 c. 4.

[165] Jan C Jansen, *Aliens in a Revolutionary World: Refugees, Migration Control and Subjecthood in the British Atlantic, 1790s–1820s*, 255 Past & Present 189, 204 (2021).

[166] Dr. Gary Girod, *Mass Surveillance in France & Britain: The Age of the Masses*, Fr. Hist. Podcast (June 8, 2024), https://www.thefrenchhistorypodcast.com/mass-surveillance-in-france-britain-the-age-of-the-masses.

[167] *See* Editors of Encyclopaedia Britannica, *Penny Post,* Encyclopaedia Britannica https://www.britannica.com/topic/Penny-Post (last visited Feb. 27, 2025) ("All letters and packets up to one pound in weight were delivered for one penny (1 d)."); David Vincent, *Surveillance, Privacy and History*, Hist. & Pol'y, https://www.historyandpolicy.org/policy-papers/papers/surveillance-privacy-and-history (last visited Feb. 27, 2025) ("In 1840 the government slashed the cost of postage to a penny irrespective of distance, and introduced pre-payment to speed the process of delivery.").

[168] *See History: Victorian Britain*, BBC, https://www.bbc.co.uk/history/british/timeline/

revealed that British officials opened some of these letters for national security purposes.[169] This led to a national outcry, increased conversations surrounding privacy, and a stain on the British government.[170] Still, it would eventually be swept under the rug: the British government claimed that the legislature was investigating the matter, and courts avoided making decisions on this practice.[171]

In the 1880s, and as a result of Irish Fenian bombings, the London Police Department formed a counterterrorism branch. Although this branch (later named the "Special Irish Branch" and then "Special Branch") was meant to focus on Irish counterterrorism, it eventually expanded its monitoring to "anarchists and suffragists."[172] In the lead up to WWI, foreign intelligence surveillance ramped up in the UK. In 1909, because of widespread fear of Jewish and German infiltrators,[173] the British government formed the Secret Services Bureau.[174] This

victorianbritain_timeline_noflash.shtml (last visited Feb. 27, 2025) ("In the decade after the implementation of the 'penny post', the volume of letters sent in Britain increased five-fold to almost 350 million a year.").

[169] *See* Vincent, *supra* note 167 ("[A] 'paroxysm of national anger' exploded when the government was caught opening letters in the interests of national security.").

[170] *See id.* ("It was the political scandal of 1844, permanently scarring the career of the Minister and recalled at intervals down the decades until new regimes of surveillance were introduced around the time of the First World War, such as the 1911 Official Secrets Act.").

[171] *See* Bernard Keenan, *A Very Brief History of Interception*, LSE (Feb. 15, 2016), https://blogs.lse.ac.uk/medialse/2016/02/15/a-very-brief-history-of-interception/#prerogative ("The brief interception scandals of the 1840s and 1950s were dealt with by a most British method for diffusing scandal and brushing it under the carpet with minimum disruption: Parliamentary Inquiry.... Legally, the courts in England avoided making any decisions on interception powers at all.").

[172] *See* Gary Edward Girod, The Rise of the Information State: Domestic Surveillance in France and Britain During World War I at 12 –13 (2021) (Ph.D. dissertation, University of Houston).

[173] *See id.* at 14 (noting that the large Jewish community in London contributed to "[a]nti-Semitic fears of Jewish involvement in radical, international plots" and that German spy literature led to a mass fear of German invasion); *see also* Dr. Gary Girod, *Mass Surveillance in France & Britain: The Age of the Individual*, Fr. Hist. Podcast (June 15, 2024), https://www.thefrenchhistorypodcast.com/mass-surveillance-in-france-britain-the-age-of-the-individual ("Special Branch monitored suspected Jewish anarchists and some agents even learned Yiddish as they attempted to infiltrate the Jewish community.").

[174] *See* Girod, *supra* note 172, at 14 ("In response to allegations of German spying combined with the naval arms race in 1909 the British government quietly created the Secret Services Bureau, overseeing both foreign and domestic counterintelligence....").

organization was charged with counterintelligence activities and would later become the Security Service (MI5) and the Secret Intelligence Service (SIS or MI6).[175] In 1911, The Official Secrets Act was passed, authorizing investigations into people deemed "suspicious" and placing the burden of proving innocence on the accused parties.[176] That same year, it was discovered that the Special Branch was opening the letters of suffragettes after the movements' radicalization.[177]

2. WWI to 21st Century

The Secret Services Bureau was relatively small until it began to grow as a result of public fear during WWI.[178] At the end of WWI, due to intelligence being critical to the war effort, the British formed the Government Code and Cypher School ("GC&CS"), an entity focused on protecting communications and decrypting enemy communications.[179] The GC&CS was the predecessor of the Government Communications Headquarters ("GCHQ"),[180] and the GCHQ was named in Snowden's leaks as an entity conducting mass surveillance. Prior to and throughout the war there were censorship efforts and retaliation against communist and socialist sympathizers.[181] During WWI,

---

[175] *See id.* at 14 –15 n.36 (noting that branches of the Secret Serviced Bureau eventually became MI5 and MI6); Christopher Andrew, *The Establishment of the Secret Service Bureau*, Sec. Serv. MI5, https://www.mi5.gov.uk/history/mi5s-early-years/the-establishment-of-the--secret-service-bureau (last visited Feb. 28, 205) ("The Security Service (MI5) and the Secret Intelligence Service (SIS or MI6) began operations in October 1909 as a single organization, the Secret Service Bureau....").

[176] *See* Girod, *supra* note 172, at 15 ("In 1911 Parliament passed the Official Secrets Act which authorized investigations into suspicious persons. Once in court, the burden of proof was upon the accused.").

[177] *See* Girod, *supra* note 173 ("In March 1911 Special Branch covertly opened suffragettes' letters, a breach of privacy that was unthinkable just a few decades before.").

[178] *See generally id.*

[179] *Our Origins & WWI*, Gov't Commc'ns Headquarters, https://www.gchq.gov.uk/section/history/our-origins-and-wwi (last visited Feb. 28, 2025) ("Over the course of the First World War, Signals Intelligence provided valuable insight into enemy plans, so much so that a peacetime cryptanalytical unit was formed in 1919 to continue the mission. Originally called the Government Code & Cypher School, it would later be renamed GCHQ.").

[180] *See id.*

[181] *See* Girod, *supra* note 172, at 36 (discussing fears of communism towards the end of WWI).

the British implemented "broad public surveillance conducted by local police and prosecuted by civilian courts" against anti-war groups.[182] Through WWI the Secret Services Bureau had expanded its surveillance and by 1919 onwards British intelligence agencies had adopted anti--communist sentiments.[183] After WWI Britian surveilled writers that they believed were left-wing, including George Orwell.[184]

Post-WWI, the GC&CS grew and monitored foreign intelligence from countries like France, Japan, and the U.S., but primarily targeted the Soviet Union.[185] By 1939, it was most closely monitoring the German nazis. It saw considerable success during WWII, then turned its attention to the soviets during the Cold War (after having 80% of its staff cut once WWII ended).[186] The extent of GC&CS's surveillance post-WWII is still shrouded in some mystery, but it is known that they targeted a variety of countries by eavesdropping on their diplomatic conversations.[187] It is also known that WWII led to the creation of the Five Eyes Alliance ("FVEY") between the US, the UK, Canada, Australia, and New Zealand.[188] FVEY, mentioned in Snowden's leaks,

---

[182] *Id.* at 53.

[183] *See id.* at 163 ("[W]orries about the threat of communism and Bolshevism were deeply entrenched [in British surveillance agencies] by 1919.").

[184] *See generally* James Smith, British Writers and MI5 Surveillance, 1930–1960 (Cambridge Univ. Press 2013).

[185] *See* Daniel Lomas, *Beyond Bletchley: GCHQ and British Intelligence*, Hist. Today (Nov. 11, 2019), https://www.historytoday.com/archive/feature/beyond-bletchley-gchq-and-british--intelligence ("GC&CS had significant early success against French, Japanese and US communications. The main target was the Soviet Union's messages, thanks to government fears of revolution and subversion at home and in the Empire.").

[186] *See id.* ("But the emergence of the Soviet threat and the start of the Cold War would see a new peacetime organisation. By the end of 1944, there were over 10,000 staff at Bletchley and GC&CS's outstations. A year later there were just under 2,000, still far bigger than the interwar GC&CS.").

[187] *See, e.g.*, *id.* ("Beyond the main Soviet target, GCHQ also enjoyed successes against smaller foes – though much of its postwar diplomatic eavesdropping remains secret.").

[188] Scarlet Kim et al., *Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements*, Yale L. Sch. (Apr. 25, 2018), https://law.yale.edu/mfia/case-disclosed/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us--about-intelligence-sharing ("Born from spying arrangements forged during World War II, the Five Eyes alliance facilitates the sharing of signals intelligence among the U.S., the U.K., Australia, Canada and New Zealand.").

was an agreement between these English speaking countries to share all signal intelligence information and the techniques used to gather that information.[189] FVEY included the ECHELON program, which has been defined as "a global communications interception system aimed at the massive collection of electronic information."[190] Towards the end of the 20th century, during the period described as "The Troubles," British intelligence focused its surveillance on the Irish Republican Army ("IRA").[191]

3. Contemporary Era

Around the turn of the 21st century, mass surveillance of foreign intelligence would emerge from secrecy and take a more active role in British society. The Intelligence Services Act of 1994[192] codified the SIS and GCHQ and allowed for intelligence warrants.[193] This was expanded upon in the Regulation of Investigatory Powers Act of 2000 ("RIPA").[194] RIPA was the foundational legislation for much of the UK's surveillance activities. RIPA enabled covert surveillance activities and provided a defense against Article 8 of the European Convention on Human Rights ("ECHR") which, as previously mentioned, addresses privacy.[195] RIPA also provided a range of different warrants types, including for things like (1) phone calls and other correspondence,

---

[189] *See id.* ("The Five Eyes countries agree to exchange by default all signals intelligence they gather, as well as methods and techniques related to signals intelligence operations.").

[190] Lohanna Reis, *The Real History of the ECHELON Program: The "5 Eyes" Global Espionage Alliance*, Atlas Rep. (Jan. 2, 2024), https://atlas-report.com/the-real-history-of-the-echelon-program-the-5-eyes-global-espionage-alliance.

[191] *See generally* Thomas Leahy, The Intelligence War Against the IRA (Cambridge Univ. Press 2020).

[192] Intelligence Services Act 1994, c. 13 (UK).

[193] *Id.* § 5(2) ("The Secretary of State may, on an application made by the Security Service, the Intelligence Service or GCHQ, issue a warrant under this section....").

[194] Regulation of Investigatory Powers Act 2000, c. 23 (UK).

[195] Regulation of Investigatory Powers Act, Reeds City Council, https://www.leeds.gov.uk/privacy-and-data/investigatory-powers-act (last visited Feb. 28, 2025) ("RIPA provides an authorisation process for covert surveillance and information gathering, and an authorisation can be used as a defence against a claim that the council has interfered with an individual's right to private life under Article 8 of the European Convention on Human Rights.").

which require adequate justifications and a warrant from the a Secretary of State; (2) metadata access; and (3) covert surveillance warrants requiring approval from a senior officer.[196]

It was later revealed that less than 0.25% of the over three million warrants/decisions for interception requests from 2000–2010 were approved by a judge.[197] Similar to the U.S., the warrant process has been criticized as being a "rubber stamp."[198] RIPA also created the Investigatory Powers Tribunal ("IPT"), which specializes in surveillance and is akin to FISC in the U.S.[199] The IPT receives public complaints but initially held proceedings in secret, later adopting a mix of open and closed sessions.[200] The IPT has, however, appeared slightly more willingly to stand up for privacy rights, leading to two European Court of Justice decisions that were unfavorable to UK mass surveillance.[201]

After 9/11 in the United States, the UK legislature passed the Anti-terrorism, Crime and Security Act of 2001.[202] This bill, among other things, allowed for the Secretary of State to require phone and internet companies to retain data and permitted police to require individuals to

---

[196] *Investigatory Powers Act 2016: Explanatory Notes*, Legilsation.Gov.UK, https://www.legislation.gov.uk/ukpga/2016/25/notes/division/6/index.htm (providing, in Part 2, Chapters 1 and 2 the different types of warrants that can be issued under RIPA).

[197] *See* Eric Metcalfe, Justice, Freedom from Suspicion Surveillance Reform for a Digital Age 5 (2011) ("In total, there have been close to three million decisions taken by public bodies under RIPA in the last decade.... Of the decisions we do know about, fewer than 5,000 (about 0.16 per cent) were approved by a judge.").

[198] *See id*. at 106 ("This practice of authorising officers simply repeating or endorsing the application is, of course, better known as 'rubber stamping'.").

[199] *See, e.g.*, Diane P. Wood et al., *Judicial Oversight of Covert Action in the United States and United Kingdom: A Report from the 2015 United States–United Kingdom Legal Exchange*, 100 Judicature 35, 36 (2016) ("The United Kingdom's counterpart to the FISA Court, the Investigatory Powers Tribunal ('IPT')... has the power to hear complaints arising from the government's surveillance activities....").

[200] *See* Clare Feikert-Ahalt, *Foreign Intelligence Gathering Laws: United Kingdom*, Libr. of Cong. (June 2016), https://maint.loc.gov/law/help/intelligence-activities/unitedkingdom.php ("

[201] *What We Do: Open and Closed Proceedings*, Investigatory Powers Tribunal, https://investigatorypowerstribunal.org.uk/open-and-closed-proceedings (last visited Feb. 28, 2025) ("When the Tribunal was first established it sat in private. However, in 2003 the Tribunal decided that, in accordance with the principle of open justice it should, where possible, sit in public.").

[202] Anti-terrorism, Crime and Security Act 2001, c. 24 (UK).

give them identifying data (such as fingerprints).[203] After global terrorist attacks in the 2000's, CCTV cameras were erected widely across the already heavily surveilled London to keep a consistent eye on the city.[204] To this day, there are as many as 942,562 CCTV Cameras in London (one for every ten people),[205] making it one of the most surveilled cities in the world and the only top ten "surveilled city" outside of China.[206]

After the deterioration of UK privacy rights in the early 2000's, however, privacy rights in the UK seemingly had a string of victories. First, in 2008 the European Court of Human Rights held that an Electronic Test Facility ("ETF")–which intercepted up to 10,000 phone calls simultaneously between Dublin and London–violated the ECHR.[207] Then, in 2009 the House of Lords Select Committee on the Constitution published a damning report about the dangers of mass surveillance and the surveillance states' negative effects.[208] The report discussed the threats mass surveillance posed to privacy and social relationships, trust in the state, discrimination, and personal security.[209] Third, the Protection of Freedoms Act was signed in 2012,[210] which provided some protections for data and against government surveillance.

However, Snowden's 2013 leaks revealed that these victories may have had a negligible effect on the UK's surveillance systems. In particular, the leaks shed light on the GCHQ's bulk surveillance programs:

---

[203] *Id.* Part 10, 11.

[204] *See How Many CCTV Cameras Are in London?*, Clarion Sec. Sys., https://clarionuk.com/resources/how-many-cctv-cameras-are-in-london ("Research by Clarion Security Systems estimates that the amount of London Borough controlled CCTV cameras has risen from 7,911 (2012) to 20,873 (2022). An increase of 238.16% over the last 10 years").

[205] *See id.* ("Research by Clarion Security Systems estimates that there are over 942,562 CCTV Cameras in London's 607 square miles....").

[206] Matthew Keegan, *The Most Surveilled Cities in the World*, U.S. News & World Rep. (Aug. 14, 2020), https://www.usnews.com/news/cities/articles/2020-08-14/the-top-10-most-surveilled-cities-in-the-world (ranking London as the third most surveilled city, with each other country being in China).

[207] Liberty v. United Kingdom, App. No. 58243/00, Eur. Ct. H.R. (July 1, 2008).

[208] House of Lords, Select Comm. on the Const., Surveillance: Citizens and the State (2d. Sess., 2008-09).

[209] *Id.* at 99 –114.

[210] Protection of Freedoms Act 2012, c. 9 (UK).

Tempora, Karma Police, and MUSCULAR. GCHQ's project Tempora took data directly from fiber optic cables and stored vast amounts of it.[211] This included phone calls, email messages, and internet user history.[212] At its peak, the GCHQ was handling 600 million "telephone events" per day.[213] Operation Karma Police stored "billions of digital records about ordinary people's online activities" daily.[214] This effort monitored both domestic British citizens and foreign nationals.[215] Finally, the MUSCULAR program–a collaboration between the GCHQ and the NSA–bugged the telecommunications infrastructure of Google and Yahoo.[216]

The British population, however, seemed to care little about this surveillance. A poll of British citizens after the Snowden leaks found that "[o]nly 19% of British Adults say the British Security Services have too many powers."[217] Further, the same poll found that a 43% plurality

---

[211] *See* Ewen MacAskill et al., *GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications*, Guardian (June 21, 2013), https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa ("One key innovation has been GCHQ's ability to tap into and store huge volumes of data drawn from fibre-optic cables for up to 30 days so that it can be sifted and analysed. That operation, codenamed Tempora, has been running for some 18 months.").

[212] *See id.* ("[Tempora] includes recordings of phone calls, the content of email messages, entries on Facebook and the history of any internet user's access to websites....").

[213] *Id.*

[214] Ryan Gallagher, *Profiled: From Radio to Porn, British Spies Track Web Users' Online Identities*, Intercept (Sept. 25, 2015), https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities.

[215] *Cf.* ("[T]he cables also transport masses of wholly domestic British emails and online chats, because when anyone in the U.K. sends an email or visits a website, that person's computer will routinely send and receive data from servers that are located overseas.").

[216] *See* Sean Gallagher, *How the NSA's Muscular Tapped Google's and Yahoo's Private Networks*, Ars Technica (Oct. 31, 2013), https://arstechnica.com/information-technology/2013/10/how-the-nsas-muscular-tapped-googles-and-yahoos-private-networks (noting that the MUSCULAR program "simply plugged into the telecommunications infrastructure that carries Google's and Yahoo's private fiber links"); *see also 10 Spy Programmes With Silly Codenames Used by GCHQ and NSA*, Amnesty Int'l (Mar. 18, 2015), https://www.amnesty.org/en/latest/campaigns/2015/03/10-spy-programmes-with-silly-codenames-used-by-gchq-and-nsa ("[MUSCULAR] intercepts user data as it passes between Google servers. Yahoo! was also said to be affected.").

[217] Will Dahlgreen, *Little Appetite for Scaling Back Surveillance*, YouGov (Oct. 13, 2013), https://yougov.co.uk/politics/articles/7546-little-appetite-scaling-back-surveillance.

felt that Snowden was aiding the "enemy" by leaking this information.[218] This provides insight into the UK legislatures next moves. In 2014, the year after the leaks, the Data Retention and Investigatory Powers Act ("DRIPA") was passed with support from the three major parties.[219] DRIPA mandates the types of data that companies must keep and requires continued cooperation with the UK government to turn communications data over under RIPA.[220]

Provisions of DRIPA were subsequently overturned by the UK courts and ultimately the European Court of Human Rights.[221] This process began with an IPT decision stating that, while mass surveillance is not allowed, the GCHQ's activities do not constitute mass surveillance.[222] The UK legislature, undeterred, enacted the Investigatory Powers Act of 2016, often referred to as "Snoopers' Charter."[223] Snowden described Snoopers' Charter as "the most extreme surveillance in the history of Western democracy."[224] On one hand, the bill required communications interception warrants to be approved by a judicial official.[225] On the other, the bill required telecommunications

---

[218] *See id.* ("Regarding the leaks themselves, 43% say they are a bad thing which aid Britain's enemies.").

[219] *See Commons Passes Emergency Data Laws Despite Criticism*, BBC (July 15, 2014), https://www.bbc.com/news/uk-28305309 ("[DRIPA is] supported by the three main parties, but opposed by civil liberties campaigners.").

[220] *See generally Data Retention and Investigatory Powers Act 2014*, UK Gov. (July 25, 2014), https://www.gov.uk/government/collectionsdata-retention-and-investigatory-powers-act-2014.

[221] R (Davis & Watson) v. Sec'y of State for the Home Dep't, [2015] EWHC (Admin) 2092 (Eng.); Sec'y of State for the Home Dep't v. Watson, Joined Cases C-203/15 and C-698/15, 2016 E.C.R. (Dec. 21, 2016).

[222] *See GCHQ Does Not Breach Human Rights, Judges Rule*, BBC (Dec. 5, 2014), https://www.bbc.com/news/uk-30345801 ("The Investigatory Powers Tribunal (IPT) says that indiscriminate trawling for information would be unlawful but the way in which the intelligence agencies go about selecting and retaining material is proportionate and lawful.").

[223] Investigatory Powers Act 2016, c. 25 (UK).

[224] Rory Cellan-Jones, *'Snoopers Law Creates Security Nightmare'*, BBC (Nov. 29, 2016), https://www.bbc.com/news/technology-38134560.

[225] *See* Home Office, Report on the Operation of the Investigatory Powers Act 2016 at 3 (2016) (noting that warrants using more intrusive powers "cannot be issued by the Secretary of State or a law enforcement chief until they have been approved by an independent Judicial Commissioner").

operators to install interception capabilities,[226] widened the scope of telecommunications operators subject to monitoring,[227] gave the Secretary of State permission to serve data retention notices to telecommunications operators (requiring them to keep data for 12 months maximum),[228] and allows for bulk warrants and bulk hacking of peoples personal devices.[229] It was around this time that Snowden claimed "the US' National Security Agency could only dream of having the same power that the UK's GCHQ exercised."[230]

Courts attempted to step in. In 2019 the UK Supreme Court ruled that IPT decisions are not immune from higher court review.[231] In 2021 the European Court of Human Rights found that the Prism and Tempora programs were too broad, did not have meaningful oversight, and harmed press freedom.[232] The 2021 decision may have come too late, as by the time that decision was handed down, the UK had already left the European Union and enacted Snoopers' Charter. In 2023, the IPT ruled that UK intelligence agencies' warrant and bulk surveillance practices were unlawful.[233] The UK government admitted to wrongdoing in the wake of

---

[226] *See* Practical Law Business Crime and Investigations, *Investigatory Powers Act 2016: Overview*, Westlaw: Practical L., https://uk.practicallaw.thomsonreuters.com/w-007-0585?transitionType=Default&contextData=(sc.Default)&firstPage=true (noting that Snoopers' Chater extended "he Secretary of State's powers to require telecommunications operators to install permanent interception capabilities").

[227] *See id.* (noting that Snoopers' Chater widened "the categories of telecommunications operators that can be subject to most powers, by including private as well as public operators").

[228] *See id.* ("Where a notice is given... [d]ata may be retained for a maximum period of 12 months.").

[229] *See People vs Snoopers' Charter: Liberty's Landmark Challenge to Mass Surveillance Powers Heard in High Court*, Nat'l Council for C.L. (June 17, 201), https://www.libertyhumanrights.org.uk/issue/people-vs-snoopers-charter-libertys-landmark-challenge-to-mass-surveillance-powers-heard-in-high-court ("[Under Snoopers' Charter] [t]hese agencies can intercept everyone's digital communications in bulk, hack into our computers, phones and tablets, and create vast 'personal datasets' without suspicion.").

[230] Girod, *supra* note 48.

[231] R (on the application of Privacy International) v. Investigatory Powers Tribunal, [2019] UKSC 22.

[232] Big Brother Watch v. United Kingdom, App. No. 58170/13 Eur. Ct. H.R. (2021).

[233] *See* David Heaton, *Investigatory Powers Tribunal Accepts Mi5 and Home Secretaries Unlawfully Issued Bulk Surveillance Warrants*, Brick Ct. Chambers (Jan. 30, 2023), https://www.brickcourt.co.uk/news/detail/investigatory-powers-tribunal-accepts-mi5-and-home-

this decision.[234] Nonetheless, the UK legislature continues to expand its mass surveillance programs. The 2023 Online Safety Act requires that social media platforms monitor all content on their platforms and make it available to UK regulators, under the banner of protecting children.[235] The 2024 Snoopers' Charter amendments require tech firms with a UK presence to notify the government of security or encryption upgrades and pause implementation pending review.[236] This is presumptively so that UK intelligence agencies can ensure continued access, while preventing companies from adapting to emerging security threats.

Contemporary mass surveillance in the UK is draconian, a violation of civil liberties under UN and EU documents, potentially unworkable, and exasperating each year. The UK government can access social media content, intercept communications with minimal oversight, and now seeks to mandate tech firms to disclose security updates–likely to ensure continued backdoor access. However, surveillance developments post-Snowden appear to have little effect on British

secretaries-unlawfully-issued-bulk-surveillance-warrants ("The Investigatory Powers Tribunal... today held that both MI5 and the Secretaries of State for the Home Department acted unlawfully over several years in relation to warrants authorising bulk interception and other bulk secret surveillance....").

[234] *See UK Government Acknowledges Past Violations of Individuals' Rights and the Fight Continues...*, Priv. Int'l (Apr. 1, 2022), https://privacyinternational.org/news-analysis/4818/uk-government-acknowledges-past-violations-individuals-rights-and-fight ("The UK government has acknowledged that section 8(4) of the Regulation of Investigatory Powers Act ('RIPA')... violated Articles 8 and 10 of the European Convention on Human Rights (ECHR).").

[235] Online Safety Act 2023, c. 50 (UK); *see also* Kevin Townsend, *UK Introduces Mass Surveillance With Online Safety Bill*, Sec. Week (Mar. 30, 2023), https://www.securityweek.com/uk-introduces-mass-surveillance-with-online-safety-bill ("To be able to determine compliance with the [Online Safety Bill], [the Government's Office of Communications] must have visibility on the content. That, in simple terms, implies mass government surveillance of any internet available to users within the UK.").

[236] Investigatory Powers (Amendment) Act 2024, c. 9 (UK); *see also* Meredith Broadbent, *A New Investigatory Powers Act in the United Kingdom Enhances Government Surveillance Powers*, Ctr. for Strategic & Int'l Stud. (May 20, 2024), https://www.csis.org/analysis/new-investigatory-powers-act-united-kingdom-enhances-government-surveillance-powers (noting that the 2024 amendments allow the UK government to "(1) force technology companies, including those based overseas, to inform the UK government of planned improvements in encryption and other enhanced security and privacy measures and (2) order a halt to such changes if the agency so chooses, pending a review, with no time limit, of the legality of the order").

public sentiment: as of 2021, a poll of UK citizens found that 58% trust British intelligence services, while less than a quarter (23%) "don't have much trust."[237]

C. France

Unlike the U.S. and UK, France was not part of the Five Eyes Alliance ("FVEY").[238] When Snowden's leaks went public, the French government expressed outrage at the purported surveillance of French citizens by the NSA.[239] The French government even required the U.S. Ambassador to France to come to Paris and explain the surveillance.[240] However, some have criticized this as a "face-saving measure" as the French government allegedly *knew* that the U.S. was spying on them.[241] Further, France was doing "the exact same thing to its own citizens" and other countries.[242] Similar to the UK, France's history of surveillance goes back centuries. Surveillance measures analogous to that of the Domesday Book (called Registers) were implemented as early as 1205 under Philip II.[243]

---

[237] Milan Dinic, *The YouGov Spying Study Part Four: Trust in UK Intelligence and Security Agencies*, YouGov (Sept. 30, 2021), https://yougov.co.uk/politics/articles/38405-part-four-trust--uk-intelligence-and-security-agenc ("One in five Britons (23%) say they don't have much trust in UK intelligence services, including 7% who say they don't trust them at all. However, 58% say they do trust the intelligence services....").

[238] However, as discussed below, France worked closely with the Five Eyes alliance.

[239] *See* Dashiell Bennett, *France Is Not Happy About the Latest Snowden Leak*, Atlantic (Oct. 21, 2013), https://www.theatlantic.com/international/archive/2013/10/france-not-happy--about-latest-snowden-leak/309770 ("A new allegation, reportedly based on leaks from Edward Snowden, claims that the NSA spied on millions of phone calls and text messages inside France. The French foreign minister calls the charge 'unacceptable'....").

[240] *See id.* ("The French foreign minister... has summoned the U.S. Ambassador to Paris, Charles Rivkin, to explain his country's actions.").

[241] *See id.* ("However, the outrage appears mainly to be a face-saving measure since French officials had to know the Americans were doing some kind of spying on them – plus, they are guilty of similar snooping as well.").

[242] *Id.*

[243] Girod, *supra* note 48 ("Philippe's new Norman administrators decided to survey his holdings in a manner similar to the Domesday Book. These are known to history as the Registers, with the first, Register A, taking place in 1205.").

Due to this, Part II.C.1 starts off with Louis XVI and the French Revolution (1787-1799), occurring contemporaneously with the founding of the U.S.[244] This period saw a continuation and exasperation of existing surveillance mechanisms, although reorientated away from the aristocracy and towards the general population. Part II.C.2 examines WWI to the 21st century, which saw the French government attempt to reel in mass surveillance efforts. Finally, Part II.C.3 examines the contemporary era. Recently, France has begun to reignite surveillance efforts and may again become a world leader in mass surveillance.

1. Pre-WWI

By 1774, French monarchs had consolidated centralized power and "Louis XVI inherited... a large bureaucracy whose royal agents surveilled the aristocracy."[245] Around this time there was considerable unrest, which cumulated in the overthrowing of the monarchy and the execution Louis XVI in 1793.[246] This gave rise to The Committee of Public Safety, whose historical reign of France was called "The Reign of Terror."[247] Maximilien de Robespierre, one of the Committee's most prominent members, established twelve member "committees of surveillance" across France, charged with monitoring and arresting those deemed suspicious.[248] As many as half a million people were targeted

---

[244] *See generally* Editors of Encyclopaedia Britannica, *French Revolution*, Encyclopaedia Britannica (Feb. 15, 2025), https://www.britannica.com/event/French-Revolution.

[245] Girod, *supra* note 172, at 4; *see also* Girod, *supra* note 48 ("France from Louis XIV to Louis XVI (r. 1774-1792) created a successful surveillance apparatus targeted against their troublesome aristocracies.").

[246] *See generally* History.com Editors, *This Day In History: King Louis XVI Executed*, Hist. (Feb. 9, 2010), https://www.history.com/this-day-in-history/king-louis-xvi-executed.

[247] *See generally* Editors of Encyclopaedia Britannica, *Committee of Public Safety*, Encyclopaedia Britannica, https://www.britannica.com/topic/Committee-of-Public-Safety (last visited Feb. 28, 2025).

[248] *See* Anthony Zurcher, *Roman Empire to the NSA: A World History of Government Spying*, BBC (Nov. 1, 2013), https://www.bbc.com/news/magazine-24749166 (noting that Maximilien Robespierre and the revolutionary government "established 12-member 'committees of surveillance' throughout the country. They were authorised to identify, monitor and arrest any suspicious former nobles, foreigners, nationals who had recently returned from abroad, suspended public officials and many more.").

by these committees.[249] During this time citizens were told they had a duty to report counter-revolutionaries.[250] Although the Committee of Public Safety would be overthrown, their successors continued to increase spies in Paris and gave sweeping authority to local military to keep the peace.[251] This shifted surveillance focuses away from the aristocracy and towards the general public, which continued when Napoleon Bonaparte effectively seized power in 1799.[252]

Napoleon developed a surveillance network that was decades ahead of the U.S. and UK and exemplified a comprehensive pre-internet surveillance society.[253] Napoleon centralized police forces by developing a hierarchical system that allowed for regular contact between localities.[254] The police would intercept communications and were required to provide reports "on [public] opinion, the press, theatres,

---

[249] *See id.* ("Historians estimate that as many as half a million people were targeted by the surveillance committees....").

[250] *See* Christopher Andrew, The Secret World: A History of Intelligence 322 (Yale Univ. Press 2018) (noting that, under the committees of surveillance, "[a]ll citizens were told they had a duty to denounce counter-revolutionaries").

[251] *See* Girod, *supra* note 172, at 4 ("In spite of Enlightenment rhetoric, the revolutionary National Assembly and its successors retained the practices of the *Ancien Régime* against anti--revolutionary threats. Already in 1789, the Assembly increased the number of police spies in Paris and adopted many of the *Ancien Régime*'s heavy-handed repressive tactics."); Girod, *supra* note 166

[252] *See* Girod, *supra* note 172, at 4 –5 ("The only major change the Revolutionary governments developed was to shift domestic surveillance from the aristocrats to the broader public."); Girod, *supra* note 166 ("[W]hile the Revolution brought down the old political order it did not greatly alter the bureaucratic apparatus nor the functions of intelligence-gathering. Its major contribution to this sector was to refocus Ancien Régime-era control mechanisms from aristocrats to the masses.").

[253] *See* Laura Kayali, *From Napoléon to Macron: How France learned to love Big Brother*, Politico (July 23, 2023), https://www.politico.eu/article/france-surveillance-cameras-privacy--security-big-brother-paris-olympics (discussing extensive surveillance efforts under Napoléon Bonaparte); Marc Fourny, *How Napoleon Monitored the French*, Le Point (July 17, 2022), https://www.lepoint.fr/histoire/comment-napoleon-surveillait-les-francais-16-07--2022-2483439_1615.php#11 (same) (translated using Google Translate); Frank Maloy Anderson, *Law for Reorganizing the Administrative System*, Napoleon Series, https://www.napoleon--series.org/research/government/legislation/c_administrative.html (last visited Feb. 28, 2025) (providing Napoleon-era legislation that helped facilitate mass surveillance).

[254] *See* Girod, *supra* note 172, at 5 ("Within three months of seizing power, Napoleon centralized police forces.... The central state established a hierarchical system and mechanisms for regular contact and supervision of localities.").

crimes, subsistence, trade, religions and emigrants."[255] This allowed Napoleon to get a consolidated view of France through networks of informants. Parisian police officers specifically were mandated to address false information and suppress misinformation (according to the states definition).[256] Napoleon also utilized the Black Chamber, or *cabinet noir*, to secretly open the mail of foreign embassies and suspected individuals.[257] However, the *cabinet noir* both preceded and lasted long after Napoleon.[258]

Napoleons police reforms lasted through the Burbon Restoration (1814-1830) and long after his reign.[259] Domestic surveillance was integrated into the Ministry of the Interior and police were continually mandated "to monitor the public mood so the state was prewarned against revolutionary outbursts."[260] France also became one of the first countries to collect national criminal statistics in 1825.[261] From the 1820's onwards France, alongside Britian, "engaged in unprecedented mass data collection as they sought to know and control their populations."[262]

However, France's shocking defeat in the 1870 Franco-Prussian

---

[255] Fourny, *supra* note 253 (translated using Google Translate); *see also* Girod, *supra* note 172, at 5 ("Minister of Police Joseph Fouché refashion the Paris police force into a well-ordered bureaucracy that monitored Parisians' views of the state.").

[256] *See* Girod, *supra* note 166 ("Uniformed police were ordered to counter false rumors and given remarkable powers to suppress what the state deemed disinformation.").

[257] *See* SpyScape, *Spy Secrets: Tales From Napoleon's Top-Secret Black Chambers*, SpyScape, https://spyscape.com/article/spy-secrets-tales-from-the-black-chambers (last visited Feb. 28, 2025) ("Codebreakers also worked alongside stenographers in the post office's secret Black Chamber, copying, deciphering, and resealing correspondence sent to foreign embassies.").

[258] *See id.* ("The *Cabinet Noir* intelligence-gathering continued as Napoleon conquered much of Europe in the early 19th century but he was not the first – or last – leader to rely on the prying eyes of the Black Chamber spies.").

[259] *See* Girod, *supra* note 166 ("While Napoleon's government maintained stability within France his foreign wars ended his empire. Yet, most of the police reforms were left in place during the Restoration.").

[260] *Id.*

[261] *See id.* ("The [French] state collected national criminal statistics starting in 1825, becoming one of the first nations to do so.").

[262] *Id.*

War exposed its intelligence shortcomings against Germany.[263] The war lasted only one year and led France to establish the *Deuxième Bureau* to conduct domestic intelligence gathering.[264] From approximately 1880 onwards the *Sûreté Générale* (originally developed by the Second Empire in the 1850's) continued to collect information on French citizens–particularly workers, Catholics, anarchists, socialists, and anti-militarists–through surveillance and attempted to shape public opinion.[265] This included the development of Carnet B in 1886, which took profiles of foreigners and subjected them to surveillance.[266]

Around the turn of the 20th century, France suffered a mass paranoia of German and Jewish spy infiltration (analogous to the British).[267] The *Section de Statistique*, part of the *Deuxième Bureau*, was at the forefront of this paranoia.[268] This period saw a multitude of accused spies being tried and convicted.[269] It also led to the Dreyfus Affair, in which the French government accused Alfred Dreyfus, an artillery officer of Jewish decent, of treason.[270] An antisemitic newspaper caught onto the story, bringing

---

[263] *See* Girod, *supra* note 173 ("The Franco-Prussian War shocked France. The country believed it was the great land power of Europe, yet Prussia and its allies defeated French armies at every turn due to their industrial and intelligence-gathering superiority which allowed for the precise movement of troops throughout eastern France.").

[264] *See id.* ("The newly-declared Third Republic recognized that France was woefully behind the new German Empire and created a series of military intelligence-gathering services. On 8 June, 1871 France inaugurated the Deuxième Bureau, which was in charge of domestic intelligence gathering." (footnote omitted)).

[265] *See id.* ("[The Sûreté Générale] collected information on all people, though primarily focused on workers and Catholic organizations.... The Sûreté's budget expanded after anarchist threats in the 1890s. Finally the gendarmerie actively engaged in surveillance, shaping public opinion and social control." (footnotes omitted)).

[266] *See id.* ("Boulanger developed the Carnet B in 1886. The Carnet B were profiles police took of foreigners.").

[267] *See id.* (discussing paranoia of German spies and rising antisemitism in the late 19th century).

[268] *See id.* ("The French military General Staff and the *Section de Statistique* inherited Boulanger's paranoia that German spies were everywhere.")

[269] *See id.* ("By 1894 a number of accused spies were convicted and even more were tried.").

[270] *See Dreyfus Affair: Topics in Chronicling America*, Libr. of Cong., https://guides.loc.gov/chronicling-america-dreyfus-affair ("French artillery officer Alfred Dreyfus, of Jewish descent, was convicted of treason in 1894 and sentenced to life in prison."); *see also* Girod, *supra* note 173 ("Lieutenant-colonel Alfred Dreyfus, an Alsatian Jew, fell victim to this paranoia when on 13 Oct. 1894 he was officially accused of treason.").

national attention and xenophobia against jews.[271] Despite strong evidence of Dreyfus's innocence, the government refused to admit its mistake, instead doubling down on the charges and even bribing witnesses against him.[272] Dreyfus was court-martialed twice, found guilty the second time, but was eventually exonerated in 1906.[273] Dreyfus's story showcases the experience that others had during this period of paranoia.

The Dreyfus Affair, and accompanying outcry, led to the *Section de Statistique* being dismantled.[274] It also led to a divide between the police and the military, as the former defended Dreyfus and the latter was his persecutor.[275] Contemporaneously, the *Sûreté Générale* kept active surveillance over anarchist and communist groups, including membership, meetings, and general activities.[276] The events of this period caused a shift in domestic intelligence gathering from the military and towards the civilian police.[277] Nonetheless, "from 1899 through WWI domestic surveillance was conducted by the *Sûreté*, *Deuxième Bureau* and local police in an overlapping web of prerogatives."[278] These different groups set the framework and infrastructure for mass surveillance through WWI and long into the future.

---

[271] *See* Girod, *supra* note 173 ("[T]he antisemitic newspaper *La Libre Parole* incensed the nation with its exposés on a traitorous Jew conspiring to destroy the French nation.").

[272] *See id.* ("The General Staff and the *Section de Statistique* did everything in its power to ensure Dreyfus' conviction rather than admit they had made a mistake which would damage their reputation.... They bribed lieutenant Eugen Lazare von Czernuski to testify against Dreyfus.").

[273] *See* Elizabeth Nix, *What Was the Dreyfus Affair?*, Hist. (June 1, 2023), https://www.history.com/news/what-was-the-dreyfus-affair (noting that Dreyfus was court martialed in 1898 and 1899, was found guilty in the 1899 trial, but was eventually exonerated in 1906).

[274] *See* Girod, *supra* note 173 ("The *Section de Statistique*'s corruption was too much for the French government. On September 12, 1899, three days after Drefyus' second conviction at Rennes, it was reorganized and stripped of its autonomy.").

[275] *See id.* ("The Affair ruptured military and police relations, as the military slandered Dreyfus and defended their prerogative while the police defended Dreyfus and the constitutional framework of the Republic.").

[276] *See* Girod, *supra* note 172, at 56 ("The *Sûreté Générale* kept an active dossier on the *Fédération Communiste Anarchiste Révolutionnaire de Langue Française*, including meeting locations, a list of its leaders, its affiliations with other radical groups, its newspapers, each chapters' year of founding, and notes on meetings and general activity.").

[277] *See* Girod, *supra* note 173 ("The [Drefyus] Affair ensured that domestic-intelligence gathering was run by civilians rather than the military.")

[278] *Id.*

During the Third Republic (1870–1940), it was also discovered that the government kept a central file of national security.[279] This file contained more than 600,000 police reports detailing political surveillance, attempts to control foreigners, and a wide variety of other things.[280] In the lead up to WWI, Paris police and the *Sûreté Générale* closely monitored labor groups and far-right groups.[281] Intelligence capabilities were expanded by the 1913 development of the Paris *Renseignements généraux de la préfecture de police* ("RGPP"), a Paris police intelligence branch and predecessor to the current *La direction du Renseignement de la préfecture de police de Paris* ("DR-PP").[282] Overall, the half-century before WWI "witnessed the emergence of agencies specialized in espionage, counterespionage, assessment, and analysis" in France.[283] These programs laid the foundation for foreign intelligence during WWI, with the war rapidly sophisticating French intelligence agencies.[284]

---

[279] *See* Kayali, *supra* note 253 ("Between 1870 and 1940, under the Third Republic, the police kept a massive file – dubbed the National Security's Central File – with information about 600,000 people, including anarchists and communists, certain foreigners, criminals, and people who requested identification documents.").

[280] *See id.*; *see also* Ministère de la Culture, *Nominative Files From the Central File of National Security (1870-1940)*, République Francaise (June 13, 2024), https://www.data.gouv.fr/fr/datasets/dossiers-nominatifs-du-fichier-central-de-la-surete-nationale-1870-1940 (Translated using Google Translate) ("The central file of the National Security... is one of the emblematic funds of the National Archives. This corpus of archives of the Ministry of the Interior is made up of more than 600,000 nominal police files from the Third Republic (1870s-1940s)....").

[281] *See* Girod, *supra* note 172, at 57–58 ("Throughout April 1914, the Paris police monitored labor groups, taking note of their meetings, speeches, organizational structure, membership and finances as they sought to measure their strength, radicalization and intentions.... Long before 1914 French intelligence services also regularly monitored far-right, antidemocratic groups.").

[282] *See generally Brief History of General Intelligence (RG)*, Direction Générale de la Sécurité Intérieure [hereinafter *France RG History*], https://www.dgsi.interieur.gouv.fr/decouvrir-dgsi/notre-histoire/breve-histoire-des-renseignements-generaux-rg (last visited Mar. 1, 2025) (Translated using Google Translate).

[283] Deborah Bauer, Marianne Is Watching: Intelligence, Counterintelligence, and the Origins of the French Surveillance State 255 (2021).

[284] *See id.* ("Intelligence agencies entered the war in a primitive, but developing, state and came out of it far more honed and professional.").

2. WWI to 21st Century

During WWI, suspected subversives to the war were closely monitored, as the French government feared again losing to the Germans in the wake of the Franco-Prussian War.[285] Internationally, France worked with Britian to establish Belgian spy networks to gather intelligence on Germany.[286] After the war, mass paranoia led to the conflation of espionage and counterespionage, leading to increased domestic surveillance efforts.[287] This period also saw a continual reorganization of intelligence efforts, particularly in the 1930s.[288] During WWII, German occupied Vichy France (1940-1944) was responsible for the "massive interception of private correspondence" to gauge public mood and watch for dissidents of the Nazi party.[289] It was also characterized by an authoritarian police state and cracking down on dissidents.[290] However, it is difficult to blame this on the French government due to the Nazi occupation.[291]

Post-WWII France gave rise to intelligence agencies focused on both domestic and international surveillance. *La direction de la surveillance du territoire* ("DST") was created in November of 1944 to operate as a domestic intelligence agency.[292] *Service de documentation*

---

[285] *See* Girod, *supra* note 172, at 60–62 (discussing extensive government control over the media and increased military strength during the start of WWI).

[286] *See* Bauer, *supra* note 283, at 257 ("The French worked in conjunction with their British allies to establish networks of observers and informers in occupied Belgium.").

[287] *See id.* at 261 (discussing French intelligence activites between WWI and WWII).

[288] *See id.* ("Throughout the 1930s the French state developed a series of branches dedicated to the collection and analysis of intelligence, for the most part tasking the army with the external collection of information and the police with domestic counterintelligence.")).

[289] Roger Austin, *Surveillance and Intelligence Under the Vichy Regime: The Service Du Controle Technique, 1939–45*, 1 Intel. & Nat'l Sec. 123, 123 (1986).

[290] *See* Lorraine Boissoneault, *Was Vichy France a Puppet Government or a Willing Nazi Collaborator?*, Smithsonian Mag. (Nov. 9, 2017), https://www.smithsonianmag.com/history/vichy-government-france-world-war-ii-willingly-collaborated-nazis-180967160 ("[A]ll the foreign Jews were put into camps, they cracked down on dissent, and it was in some ways increasingly a police state.").

[291] *Cf. id.* (noting that the Vichy France government may have been complicit in Nazi war crimes).

[292] *See France RG History*, *supra* note 282 ("In November 1944, General de Gaulle restructured the intelligence and counter-espionage services. He created the Directorate of Territorial

extérieure et de contre-espionnage ("SDECE") was created in 1946 to monitor external intelligence,[293] and was the predecessor of *Direction Générale de la Sécurité Extérieure* ("DGSE").[294] DGSE is the modern--day French analog to the NSA and GCHQ along with *Direction générale de la Sécurité intérieure* ("DGSI"),[295] which was formed in 2008.

Public outcry came in 1974 when *Le Monde* published an article that exposed the French government's Safari project, which sought to create a national computerized database of all its citizens.[296] As a result of this backlash, the *Loi Informatique et Libertés* was enacted in 1978 to better protect personal data. This act also formed the *Commission nationale de l'informatique et des libertés* ("CNIL"), which was charged with monitoring "the processing of personal data."[297] However, it is unclear how successful CNIL has been in monitoring mass surveillance, as shown by developments in the late 20th century and throughout the 21st century. One example of this is the Elysée wiretapping scandal, where it was discovered that President François Mitterrand "tapped the

---

Surveillance (DST) and confirmed the missions of the General Intelligence Service, placed within the national security.").

[293] *See From the BCRA to the DGSE*, Ministre des Armées, https://www.cheminsdememoire.gouv.fr/en/bcra-dgse (last visited Mar. 1, 2025) ("The Service de Documentation Extérieure et de Contre-Espionnage (Foreign Documentation and Counter-Espionage Service – SDECE), which came into being in 1946.... The SDECE moved to Boulevard Mortier, where it has remained ever since, only changing its name in 1982 to become the DGSE.").

[294] *See id.*

[295] *See* Nicolas Boring, *Foreign Intelligence Gathering Laws: France*, Libr. of Cong. (Dec. 2014), https://maint.loc.gov/law/help/foreign-intelligence-gathering/france.php ("It appears that large-scale communications interception is mainly done by the DGSE, which has been reported to systematically collect all telephone and electronic communications metadata in France."); *see also* Christian Chesnot, *Guilhem Giraud: "Thanks to Artificial Intelligence, Mass Surveillance Has No Limits!"*, Radio Fr. (Dec. 29, 2022), https://www.radiofrance.fr/franceculture/guilhem--giraud-grace-a-l-intelligence-artificielle-la-surveillance-de-masse-n-a-pas-de-limite-2112778 (Translated using Google Translate) (discussing mass surveillance at the DGSI).

[296] Philippe Boucher, *An IT Division is Created at the Chancellery "Safari" or the Hunt for the French*, Le Monde (Mar. 21, 1974), https://www.lemonde.fr/archives/article/1974/03/21/une-division-de-l-informatique-est-creee-a-la-chancellerie-safari-ou-la-chasse-aux--francais_3086610_1819218.html (Translated using Google Translate).

[297] Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés art. 8 [Law no. 78-17 of January 6, 1978 Relating to Information Technology, Files and Freedoms].

phones of some 150 people" including politicians and journalists in the 1980s.[298] France's lack of a clear legal framework for wiretapping led to two unanimous European Court of Human Rights rulings invalidating its wiretap warrants.[299]

In response to these decisions, the French legislature tried to clarify the bounds and procedures for state surveillance. *Loi sur l'Enregistrement des Communications Électroniques* enacted in 1991 ("Wiretap Act") allowed the Prime Minister, or his designees, to approve interceptions of electronic correspondence for national security purposes.[300] It did not provide for judicial review of these decisions.[301] It did, however, establish the *Commission nationale de contrôle des interceptions de sécurité* ("CNCIS") to ensure compliance with the act.[302] CNCIS reviews authorizations made by the Prime Minister.[303] However, CNCIS decisions are not binding, and "out of 6,396 interception authorizations granted in 2011, only fifty-five received a negative recommendation by the CNCIS."[304] It is likely that oversight under the

---

[298] Jon Henley, *Bugging Scandal Lands Mitterrand Allies in Court*, Guardian (Aug. 9, 2022), https://www.theguardian.com/world/2002/aug/09/france.jonhenley.

[299] *See* Félix Tréguer, Hal Open Sci., From Deep State Illegality to Law of the Land: The Case of Internet Surveillance in France 10 (2016) ("[I]mportant criminal cases from France eventually reached the ECHR. And in two unanimous decisions issued in April 1990, the Court eventually struck down French wiretap warrants for they were not carried on 'in accordance with the law.'" (citing ECHR, Kruslin v. France, n. 11801/85, 24 April 1990; ECHR, Huvig v. France, n. 11105/84, 24 April 1990)).

[300] Loi n. 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques Title 2 [Law No. 91-646 of July 10, 1991 Relating to the Secrecy of Correspondence Sent by Electronic Communications] [hereinafter 1991 Wiretap Act] (authorizing the interception of foreign intelligence for national security purposes based on approval from the Prime Minister or his designates).

[301] *See generally id.*; Boring, *supra* note 295 (noting that communication interception authorizations are fully within the purview of the executive branch).

[302] 1991 Wiretap Act, *supra* note 300, at art. 13; *see also* Boring, *supra* note 295 ("The main body responsible for the oversight of interception surveillance is the Commission nationale pour les interceptions de securité (CNCIS, National Commission for Security Interceptions). When the Prime Minister (or one of his/her delegates) authorizes a communication interception, the CNCIS is to review this authorization." (footnote omitted)).

[303] *See* sources cited *id.*295

[304] Boring, *supra* note 295.

Wiretap Act has historically been weak,[305] and at the time served as the legislation underpinning France's mass surveillance activities.

3. Contemporary Era

Just prior to 9/11, in 2000, the French legislature enacted a bill requiring internet service providers "to hold and retain data that allows the identification of *any person* who has contributed to the creation of content for the services they provide."[306] Then, like the U.S. and UK, 9/11 increased mass surveillance efforts. A former DGSI engineer noted that–in the years leading up to 9/11, even with the 1990's bills–French mass surveillance was generally left to the police.[307] But after 2001 the French government began to enhance its surveillance activities.[308] In November of 2001, the French legislature amended an existing law to require telecommunications operators to retain phone and metadata.[309] While this had a sunset provision, it was later permanently codified.[310] In the 1990s France also saw the widespread implementation of video surveillance across the country.[311]

---

[305] *See id.* ("The CNCIS's recommendations do not appear to be legally binding. Parliamentary oversight appears to be weak, as requests for classified documents from parliamentary committees tend to be rejected, and members of the French Parliament have no right to hear or question members of the intelligence services.").

[306] Loi n. 2000-719 du 1er août 2000 modifiant la loi no 86-1067 du 30 septembre 1986 relative à la liberté de communication [Law No. 2000-719 of August 1, 2000 Amending Law No. 86-1067 of September 30, 1986 Relating to Freedom of Communication] (Translated using Google Translate); *see also* Tréguer, *supra* note 299, at 13–14 (translating the bill as requiring providers to retain "data allowing the identification of anybody who contributed to the creation of the content").

[307] *See* Chesnot, *supra* note 295 (noting that around 1997-1998 surveillance was a police responsibility).

[308] *See id.* ("From 2001, I noticed profound changes in doctrine, and when I returned to the DST as an engineer, I began to see this new mode of operation being put in place.").

[309] Loi n. 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne art. 29 [Law No. 2001-1062 of November 15, 2001 Relating to Daily Security]; *see* Tréguer, *supra* note 299, at 14 ("French... parliament[] amended their national law to force telecom operators to retain their users' telephone and Internet metadata." (citing *id.*)).

[310] *See* Tréguer, *supra* note 299, at 14 ("In March 2006 however, the provision was made permanent through a new vote in Parliament, though it was only in March 2006 that its implementation decree was adopted." (footnotes omitted).

[311] *See* Nteboheng Maya Mokuena, *Playing Games with Rights: A Case Against AI Surveillance at the 2024 Paris Olympics*, Geo. L. & Tech. Rev. (May 2024), https://

In 2004, amendments to the Wiretap Act replaced "telecommunications" with "electronic communications," broadening surveillance to include internet activity.[312] The 2006 attacks in Madrid and London paired with an EU 2006 data retention policy led the French legislature to enact *Loi relative à la lutte contre le terrorisme* ("2006 Terrorism Act").[313] The 2006 Terrorism Act permitted French intelligence services to access metadata retained under the 2001 bill and online content under the 2000 bill.[314] Intended solely for counterterrorism, the law included a sunset provision but was repeatedly extended.[315]

In 2008, France faced another scandal when details of EDVIGE, a sweeping government surveillance database, was leaked.[316] It was just a couple years later in 2011 when France signed the Lustre agreement with the Five Eyes Alliance ("FVEY").[317] The Lustre agreement was an international cooperation agreement that shared mass surveillance

georgetownlawtechreview.org/playing-games-with-rights-a-case-against-ai-surveillance-at-the--2024-paris-olympics ("[I]n the 1990s, France implemented widespread video surveillance across the country to reduce police response time and petty crime.").

[312] *See* Tréguer, *supra* note 299, at 17 ("[T]he Wiretapping Act was also quietly amended in 2004.... This legislative patch changed the word 'telecommunications' for 'electronic communications,' which was deemed enough to extend the Act's scope to Internet communications." (citing Loi n. 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle [Law No. 2004-669 of July 9, 2004 Relating to Electronic Communications and Audiovisual Communication Services])).

[313] Loi n. 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers [Law No. 2006-64 of January 23, 2006 Relating to the Fight Against Terrorism and Containing Various Provisions Relating to Security and Border Controls].

[314] *See* Tréguer, *supra* note 299, at 14 –15 (discussing the type of data that the 2006 bill authorized intelligence agencies to access).

[315] *See id.* at 15 ("Also introduced as a sunset provision, administrative metadata access was prolonged a first time in December 2008 and then again in December 2012, despite criticisms from the French Human Rights League.").

[316] *See* Julian Sanchez, *Big Sister is Watching: EDVIGE and the Angry French*, Ars Technica (Sept. 9, 2008), https://arstechnica.com/tech-policy/2008/09/big-sister-is-watching-edvige--and-the-angry-french ("The new database, known as EDVIGE, has sparked a firestorm of opposition from French unions, non-profits, and civil liberties groups since the national privacy watchdog, CNIL, forced the government to make its existence public in July.").

[317] *See generally* Jacques Follorou, *Surveillance: DGSE Transmitted Data to the American NSA*, Le Monde (Oct. 30, 2013), https://www.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html (Translated using Google translate).

intelligence between France and FVEY.[318] The Lustre agreement led DGSE to transmit "millions of data relating to the private lives of millions of French people" to the NSA, with little apparent oversight from CNCIS.[319]

It is interesting to note that Snowden's 2013 leaks did not lead to a strong backlash in France.[320] Later that year, the muted public response enabled the French legislature to further erode privacy rights. *Loi de programmation militaire 2014-2019* ("Military Bill 2013"),[321] which faced strong opposition,[322] gave government surveillance agencies real time access to metadata.[323] The following year, amid the rise of ISIS, a new law was passed that circumvented warrant requirements and gave additional powers to law enforcement and intelligence agencies.[324] These terrorism fears were realized in January 2015 when terrorists attacked Charlie Hebdo, a French satirical magazine, for their depictions of Islam.[325] This contributed to the passing of France's first comprehensive surveillance law, the *Loi relative au renseignement*

---

[318] *See id.* (noting that the Snowden leaks revealed "the existence of a cooperation agreement on surveillance between France and the United States known as 'Lustre'".).

[319] *Id.*

[320] *See* Tréguer, *supra* note 299, at 23 ("[T]he French civil society reaction to the Snowden disclosure –the first of which appeared in Guardian article on June 5th, 2013– was relatively mild.").

[321] Loi n. 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale [Law No. 2013-1168 of December 18, 2013 Relating to Military Programming for the Years 2014 to 2019 and Containing Various Provisions Concerning Defense and National Security].

[322] *See* Tréguer, *supra* note 299, at 31 (noting that the Military Bill 2013 has "growing mobilization by civil society, media attention to the issue, and increasingly vocal opposition by a few MPs....").

[323] *See* source cited *supra* note 321; Tréguer, *supra* note 299, at 29 ("[T]he government's proposal provided intelligence agencies with both ex post and real-time access to metadata, including geographic metadata.").

[324] *See* Tréguer, *supra* note 299, at 34 ("[A]nother [bill] was introduced in great fanfare in July 2014. The law greatly reinforced the power of intelligence and police agencies by circumventing traditional criminal procedures." (citing Loi n. 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme [Law No. 2014-1353 of November 13, 2014 Strengthening the Provisions Relating to the Fight Against Terrorism])).

[325] *See generally* John Leicester, *The Charlie Hebdo Slaughter and Follow-up Terror Attacks 10 Years Ago That Changed France*, Assoc. Press (Jan. 7, 2025), https://apnews.com/article/france-charlie-hebdo-photos-terror-f42dc6d41b376ce2f7abec0e75760e7e.

("Intelligence Act").[326] Unlike the U.S. post-9/11 Patriot Act, however, the Intelligence Act may have been long in the making.[327] Terrorism fears were again exasperated on November 13, 2015, when terrorists attacked Paris, killing at least 130 and injuring 350.[328]

The Intelligence Act expanded permissible intelligence-gathering techniques, broadened surveillance justifications, permitted the French government to increase the amount of agencies with surveillance capabilities, and provided penalties (including imprisonment) for companies failing to comply with surveillance measures or data requests.[329] It also developed a new commission to replace the CNCIS, the *Commission nationale de contrôle des techniques de renseignement* ("CNCTR").[330] Like the CNCIS, the CNTCR only issues non-binding opinions on surveillance requests, and the Intelligence Act did not provide for judicial oversight.[331] Moreover, CNTCR lacks oversight of data-sharing with international foreign intelligence agencies, creating a significant loophole.[332]

The Intelligence Act also permitted the installation of black boxes in telecommunication and internet service provider infrastructure to monitor and collect real-time web traffic.[333] The Intelligence Act

---

[326] *Cf.* Boring, *supra* note 295 ("Although the adoption of the Law was probably accelerated by the intensity of the threat of terrorism and, in particular, the January 2015 attacks in France, the government emphasized that it was the result of thorough reflection and not enacted under the pressure of any specific urgent situation.").

[327] *See id.*

[328] *See generally* Michael Ray, *Paris Attacks of 2015*, Encyclopedia Britannica (Feb. 14, 2025), https://www.britannica.com/event/Paris-attacks-of-2015.

[329] *See* Tréguer, *supra* note 299, at 38 –39 (discussing general provisions of the Intelligence Act).

[330] *See id.* at 39 (discussing the CNCTR and surveillance oversight under the Intelligence Act).

[331] *See id.* at 39 –40 (same).

[332] *See id.* at 40 ("One hugely significant exception to the CNCTR's oversight powers are [the] bulk of data obtained through data-sharing with foreign intelligence agencies." (citation omitted)).

[333] *See id.* at 40 –41 (discussing black boxes under the Intelligence Act); *see also France: New Surveillance Law a Major Blow to Human Rights*, Amnesty Int'l (July 24, 2015), https://www.amnesty.org/en/latest/news/2015/07/france-new-surveillance-law-a-major-blow-to-human-rights ("[The Intelligence Act] allows the use of mass surveillance tools that capture mobile phone calls and black boxes (for the purposes of counterterrorism) in internet service providers that collect and analyse the personal data of millions of internet users.")

further authorized the hacking of computer systems, explicitly legalized the DGSE's international surveillance, and imposed data retention requirements for government intelligence agencies, among other provisions.[334] Later, in 2023, the French legislature adopted a bill permitting "law enforcement agents to remotely tap into the cameras, microphones and location services of phones and other internet-connected devices of some suspected criminals."[335]

There have been judicial challenges against this surveillance. In a Constitutional Court challenge to the Intelligence Act, it was generally upheld, but some provisions were declared invalid including Article 854-1 (which addressed international surveillance) and parts of Article 821-6 (which addressed real-time monitoring through devices).[336] In 2020 the Court of Justice of the European Union mandated that EU law applies to member states forcing telecommunications operators to retain data.[337] In 2021 the *Conseil d'État* referred the legality of mandated data retention measures in France to the Court of Justice of the European Union.[338] In 2024 the EU Court of Justice ruled on this by reemphasizing that access to personal data must meet the proportionality requirement in Article 15(1) of Directive 2002/58.[339] It is worth noting that, unlike the U.S. and UK, France operates on a Civil Law system that does not have binding judicial precedents.[340]

---

[334] *See* Tréguer, *supra* note 299, at 41–44.

[335] Youcef Bounab, L*awmakers Approve Bill Allowing French Police to Locate Suspects by Tapping Their Devices*, PBS News (July 18, 2023), https://www.pbs.org/newshour/world/lawmakers-approve-bill-allowing-french-police-to-locate-suspects-by-tapping-their-devices.

[336] Conseil constitutionnel [CC] [Constitutional Court] decision No. 2015-713 DC, July 23, 2015, https://www.conseil-constitutionnel.fr/decision/2015/2015713DC.htm.

[337] *See LQDN, FDN and Others v. France*, Priv. Int'l, https://privacyinternational.org/legal-action/lqdn-fdn-and-others-v-france (last visited Mar. 1, 2025) ("EU law applies every time a national government forces telecommunications providers to process data, including when it is done for the purposes of national security.").

[338] Conseil d'État, Assemblée, 21/04/2021, 393099 [Council of State, Assembly, 04/21/2021, 393099].

[339] 2024 E.C.J. Case C-470/21, La Quadrature du Net and Others.

[340] *See, e.g.*, *The Layout of the French Legal System*, Geo. L. Libr. (Nov. 11, 2024), https://guides.ll.georgetown.edu/francelegalresearch/legalsystem ("France is a civil law system which means it places a greater emphasis on statutes as found within various codes, instead of case law.").

From the Age of Aristocracy through Napoleon, the French outpaced the U.S. and UK in their surveillance efforts. Then, arguably, from the late 19th century through to the 21st century France's mass surveillance efforts fell behind. Now, they may have moved back into the forefront (based on public knowledge of government surveillance activities), partially as a result of the 2024 Paris Olympics. *Loi olympiques et paralympiques* ("Olympics Law")[341] was passed in May 2023 in the midst of civil rights campaigns against it.[342] The Olympics Law allowed, for the first time in Europe, AI-powered mass video surveillance.[343] Under the Olympics Law AI analyzes real-time footage to make determinations about suspicious activity.[344] This measure also led to hundreds of cameras being added to the already heavily-surveilled Paris.[345] This AI facial recognition bill had a sundown provision for December 2024, but was already extended until March 2025,[346] and police members have advocated for its extension or permanent codification.[347]

---

[341] Loi n. 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions [Law No. 2023-380 of May 19, 2023 Relating to the 2024 Olympic and Paralympic Games and Containing Various Other Provisions].

[342] *See generally* Laura Kayali, *French Surveillance System for Olympics Moves Forward, Despite Civil Rights Campaign*, Politico (Mar. 8, 2023), https://www.politico.eu/article/paris-olympics-surveillance-arsenal-moves-ahead-despite-civil-rights-campaign; *France: Allowing Mass Surveillance at Olympics Undermines EU Efforts to Regulate AI*, Amnesty Int'l (March 23, 2023), https://www.amnesty.org/en/latest/news/2023/03/france-allowing-mass-surveillance-at-olympics-undermines-eu-efforts-to-regulate-ai.

[343] *See 'All-out Assault on Privacy': France is First EU Country to Legalise AI-driven Surveillance*, Brussels Times (Mar. 29, 2023), https://www.brusselstimes.com/430820/all-out-assault-on-privacy-france-is-first-eu-country-to-legalise-ai-driven-surveillance ("This is the first time algorithmic mass surveillance is authorised in Europe....").

[344] *See id.* ("AI-driven surveillance analyses footage in real-time, scans and captures data from all people within its radius, and makes predictions and determinations about them.").

[345] *See* Alberto Senante, *Paris Olympics Security: Unprecedented AI Surveillance Creates Another Risk*, WorldCrunch (July 26, 2024), https://worldcrunch.com/culture-society/paris-olympics-security-surveillance ("More than 400 cameras will be added to the 4,000 already operating in Paris and placed at the entrances to stadiums, streets and nearby transport....").

[346] *See* David Coffey, *Privacy Fears Grow as France Extends Ai Surveillance Beyond Olympics*, RFI (Nov. 11, 2024), https://www.rfi.fr/en/france/20241011-privacy-fears-grow-as-france-extends-ai-surveillance-beyond-olympics-avs (noting that France extended "AI-powered video surveillance in public spaces until March 2025").

[347] *See id.* ("Paris Police Chief Nunes has backed the system, calling it necessary for public safety.").

This potentially conflicts with the EU Artificial Intelligence Act ("EU AI Act") and GDPR.[348] The EU AI Act banned biometric categorizations and the development of facial recognition databases.[349] There is a law enforcement carve-out in public spaces, but the carve-out is limited to narrow situations targeting specific individuals under specific circumstances.[350] The Olympics Law also may run afoul of EU court precedents banning mass surveillance.[351] Outside of the legal considerations, AI facial recognition efforts in the U.S. have already led to racial disparities in accuracy and enforcement.[352] However, the European Court on Human Rights tossed a challenge to French surveillance programs in January of 2025.[353] It remains to be seen whether this AI driven surveillance will be extended yet again.

III. JURISDICTIONAL COMPARISON

Overall, in recent history each jurisdiction has implemented wide-spread mass surveillance practices in the name of national security. The U.S., UK, and France took different paths to arrive at this point. Prior to the 20th century, France's surveillance practices were considerably

---

[348] *See* Mokuena, *supra* note 311 (noting that the surveillance may violate the GDPR due to processing mass biometric data).

[349] Press Release, Artificial Intelligence Act: MEPs Adopt Landmark Law, (Mar. 13, 2024), https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law ("The new rules ban certain AI applications that threaten citizens' rights, including biometric categorisation systems based on sensitive characteristics and untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases.").

[350] Artificial Intelligence Act (Regulation (EU) 2024/1689) art. 5(1)(h).

[351] A list of such cases can be found at Press Unit, Eur. Ct. Hum. Rts., Mass Surveillance: Fact Sheet (2024), https://www.echr.coe.int/documents/d/echr/fs_mass_surveillance_eng.

[352] *See* Kashmir Hill, You Face Belongs to Us (2023) (noting that, when AI facial recognition used by law enforcement identified the wrong person, "[i]n every case, the man wrongfully arrested was black").

[353] *See generally* Press Release, Eur. Ct. Hum. Rts., Court Declares Inadmissible Applications by Journalists and Lawyers Concerning Convention Compatibility of French Intelligence-Gathering Legislation (Jan. 16, 2025) (available at HUDOC).

more comprehensive than either the U.S. or UK. France has a long tradition of collecting data and closely monitoring its citizens.[354] Surveillance author Olivier Aïm adopted this position, noting: "Historically, France has been at the forefront of these issues, in terms of police files and records."[355] Britian was often not far behind. Dr. Gary Girod, an expert in World War I domestic intelligence, explains that "[a]rguably since the Middle Ages, England, then Britain followed a pattern with regards to French social control mechanisms: first they sneered, then they copied."[356] However, France (as far as we know) fell behind the U.S. and UK through the 20th century until recently catching up with the Intelligence Act and Olympics Law.

The chronology of surveillance practices also sheds light on how mass surveillance mechanisms develop. Often war or civil unrest is the catalyst for the development of surveillance infrastructure. In the U.S., this came in the form of the Civil War, WWI, First Red Scare, WWII, Second Red Scare, Civil Rights Movement, and 9/11. In the UK, it was colonial unrest, Irish Fenian bombings, pre-WWI mass hysteria, WWI, WWII, 9/11, and the 2005 London Bombings. In France, it was the French Revolution, Napoleon's reign, the 1870 Franco-Prussian War loss, pre-WWI mass hysteria, WWI, WWII, 9/11, and terrorist attacks in the 2010's. However, it is worth noting that even before the French Revolution there was existing surveillance infrastructure in France. The correlation between these periods of uncertainty and increased surveillance echoes a point made earlier in the paper: people are more willing to give up civil liberties when they are afraid.[357]

Contemporary mass surveillance appears to be faltering in the U.S. but exasperating in the UK and France. The USA Freedom Act in 2015 sought to rein in mass surveillance practices, and there has been little

---

[354] See Kayali, *supra* note 253 ("[France's] tradition of snooping, monitoring and data collection dates way back....").

[355] *Id.*

[356] Girod, *supra* note 173.

[357] *See generally* Sunstein, *supra* note 21.

public development since then. In the UK, the 2016 Snoopers' Charter, 2023 Online Safety Act, 2024 Snoopers' Charter amendments, and extensive CCTV surveillance of London all appear to be going in the other direction. In France, the 2015 Intelligence Act and 2023 Olympics Law similarly increased mass surveillance. Part of this is likely due to public sentiments on mass surveillance programs. As previously mentioned, contemporary Americans tend to be extremely averse to mass surveillance,[358] while British people are much more open to it.[359] Polling of French citizens on the matter does not appear to be readily available, but French civil rights groups have constantly opposed surveillance legislation. It remains to be seen what effect EU precedents and law have on French surveillance practices, but it appears to have done little thus far.

In each of these three jurisdictions, their respective judiciaries have had an insignificant effect on these practices. The U.S. Supreme Court has several lines of cases addressing privacy rights,[360] but has not addressed the parameters governing, or the legality of, mass surveillance. UK courts have been more willing to step in, but the UK legislature continues to increase surveillance mechanisms. EU courts have similarly been critical of the UK's surveillance practices, but to little effect. This is especially true given the UK's decision to leave the EU. In France, courts have cautiously attempted to set the outer bounds of this surveillance with help from EU courts, but it is difficult to say that this has led to decreased surveillance activities. Also, France has seen less strategic litigation related to surveillance practices and has less mechanisms to receive government information.[361] While U.S. citizens can

---

[358] *See supra* notes 43–45 and accompanying text.

[359] *See supra* note 237 and accompanying text.

[360] *Katz v. United States* and its progeny provide for a "reasonable expectation of privacy." There was another string of cases protecting abortion and contraceptives through a "penumbras" of privacy rights in the constitution, but that line of cases has since been overturned. *See* Dobbs v. Jackson Women's Health Organization, 597 U.S. 215 (2022).

[361] *See* Tréguer, *supra* note 299, at 26 ("[R]egarding strategic litigation, itis worth noting that in the French legal system, legal opportunities had been lacking.").

place Freedom of Information Act ("FOIA") requests, the French equivalent "has extremely broad national security exemptions and is generally much weaker."[362]

Lastly, it is important to note a limitation in the chronology of surveillance practices and the accompanying comparison. Historically and inherently surveillance practices have been secretive. Surveillance is effective *precisely because* foreign intelligence can be intercepted without the sender or recipient being aware that the data may be compromised. As such, countries often seek to keep their surveillance outside of the public eye. This means that, often, public knowledge is limited to information that has either been leaked or declassified. Declassification often comes after a considerable amount of time has passed (if it is declassified at all) and does little to inform the public's understanding of contemporary surveillance. The programs included in Snowden's leaks may still continue outside of the public's eye. Or maybe they were replaced by newer and more intrusive programs. Even if the government unequivocally tells its citizens that surveillance has been rolled back, or that they are transparent about current practices, history has shown that it may not be the case.

IV. BALANCING NATIONAL SECURITY AND CIVIL LIBERTIES

The negative impacts of mass surveillance on privacy and civil liberties has already been delineated, but a few more points deserve attention.[363] Mass surveillance has often been weaponized against marginalized groups, protestors, and migrants.[364] Fiscally it has proven

[362] *Id.*

[363] *See supra* Part I.

[364] *See Costs of War: Surveillance*, Brown Univ.: Watson Inst. for Int'l & Pub. Affs. (Sept. 2023), https://watson.brown.edu/costsofwar/costs/social/rights/surveillance ("Mass surveillance has intensified the criminalization of marginalized and racialized groups, from Muslims and Arabs to Latinx immigrant communities to Black and Indigenous organizers, and has

expensive. For example, in 2023 the U.S. allocated $99.6 billion to intelligence.[365] From 2015 to 2019, one NSA program cost taxpayers $100 million and provided no tangible security benefits.[366] The legal grey areas that these agencies have operated in provide little meaningful oversight from legislators, the judiciary, or the general public. Mass surveillance and logging recorded information also threatens the security of that data. Intelligence agencies backdooring or black boxing into telecommunications and social media platforms exposes (and potentially creates) weaknesses that others can exploit.[367] The UK's 2024 Snoopers' Charter amendments go a step further, allowing the government to block security updates. Government's storing data also provides hackers with another potential avenue to access that data and use it for insidious goals such as blackmail.

Yet, the pertinent question remains: does mass surveillance keep us safe? Safety, or at least the appearance of safety, has justified mass surveillance on the grounds of national security. It is also the reason that British people still strongly support surveillance activities. However, there is evidence that mass surveillance actually hinders national security. The Council of Europe Parliamentary Assembly, after the Snowden leaks, cited several studies concluding that "mass surveillance does not appear to have contributed to the prevention of terrorist attacks."[368] This

---

increasingly targeted protest movements such as Black Lives Matter and the movement to stop the Dakota Access Pipeline.").

[365] *See* Michael E. DeVine, Cong. Rsch. Serv., R44381, Intelligence Community Spending Trends (2024) ("For FY2023, Congress appropriated a total of $99.6 billion [for intelligence].") The report also indicates there may be considerable spending that is not publicly available.

[366] *See* Conor Friedersdorf, *The Costs of Spying*, Atlantic (Feb. 28, 2020), https://www.theatlantic.com/ideas/archive/2020/02/costs-spying/607177 ("A new study reveals that from 2015 to 2019, the NSA's call-metadata program cost taxpayers $100 million and provided practically no useful information.").

[367] U.N. GAOR, 51st Sess., U.N. Doc. A/HRC/51/17 at 4 (Aug. 4, 2022) ("[H]acking relies on and exploits the existence of security flaws in computer systems. By keeping such vulnerabilities open, or even creating them, those resorting to hacking may contribute to security and privacy threats for millions of users and the broader digital information ecosystem.").

[368] Council of Eur., Parliamentary Assembly, Comm. on Legal Affs. & Hum. Rts., Mass Surveillance 2 (2015).

report also noted that mass surveillance programs used extensive resources that could have been used to successfully prevent attacks, but were instead diverted to ineffective mass surveillance programs.[369] Independent reviews conducted by U.S government agencies came to the same conclusion: mass surveillance has not made us any safer.[370] Instead, legitimate signs of danger have been lost amongst massive amounts of irrelevant data about millions of citizens worldwide.[371] These reports led to the startling conclusion that "the government's mass surveillance programs operating under Section 215 of the Patriot Act have *never* stopped an act of terrorism."[372] It is important to note that further research into mass surveillance's effectiveness is somewhat limited by the lack of publicly available information.

None of this is to say that foreign intelligence surveillance should be abandoned completely. Foreign intelligence surveillance remains a national defense necessity. This is evident as foreign intelligence has enabled the U.S., UK, and France to thwart terrorist attacks in recent years.[373] However, the surveillance practices of these three countries all

---

[369] *Id.* ("[R]esources that might prevent attacks are diverted to mass surveillance, leaving potentially dangerous persons free to act.").

[370] *See* Elizabeth Goitein, *Rolling Back the Post-9/11 Surveillance State*, Brennan Ctr. for Just. (Aug. 25, 2021), https://www.brennancenter.org/our-work/analysis-opinion/rolling-back-post-911-surveillance-state ("Two independent reviews found that [NSA's bulk collection] program yielded little-to-no counterterrorism benefit.

[371] *See id.* ("[T]here is evidence that overcollection is counterproductive. Multiple government reviews of domestic terrorist incidents have found that agents missed signs of trouble because those signs were lost in the noise of irrelevant data.").

[372] Rachel Nusbaum, *Ignore the Drumbeat of Doom, the NSA's Call Records Program Didn't Stop a Single Terrorist Attack*, Am. C.L. Union (Mar. 4, 2015), https://www.aclu.org/news/national-security/ignore-drumbeat-doom-nsas-call-records-program-didnt-stop-single-terrorist-attack (emphasis added); *see also* Cindy Cohn & Dia Kayyali, *The Top 5 Claims That Defenders of the NSA Have to Stop Making to Remain Credible*, Elec. Frontier Found. (June 2, 2014), https://www.eff.org/deeplinks/2014/06/top-5-claims-defenders-nsa-have-stop-making-remain-credible ("[T]op NSA official John Inglis admitted that the phone records program has not stopped any terrorist attacks aimed at the US....").

[373] *See generally FISA Section 702 Value*, Intel.gov (Feb. 14, 2024), https://www.intel.gov/assets/documents/702%20Documents/FISA_Section_702_Vignettes-20240214_Final.pdf; *see also* Sec'y of State for the Home Dep't, The United Kingdom's Strategy for Countering Terrorism 8 (2018) ("Since last year's Westminster attack, the police and the security and intelligence agencies have successfully foiled a further 12 Islamist plots, and since 2017, have

suffer from flaws related to *proportionality* and *transparency*. The *proportionality* flaw is that these mass surveillance programs are analogous to "scooping up the entire ocean to guarantee you catch a fish."[374] Not only is it impractical, but the time and effort required to implement and monitor these systems diverts resources away from targeted efforts with higher success rates. This ensures that crucial leads, which could prevent attacks, are likely to be missed.

The *transparency* flaw is that these mass surveillance programs have little effective oversight. This allows these foreign intelligence programs to be weaponized against non-foreign actors that do not pose threats to the population (civil rights groups, labor unions, political parties, etc.). Further, it has perpetuated the risk of civil rights abuses against already marginalized groups. These programs that have operated primarily in secret often provide little recourse for errors, and often the victims of those mistakes never get their day in court. Since the implementation of mass surveillance regimes has been ineffective (from a national security standpoint) and harmful (from a privacy and civil liberties standpoint), yet foreign intelligence remains a critical aspect of national security, these programs need to be restructured into a framework that seeks to maximize the benefits while minimizing the drawbacks. The next section provides guidance on how that can be done.

V. RECONCILIATION & THE PATH FORWARD

Throughout the years, mass surveillance has continually taken different forms and has been informed by different rationales. However,

disrupted four extreme right-wing plots."); *see also, e.g.*, Kim Willsher, *French Minister Warns of 'Threat From Within' on Charlie Hebdo Attack Anniversary,* Guardian (Jan. 7, 2025), https://www.theguardian.com/world/2025/jan/07/social-media-fuelling-rising-terror-threat-in-france-says-minister ("Bruno Retailleau said French intelligence had foiled nine planned attacks last year....").

[374] Schneier, *supra* note 1, at 174.

the throughline for all of histories surveillance practices is that innocent people, generally those from marginalized groups, unnecessarily suffer. Surveillance practices and mass hysteria hurt people like Dreyfus and Dr. Ibrahim. Their stories are the ones that we know about – many more have suffered from these policies, but their stories were never told. Dreyfus and Dr. Ibrahim were also vindicated in the end, while countless suffered and were never granted respite. Often, this suffering has been chalked up to a "necessary evil" in order to protect national security.

However, as this paper shows, mass surveillance is ineffective at best and at worst actively hinders national security efforts. Mass surveillance is time consuming and resource intensive, and there is little evidence that it is money and time well spent. Even if AI is integrated into mass surveillance technology, it cannot serve as a substitute for human judgement, and risks perpetuating racism and stereotypes that could further harm marginalized communities.[375] Overall, there is no place in contemporary society for mass surveillance as it was presented in Snowden's leaks. However, this paper proposes four reforms that can maximize the benefits of foreign intelligence surveillance while mitigating the drawbacks.

A. Meaningful Surveillance Oversight

The first proposal is for the development of meaningful oversight throughout the intelligence surveillance process. There should be three branch oversight of intelligence surveillance activities. This was *de jure* enacted through FISA in the U.S. and Snoopers' Charter in the UK but was not followed closely. The legislature should require warrants for surveillance and outline the applicable standards for these warrants.

---

[375] *See* Rachel Fergus, *Biased Technology: The Automated Discrimination of Facial Recognition*, Am. C.L. Union: Minn. (Feb. 29, 2024), https://www.aclu-mn.org/en/news/biased-technology-automated-discrimination-facial-recognition ("Studies show that facial recognition is least reliable for people of color, women, and nonbinary individuals. And that can be life-threatening when the technology is in the hands of law enforcement.").

These standards should require individualized and reasonable suspicion. Surveillance legislation should also provide strict regulations on the scope and duration of data retention. This would include ensuring that collected data is securely stored and should seek to limit mass transfers of data to international governments. There should also be additional whistleblower protections for people that expose government surveillance malfeasance like Edward Snowden. Further, surveillance legislation should have sundown provisions and be subject to continual reviews by the legislature.

The judicial branch should receive warrant requests and make determinations based on the guidelines set by the legislature and, if applicable, case law precedent. This should be a meaningful review, not the rubber stamp process we have seen from FISC. Further, these rulings should be declassified after 2-3 years (or as soon as practicable), barring extraordinary circumstances. This would allow public oversight by providing the standards and rationales employed in making warrant determinations. Also, unlike FISC, the judges sitting on this body should not be elected for a part-time or short-term assignment. They should, like other judges in specialized courts, become subject matter experts in foreign intelligence surveillance warrants. This specialization should foster the speed and knowledge to ensure that government warrants can be decided with the requisite swiftness while carefully adhering to constitutional and legal safeguards.

The executive branch should closely abide by the rules set by the legislature and the judicial system's determinations. The executive branch should never bypass warrant requirements, as both the U.S. and UK have historically done. Nor should the judiciary be left out of the surveillance framework, which France has historically done. The executive branch should also be as transparent as possible. While they may not be able to provide details about individual investigations, they should continue to publish data related to the number of warrants authorized and the effectiveness of the programs. These transparency reports should provide adequate information to inform the public on the breadth

of government surveillance activities. There should also be an ombudsman that receives complaints at any point in the foreign intelligence process. If people are unjustly targeted and harmed, they should be able to seek redress through administrative or judicial bodies.

This process would prevent the most intrusive government programs from being implemented. For instance, the NSA and GCHQ hacking into corporate or telecommunication infrastructure and setting up "black boxes" to monitor mass data would violate these procedural requirements. They would inevitably be surveilling a multitude of individuals without a warrant, and it would not adhere to the legislature's individualized suspicion guidelines. Further, this should also remove the coercive elements we have seen from agencies like the NSA (recall the NSA threatening Yahoo with a $250,000 a day fine for not letting them bug their infrastructure). It would also, in theory, repeal other pieces of legislation or executive orders that have historically permitted mass surveillance. This would include much of the UK's surveillance legislation in recent years. Most importantly, there must be a legislative or judicial mechanism to ensure that the executive branch is adhering to these guidelines. This could take the form of independent committees between those two branches, or another independent watch group, which is mandated to ensure executive branch compliance with surveillance laws. While it would be ideal to trust the executive branch to abide by the law, history has shown that it is insufficient.

In fact, in each of the three countries examined, executive branch discretion historically facilitated the development of mass surveillance infrastructure. The United States saw this with various surveillance efforts conducted by law enforcement agencies post-WWII, such as COINTELPRO and Operation Chaos. More recently, it came in the form of the NSA unilaterally expanding the permissible bounds of the Patriot Act's surveillance, as was noted by the bills' author. There was similarly an absence of legislative mandates for the French DGSE's data collections and transfers under the Lustre agreement, as well as the British GCHQ's mass surveillance. The primary goal of these

executive branch agencies is to gather intelligence and protect national security, which–particularly in the case of mass surveillance–may not always align with protecting the civil liberties of domestic citizens. There needs to be checks and balances against these agencies' discretion, but more importantly, there must be mechanisms to ensure that these intelligence agencies are closely following those requirements.

B. Ensure Privacy Rights

The United States, UK, and France should better protect their citizens' privacy against the government. A suitable place to look for guidance would be the EU. The EU has historically appeared to be a staunch supporter of privacy rights. Article 8 of the ECHR explicitly recognizes privacy as a fundamental right. The Council of Europe Convention 108 goes a step further in ensuring data privacy. There is also relatively robust EU caselaw on mass surveillance.[376] The GDPR is potentially the landmark data privacy legislation globally. The countries discussed in this paper, however, have yet to follow this track.

In fact, in France and the UK things seem to be getting worse, with the UK currently being an archetypical surveillance state and perhaps the most invasive in Europe. Ironically, things seem to be getting better in the U.S., even though the U.S. remains one of the only nations without comprehensive data protections laws nor a constitutional guarantee of privacy. The U.S. should take steps to permanently codify privacy rights in the constitution and therefore provide a constitutional basis for data privacy legislation. For France and the UK, after centuries of surveillance and privacy rights violations, these governments should move towards ensuring that the fundamental liberty of privacy is guaranteed to their citizens. France and the UK are currently moving in the wrong direction, and it is a perfect time to change course.

Another key point is that while many countries constitutionally guarantee the right to privacy, the three countries examined do not. As

[376] *See* source cited *supra* note 351.

previously mentioned, the U.S. analog to constitutional privacy rights is the Fourth Amendment, but the Fourth Amendment does not mention "privacy." Nor does the 1958 French Constitution explicitly provide for privacy rights.[377] However, Article 9 of the French Civil Code does stipulate that "[e]veryone has the right to respect for his private life."[378] France is also bound by Article 8 of the ECHR and EU data protection laws like the GDPR. The UK does not have a codified constitution, but the Human Rights Act of 1998 incorporated Article 8 of the ECHR into UK law.[379] Out of the three countries, France appears to have the most privacy protections due to the ECHR, binding EU precedent, and Article 9 of the French Civil Code. It is possible that these protections contributed to France conducting less mass surveillance throughout the 20th and early 21st century.

It is difficult to determine whether the existence–or absence–of constitutional privacy rights has directly influenced the development of mass surveillance regimes in these three countries. The U.S. has the weakest privacy guarantees, yet FISA theoretically provided the most expansive protections–though rarely implemented in practice. Similarly, the U.S. has had the strongest rollback of mass surveillance in recent years, even without this constitutional protection. Nonetheless, this should not diminish the importance of protecting privacy rights at the highest level, whether that be constitutionally (in the United States and France) or through binding federal legislation (in the UK). This would provide an additional avenue for litigants to challenge mass surveillance regimes or vindicate being unjustly targeted by intelligence agencies.

A constitutional right to privacy may have led to *Clapper v. Amnesty International* being decided differently. Alternatively, the U.S. Supreme Court may have been more willing to accept cases based in

---

[377] *See* Priv. Int'l, U.N. Hum. Rts., Off. of the High Comm'r, The Right to Privacy in the French Republic 5 (29th sess. 2017) ("There is no specific personal data protection or privacy guarantee in the 1958 Constitution.").

[378] Code civil [C. Civ.] [Civil Code] art. 9 (Fr.) ("Everyone has the right to respect for his private life.").

[379] *See generally* Human Rights Act 1998, c. 42 (UK).

mass surveillance if there was a clear constitutional violation occurring. It could also provide a constitutional basis for GDPR-like legislation in the U.S., which could restrict data collection efforts by data processors. This would reduce the available avenues that U.S. intelligence agencies have to gather data on citizens. The presence of this privacy right could also equip litigants in France and the UK with additional weapons to successfully challenge the recent bills expanding mass surveillance. Although success on the merits in litigation is never guaranteed, expanding privacy protections could help balance the scales in favor of those conducting legal challenges to mass surveillance legislation.

Even with a guaranteed right to privacy in these jurisdictions, governments will likely seek exceptions based in national security for foreign intelligence surveillance. As previously mentioned, intelligence can be pertinent to national security but must be accompanied by the appropriate safeguards. Like other fundamental guarantees, there are limited situations where it can be abridged, but only if accompanied by reasonable individualized suspicion, a warrant, and the possibility for redress if errors occur. Ensuring a fundamental right to privacy is a necessary, but not sufficient, step that governments should take to prevent citizens from being arbitrarily subject to surveillance. Because of this, the recommendation for guaranteed privacy rights must be implemented in tandem with the oversight of foreign intelligence proposed in the previous section if indiscriminate mass surveillance is going to be defeated.

C. Protect Civil Liberties in the Face of Fear

In times of war or social unrest, citizens must demand that their governments do not carte blanche violate their civil liberties. Many things can be justified in war–stripping away the natural rights and fundamental liberties of people should not be one of them. Often, in each country, we saw the domestic surveillance of war dissidents and suppression of the media during times of war or unrest. These were inevitably used to target individuals based on affiliations deemed undesirable by the government, such as jews, socialists, laborers, suffragettes,

civil rights activists, and even Catholics. The prospect of war, or terrorism, does not permit the government to intrude on the privacy and free speech rights of its citizens. These intrusions suppress public opinion, silence public discourse, and can cause large segments of the population to suffer. It is on the masses to ensure that they stand up to government oppression, even when they may be afraid.

These emergency powers have also historically outlived the conflicts they were meant to address. In 2013, Edward Snowden was charged with violating the Espionage Act of 1917. This statute was enacted during WWI to protect the war effort, yet was weaponized against a mass surveillance whistleblower almost a century later. The Patriot Act similarly went well beyond its sundown provision after 9/11. The French Olympics Law authorizing AI mass surveillance is still in effect, even though the 2024 Olympics ended seven months ago. Often, in each of the three countries examined, the intelligence agencies were developed or expanded in the face of conflict or terrorism. Instead of these agencies being disbanded or diminished after this unrest ended, often they were reorientated towards domestic citizens with dissenting views on government activities.

Admittedly, there may be times of grave uncertainty that require an expansion of government surveillance efforts. But WWII ended eighty years ago. WWI ended over a century ago. The most recent full-scale civil war in these countries was in the U.S. and ended in 1865. If somehow these countries end up in another period of grave uncertainty, an expansion may be justified, but it should be rolled back as soon as the conflict is over. Each of these three countries are democracies and elected officials are subject to the will of their voters. People should stand up for their privacy rights and other civil liberties and ensure that the government does not overreach.

D. AI and Intelligence Surveillance

The use of AI should be embraced, but *extremely* cautiously. The French Olympics Law is a stereotypical example of AI being used in a

negative manner. There are several steps that can be taken to ensure the ethical use of AI in surveillance activities. Ethical guidelines should be published regarding the collections and analyzation of biometric data through AI. Mass surveillance generally should be abolished, not exasperated by the use of AI. AI-driven surveillance efforts seek to monitor massive segments of the population and make predictions about what people *might do*. From this arises the prospect of arbitrary enforcement and heightened scrutiny on minority groups. It also goes a step further than metadata retention, instead collecting and analyzing the real-time biometric (and personally identifiable) data of millions. AI-driven surveillance undermines the presumption of innocence by deciding guilt before any crime is committed. Few things are more Orwellian than machines constantly tracking you, predicting your next move, and waiting to catch you doing something wrong.

Of course, AI could be strategically employed in a positive manner if the appropriate safeguards are in place. AI facial recognition could be used to help locate a missing person through targeted facial recognition efforts supported by a warrant. It can help identify online human trafficking or financial crimes with speed that humans simply do not possess. It can process terabytes of legally acquired evidence in a criminal case to help identify patterns. AI can also monitor potential cybercrimes and reinforce data security infrastructure. But AI must be used with the appropriate safeguards of individualized suspicion, targeted efforts, and a warrant. Otherwise, the world will see the surveillance state–which each of these three countries are guilty of establishing–reaching powers and breadth never previously thought achievable.

Conclusion

Privacy, and by extension data privacy, should be viewed as a natural and fundamental civil liberty. Human and natural history has shown that this is a fundamental need for humans. In the U.S., UK, and France

we have seen the pendulum of mass surveillance swing back and forth, often being established in times of uncertainty but continuing well into the future. Mass surveillance undermines privacy rights, increases self--censorship, leads to intimidation-induced chilling effects on speech, undermines the freedom of assembly, and reduces trust in the state. All of this is done in the name of national security, but evidence indicates that mass surveillance does not make us safer and actively diverts resources from programs that could have.

There should be meaningful three-branch oversight of foreign intelligence surveillance supported by an ombudsman to receive complaints at any point in the process. Court decisions issuing warrant should be made public as soon as it is feasible to do so. Governments should guarantee the right to privacy, citizens should stand up for their rights even when they are afraid, and the use of AI should be done narrowly and with the appropriate safeguards. Society can achieve adequate foreign intelligence surveillance without abridging civil liberties, but it appears that some countries are headed in the wrong direction: now is the time to change course.

The impact of Schrems case law on the development of the Transatlantic Data Privacy Framework

Maria Miguel Rios[1]

Abstract: This article examines European and American legal policies, focusing on data protection developments, particularly analysing CJEU judgments: Schrems I and II. It discusses the United States' disregard for data subjects' rights and the surveillance conducted by American governmental agencies, leading to the invalidation of previously adopted adequacy decisions. This piece studies the creation of the Transatlantic Data Privacy Framework and its Data Protection Review Court, standing for a deeper convergence of EU and US data protection laws to resolve privacy conflicts amidst technological advancements.

Keywords: Data Protection, General Data Protection Regulation, Schrems, Adequacy Decisions, Transatlantic Data Privacy Framework.

Resumo: Este artigo examina as políticas jurídicas europeias e americanas, concentrando-se nos desenvolvimentos em matéria de proteção de dados, analisando particularmente acórdãos do TJUE: Schrems I e II. Discute o desrespeito dos EUA pelos direitos dos titulares de dados e a vigilância governamental por parte de instituições públicas americanas, contribuindo para a invalidação das decisões de adequação previamente adotadas. Este artigo estuda a criação da *Transatlantic Data Privacy Framework* e do *Data Protection Review Court*, defendendo uma convergência mais profunda das leis de proteção de dados

[1] Data Protection Consultant. Master's in International and European Law at NOVA School of Law and Bachelor's law degree at Universidade Católica do Porto.

da UE e dos EUA para resolver conflitos de privacidade face aos avanços tecnológicos atuais.

Palavras-chave: Proteção de Dados, Regulamento Geral sobre a Proteção de Dados, Schrems, Decisões de Adequação, Quadro Transatlântico de Privacidade de Dados.

1. Introduction

In the globalized world in which we live, where cross-border data-flows reach frenetic rates, the General Data Protection Regulation (GDPR)[2] serves as a key legal instrument regulating international data transfers. The GDPR, which came to repeal the previous Directive 95/46/CE[3] of the European Parliament and of the Council, emphasises the protection of personal data. More importantly, it prohibits personal data transfers to third countries outside of the European Union unless an adequate level of protection is guaranteed.

This research analyses the Schrems I and II[4] cases and examines the latent risks arising from data transfers between Europe and the United States, evaluating whether the new Transatlantic Data Privacy Framework (TADPF) can address these risks. It then turns to the framework's main concerns[5], beginning with the US governments implementation of the framework and its effectiveness in protecting the

[2] 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), *OJ* L 119, 4.5.2016, p. 1-88. (hereinafter, 'GDPR').

[3] 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, OJ L 281, 23.11.1995, p. 31-50.

[4] CJEU, Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650; and Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, ECLI:EU:C:2020:559.

[5] Douwe Korff, *The Inadequacy of the October 2022 New US Presidential Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities*, SSRN, 2022, p. 1-28.

guarantees and safeguards afforded to data subjects under the Charter of Fundamental Rights of the European Union (CFREU).[6] This includes an assessment of the new set of rules and constraints the US government faces and whether these regulatory measures ensure effective oversight of citizens' rights.

2. Schrems Saga

2.1 Schrems I

Austrian activist and lawyer, Maximilian Schrems filed a complaint to the Irish Data Protection Commissioner declaring that Facebook was not adequately protecting his data from American surveillance agencies when transferring it to US servers.[7] The Commissioner declined to investigate the complaint, reasoning that Meta's adherence to the Safe Harbour framework ensured an adequate level of data protection. Nevertheless, Schrems appealed the Commissioner's decision to the Irish High Court, which submitted the case to the Court of Justice of the European Union (CJEU).[8]

The main concerns in the *Schrems v. Irish Data Protection Commissioner*[9] pertained to whether the Commissioner had properly investigated Schrems complaint, adhered to the principle of adequacy, held the necessary powers to carry out such task, and whether the Safe Harbour framework was indeed consistent with EU law.[10]

---

[6] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391-407.

[7] Martin A. Weiss and Kristin Archick, *US-EU Data Privacy: From Safe Harbor to Privacy Shield*, Congressional Research Service, 2016, p. 5-8.

[8] Christina Lam, *Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in Schrems v Irish Data Protection Commissioner*, *Boston College Law Review*, 2017, p. 4-5.

[9] CJEU, Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650.

[10] CJEU, Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, par. 36-67.

In its analysis, the CJEU relied on the Data Protection Directive (DPD) and the CFREU. The Court examined whether US surveillance practices aligned with EU privacy rights, assessing whether arts. 7.º, 8.º, and 47.º of the CFREU were respected and whether individual's rights to privacy, to an effective remedy and fair trial were adequately protected.[11]

The CJEU ultimately declared the Safe Harbour framework invalid,[12] justifying the decision on the grounds that the US did not provide an "adequate level of protection" comparable to that guaranteed by the EU under the DPD.[13] The Court considered that the Safe Harbour unfulfilled the essentially equivalent requirement, because it allowed the US to override the Safe Harbour principles whenever they conflicted with national security or America's public interests. Consequently, the self-certification system, in which a company or organization pledges to follow the Safe Harbour principles, could only serve as a reliable measure of adequacy if mechanisms were in place to identify and sanction non-compliant US companies.

The CJEU found that the absence of rules or legal safeguards limiting government interference with data protection, as well as the lack of an effective judicial remedy,[14] rendered the Irish Data Protection Commissioner assessment insufficient.[15]

2.2 Schrems II

Following the CJEU decision on the Schrems I judgment, the EU and the US engaged in negotiations to conceive a data protection

---

[11] Hendrik Mildebrath, *The CJEU Judgment in the Schrems II Case*, European Parliamentary Research Service, 2020, p. 1-2.

[12] CJEU, Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, par. 100-106.

[13] Art. 25.º of Directive 95/46/EC of the European Parliament and of the Council, 24 October 1995, OJ L 281, 23.11.1995.

[14] Arts. 7.º and 47.º of the Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012.

[15] Christina Lam, *Unsafe Harbor*, *Boston College Law Review*, 2017, p. 7 and 13.

agreement capable of replacing the Safe Harbour.[16] In February 2016, the EU and US revealed they had agreed upon a new regulatory framework for transatlantic data transfers. The new arrangement, known as the Privacy Shield, sought to address the shortcomings of its predecessor by strengthening the protection of EU citizens' personal data.

However, in July of 2020, more than two years after the GDPR had entered into force, Maximillian Schrems reformulated his earlier allegations, prompting the landmark Schrems II judgment in which the CJEU reassessed the validity of the Privacy Shield framework. This time adding that Facebook's use of Standard Contractual Clauses (SCC) as approved by the Commission's SCC Decision and the Privacy Shield, could no longer serve as a valid legal basis for data transfers to the US.[17] Schrems argued that US law continued to require Meta to disclose personal data to governmental surveillance authorities.[18]

The Court held that, for SCCs to provide safeguards essentially equivalent to those guaranteed in the European Union, the level of protection in a given transfer must take into account both the contractual provisions agreed between the EU controller or processor and the recipient in the third country, as well as the extent of access by public authorities to such data and the legal framework of the third country. It further emphasized that it is the responsibility of the data controller or processor settled in the EU to decide on a case-by-case analysis whether the law of the third country provides adequate protection for the transferred data. If the SCC pre-approved by the European Commission, the Binding Corporate Rules (BCR), which are data protection procedures that companies abide to in order to transfer data to enterprises outside of the EU,[19] and other *ad hoc* contractual clauses that have been agreed

---

[16] Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, *German Law Journal*, vol. 18, 2017, p. 2-3.

[17] Sharp Advisors, *Schrems II: A Summary – All You Need to Know*, GDPR Summary, 2020.

[18] Róisín Áine Costello, *Schrems II: Everything is Illuminated?*, *European Papers*, 2020, p. 1048.

[19] European Commission, *Binding Corporate Rules – Corporate Rules for Data Transfers within Multinational Companies*, 2022.

upon by the controller and the processor are not qualified as valid by a national supervisory authority, the transfer shall be suspended or prohibited.[20] Nevertheless, if national supervisory authorities in different member states adopt varying decisions about the adequacy of safeguards in the third country, the GDPR allows such matters to be referred to the European Data Protection Board (EDPB) for an opinion.[21]

The CJEU also decided that the national supervisory authorities should assess complaints and raise concerns, therefore, if they believe the level of protection is inadequate, they may bring these concerns before national courts.[22] Applying the same methodology as when assessing the SCC, the Court reviewed the Privacy Shield Decision, emphasizing that the GDPR ought to be interpreted in conformity with arts. 7.º, 8.º, and 47.º of the EU Charter.[23] The interferences with rights protected in art. 7.º and 8.º of the EU Charter were not *prima facie* unlawful, nevertheless, the US authorities' access and use of personal data was not restricted in a way that satisfied the requirement for essential equivalence.[24]

The CJEU concluded that the Privacy Shield could not establish a level of protection "essentially equivalent" to the CFREU and, therefore, was ruled invalid.[25] The Court determined that US government's use of EU citizens personal data was not narrowed by the proportionality principle, and that the Ombudsperson mechanism did not provide data subjects with an independent body offering enforceable guarantees.[26]

---

[20] Ivan Hmelina, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, University of Zagreb – Faculty of Law, 2022, p. 26.

[21] According to Art. 65.º (1) of the GDPR, the EDPB may adopt a binding decision.

[22] CJEU, Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, ECLI:EU:C:2020:559, par. 143.

[23] Róisín Áine Costello, *Schrems II: Everything is Illuminated?*, *European Papers*, 2020, p. 1050.

[24] Róisín Áine Costello, *Schrems II: Everything is Illuminated?*, *European Papers*, 2020, p. 1050-1051.

[25] CJEU, Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, ECLI:EU:C:2020:559, par. 181.

[26] Data Guidance, 2022, https://www.dataguidance.com/.

2.3 Decision's Outcomes

Many issues culminating in the Privacy Shield's invalidity were "merely echoes of the same criticisms which had doomed Safe Harbour."[27] The invalidation of this adequacy decision accentuated relevant problems regarding policy analysis and negotiation processes within the EU, as well as broader political implications affecting EU-US relation.[28] Given these complexities it is difficult to envision a single legal solution capable of regulating and resolving all disputes. Such a solution is only feasible if the parties involved are willing to seek common ground, even when it challenges their usual policies or practises.[29]

The Privacy Shield represented a vital attempt at reconciliation between contrasting perceptions and legal constructions regarding data protection and privacy. In spite of its inadequacies, the Privacy Shield could have functioned as a paradigm for safeguarding international data transfers. For this to have happened, the US should have acted beyond formalistic measures and prioritize data subjects' rights. However, because data protection law cannot by itself resolve national security problems, it is essential to reform intelligence-gathering practices with an emphasis on transparency.

Apart from the challenges revealed by the ruling, Schrems II represented a turning point for data protection and fundamental rights, with its judgement impacting transatlantic economic relationships valued at approximately 7 trillion dollars. As a result, the CJEUs ruling produced repercussions beyond initial expectations. Although, the relationship between Chapter V of the GDPR and the Charter have been clarified, the Court's decision has nonetheless diminished the GDPRs

---

[27] Róisín Áine Costello, *Schrems II: Everything is Illuminated?*, *European Papers*, 2020, p. 1059.

[28] Francesca Bignami, *Schrems II: The Right to Privacy and the New Liberalism*, *Verfassungsblog*, 2020, p. 1-7.

[29] Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, *German Law Journal*, vol. 18, 2017, p. 34-38.

attractiveness as a model for other countries to adopt.[30] To develop a more effective system for regulating data transfers, other jurisdictions must clearly define their regulatory framework and evaluate competing models from a broader perspective, thereby enhancing the protection of citizens' rights in international operations.[31]

3. Transatlantic Data Privacy Framework

3.1 The American Data Protection Model vs EU model

The data protection panorama worldwide has changed significantly in the last few years due to ground-breaking judgments, as previously discussed, that challenged existing data protection regulations, revealing them to be inadequate or disproportionate.

The American data protection model has suffered several reforms in the last decades, mainly to reach equivalent protection to the European prototype. With the GDPR setting a high global standard for data protection, the US' approach to privacy and protection of fundamental rights had to evolve, imposing stricter requirements on both public authorities and private entities.[32] Nevertheless, this attempt to produce a similar data framework revealed, and continues to reveal, numerous differences and misunderstandings, which are discussed in the following sub-chapter.

The US polarity regarding EU law is largely shaped by the absence of a comprehensive and binding framework governing data protection. The American blueprint for data protection is based on separate legislative models and is often described as "sectoral", since only certain

[30] Christopher Kuner, *Schrems II Re-Examined*, *Verfassungsblog*, 2020, p. 1.

[31] Róisín Áine Costello, *Schrems II: Everything is Illuminated?*, *European Papers*, 2020, p. 1059.

[32] Cristina Pop, *EU vs US: What Are the Differences Between Their Data Privacy Laws?*, *Endpoint Protector Blog*, 2022.

federal states provide safeguards.[33] Historically, the US, often regarded as the "leader of the free world" has prioritized freedom of expression and information over privacy and overall security. As the home of one of the world's largest economies and a key technology hub, the US has favoured corporations through an overly capitalistic approach, placing profit above individual rights.[34]

In contrast, the EU has taken a unified approach, epitomized by the GDPR[35] and reinforced by key CJEU rulings that uphold fundamental rights. The EU's take on privacy is deeply shaped by its historical and political context, resulting in strong resistance to governmental intrusion. This mindset, shaped by experiences with authoritarian regimes and socialist measures[36] has fostered a culture of privacy awareness among citizens.[37]

Cultural disparities between the EU and the US[38] continue to shape their views on data protection and privacy.[39] Yet, growing public concern in the US has recently prompted a shift leading to a renewed focus on privacy and development of stronger data protection measures.

3.2 The Need for its Creation

The world is becoming increasingly interconnected, marked by rising volumes of data and a more complex information ecosystem,

---

[33] Daniel R. Leathers, *Giving Bite to the EU-US Data Privacy Safe Harbor: Model Solutions for Effective Enforcement*, *Case Western Reserve Journal of International Law*, vol. 41, 2009, p. 197.

[34] Paul J. Watanabe, *An Ocean Apart: The Transatlantic Data Privacy Divide and the Right to Erasure*, *Southern California Law Review*, 2016, p. 1112-1126.

[35] Art. 5.º of the GDPR.

[36] Joel Araújo Alves, *The New Model of European Personal Data Protection: From Hetero-regulation to Publicly Regulated Self-Regulation*, Almedina, 2021.

[37] Frits Willem Hondius, *Emerging Data Protection in Europe*, North-Holland Publishing Company, 1975, p. 282.

[38] Francesca Bignami, *European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, *Boston College Law Review*, 2007, p. 609-698.

[39] Paul M. Schwartz and Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, *Georgetown Law Journal*, vol. 106, 2017, p. 122.

creating a pressing need for robust protection and regulation. Today, companies must navigate an intricate web of requirements, as an expanding array of rules demands careful attention to how citizens' personal data is collected, stored, and used.

Following the failure of the Privacy Shield to provide equivalent protection, the Commission and the US recognized the need to develop a system that would meet the protection standards required by the Charter and EU data protection law.[40] The creation of a new framework to regulate transatlantic data transfers was necessary to limit the US intelligence agencies' access to personal data, since the premise of "protection of national security" can be quite vague, having no clear requirements or boundaries.[41]

To achieve this, it was essential to implement backdrop, that provided effective oversight of privacy and data protection, including entities capable of monitoring, adjudicating, and sanctioning government or private actors, as well as review and redress mechanisms that protected citizens' rights.[42] Against this backdrop, a transatlantic adequacy decision has been long awaited to resolve the uncertainty businesses have faced over the past years due to the absence of clear and well-defined guidelines.[43]

3.3 Analysis of President's Biden Executive Order

In order to protect its citizens and allies from potential security threats and to uphold the US national security objectives, the US issued Executive Order (EO) 14086 on October 2022. This Order lists out three

---

[40] Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, *German Law Journal*, 2017, p. 34.

[41] Juan Fernando López Aguilar, *Draft Motion for a Resolution to Wind Up the Debate on the Statement by the Commission on the Adequacy of the Protection Afforded by the EU-US Data Privacy Framework*, European Parliament, 2023.

[42] Ivan Hmelina, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, University of Zagreb – Faculty of Law, 2022, p. 31.

[43] Cristina Pop, *EU vs US: What Are the Differences Between Their Data Privacy Laws?*, *Endpoint Protector Blog*, 2022.

essential principles governing signals intelligence. Firstly, section 2 (a) defines that intelligence services should be authorized by "statute, executive order, or presidential order" and always follow the American constitution. It must regard the appropriate safeguards to "ensure that privacy and civil liberties are integral considerations in the planning and implementation of such activities," considering the necessity and proportionality of the intelligence activity. Therefore, establishing a "rigorous oversight" to assure that its principles are followed.

Section 2 (b) embodies the objectives and non-objectives of signal intelligence activities, as well as the process for validation of surveillance activities considering the listed purposes. Section 2 (c), on the other hand, explains that the data collection can be targeted and customized. While targeted collection should be prioritized, bulk data collection may still occur under more limited circumstances, provided no alternative means of obtaining the data exist.

Overall, these procedures are evaluated by the Privacy and Civil Liberties Oversight Board (PCLOB), an independent US government organ tasked with ensuring that privacy and civil rights are adequately protected while preventing terrorist activities.[44]

Nevertheless, despite this EO establishing stricter requirements for government's intelligence activities, it remains crucial to assess whether these measures are compatible with EU law and the European Essential Guarantees (EEG) on surveillance. These guarantees set obligations and duties for the government authorities, requiring that: "A. Processing should be based on clear, precise, and accessible rules; B. The necessity and proportionality of the measures in relation to the legitimate objectives pursued, such as threats or potential risks to national security, must be demonstrated; C. An independent oversight mechanism should be in place; and D. Effective remedies must be available to the individual."[45]

---

[44] US Privacy and Civil Liberties Oversight Board, *https://www.pclob.gov/*.

[45] European Data Protection Board, *Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures*, EDPB, 2020, p. 1-15.

When analysing the presidential EO, it is not explicit nor comprehensible if its application can be modified by the President at any given time, thereby creating significant legal uncertainty. This uncertainty is compounded by the EO allowance for broad-scope bulk collection in exceptional circumstances.[46] and by the fact that the redress mechanism it outlines is neither fully "autonomous" nor "free from hierarchical constraint",[47] as discussed in detail in Chapter 3.5. Thus, the EO falls short of providing an equivalent to European standards with regard to impartiality, independence, and legal safeguards in the handling of data by American surveillance agencies.[48]

3.4 Data Protection Review Court

The Data Protection Review Court (DPRC) was first authorized on October 7, 2022, under President Biden's EO 14086.[49] This EO enacted commitments made by the US as part of the TADPF in retaliation for the CJEU ruling invalidating the Privacy Shield adequacy decision. The goal of the DPRC was to establish a two-tier redress mechanism to review complaints by individuals filed through appropriate public authorities in designated foreign countries or regional organizations defined as a qualifying state by the Attorney General (AG) under section 3(f) of the EO.

The first-tier mechanism is constituted by the process of investigation, review, and determination by the Civil Liberties Protection Officer (CLPO) of whether a violation took place and if the appropriate remediation in response to a qualifying complaint was taken. The second-tier

---

[46] Elizabeth Goitein, *The Biden Administration's SIGINT Executive Order, Part I: New Rules Leave Door Open to Bulk Surveillance*, *Just Security*, 2022.

[47] Ashley Gorski, *The Biden Administration's SIGINT Executive Order, Part II: Redress for Unlawful Surveillance*, *Just Security*, 2022.

[48] Douwe Korff, *The Inadequacy of the October 2022 New US Presidential Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities*, SSRN, 2022, p. 21.

[49] The White House, *Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities*, 2022.

mechanism allows a complainant or a member of the intelligence community to request a review by the DPRC, which adjudicates legal disputes arising from CLPO determinations and evaluates whether the appropriate remedies were correctly applied in accordance with the EO.

The DPRC operates through a panel of six or more judges appointed by the AG who have not been employed by the US government in the preceding two years. During their duties, which can extend to four-year renewable terms, they cannot exercise any functions within the US government. When a complaint is solicited to be reviewed, a three-judge panel of the DPRC is dispatched by the Office of Privacy and Civil Liberties (OPCL) and convened by the presiding judge.[50] The DPRC panel will select a Special Advocate who, in accordance with section 3(d)(i)(C) of the EO, will assist the panel by representing the complainant. The AG elects the special advocates together with the Secretary of Commerce, the Director of National Intelligence, and the Privacy and Civil Liberties Oversight Board (PCLOB), where they nominate two individuals to serve as Special Advocates for two-year renewable terms, choosing citizens that have not been government employees in the past two years and who possess expertise in data protection and national security.

A complainant wishing to request a review by the DPRC must submit their request within sixty days of being notified of the OPCL's determination. The application for review should be submitted through the appropriate authority in a qualifying state. Also, an element of the Intelligence Community may request a review of a CLPO decision by submitting a review application to the OPCL. To protect sensitive information, the DPRC, Special Advocate, and OPCL are prohibited from providing the complainant with any details regarding the existence, review, or outcome of a review request submitted by an intelligence community member.[51]

---

[50] US Department of Justice, *Data Protection Review Court* – Final Rule, 2022, *https://www.justice.gov/.*

[51] US Department of Justice. *Data Protection Review Court – Final Rule,* section n. .º 201.6. *https://www.justice.gov/.*

The DPRC needs to review the complaints through an independent and impartial lens. Therefore, judges are not subject to day-to-day supervision by the AG, except in cases of "misconduct, malfeasance, breach of security, neglect of duty, or incapacity." At the same time, DPRC panels are granted access to classified information when necessary to reach a decision. The Court's decisions are final and binding, and the individual complainants will only be notified if any violations are identified. The DPRC procedural rules may be amended by a majority of judges, a quorum of six, if deemed necessary and appropriate to further DPRC's objectives.

3.5 Main Concerns

3.5.1 US Government

The US federal government and its supporting body of jurisprudence are commonly known for not providing adequate protection for personal data. The absence of legislation to protect citizens' rights has enable US intelligence agencies to overuse their powers. Despite several attempts to regulate American activities through court rulings and executive orders, significant gaps and compliance issues persist.

Although the TADP framework marks a significant step forward in regulating international data transfers, the US government still has to ensure that it fulfils what was agreed upon. After not following the Safe Harbour and the Privacy Shield adequacy decisions, the federal government has gained a reputation for not performing accordingly.

The TADPF introduced new principles and measures that limit US intelligence agencies' access to data while still safeguarding national security. Concerns remain, however, regarding whether the assessment of citizens' personal data is consistently necessary and proportionate, and to what extent the oversight mechanism will be enough. The first--tier mechanism involves the CLPO investigating, reviewing, and determining whether a violation occurred and whether appropriate remediation was taken in response to a qualifying complaint.

Nevertheless, the CLPO's primary objective is the prevention of terrorist offenses which may involve analysing and retaining citizens personal data in anticipation of potential criminal activity.

Furthermore, the second-tier mechanism allows a complainant or a member of the intelligence community to request a review by the DPRC of the CLPO determinations. However, it is likely to be ineffective, as the outcomes are not made public or shared with the complainant. Citizens who have been subject to surveillance but not implicated in any of the threats addressed by the TADPF remain uninformed about ongoing investigations, raising profound concerns regarding transparency and accountability.

Besides, the DPRC is composed of judges appointed by the AG, and the review process begins with an investigation conducted by the Office of the Director of National Intelligence (ODNI), with both entities situated within the intelligence community. This close connection to the government raises concerns regarding the impartiality of the process.

Another potential issue with impartiality arises from the judges' renewable four-year terms, which may incentivize them to render decisions favouring the government to secure reappointment. Also, because the President has unlimited authority to remove judges from the Court, they may feel indirectly pressured to align their decisions with the government's position.

Under sections 2 (ii) (C) and 2 (i) (B)[52] the US President is granted a power that has generated significant controversy, namely, the authority to update the list of national security objectives, allowing bulk data collection and signal intelligence activities when deemed necessary for security purposes. Such authority raises concerns regarding secrecy, as well as lack of independence, impartiality and transparency in the US government's regulation of intelligence activities.

---

[52] US Department of Justice. *Data Protection Review Court – Final Rule,* section II and 201.10, p. 4 and 16. *https://www.justice.gov/.*

Even if the US government would argue that the national security objectives list is proportionate and necessary, the principles referenced are not assessed under international law. When publishing the EO, the AG and the US Department of Justice clarified that it is to be interpreted "in light of US law and the US legal tradition, and not any other source of law." Moreover, the President has the authority to update and publish this list, potentially creating rules that differ from the publicly available version, which casts doubt on the transparency and reliability of the information provided to the public.[53]

3.5.2 Rights, Guarantees, and Safeguards of Citizens

The TADP framework, overall, seems to respect the EEG and the CJEU intake on arts. 7.º, 8.º, 47.º, and 52.º of the CFREU.[54] However, when assessing the TADPF, particularly the DPRC, as detailed in the EO several concerns regarding fundamental rights emerge. Art. 7.º of the CFREU is compromised because the EO permits bulk data collection, infringing the right for private life by allowing personal data to be gathered without notifying the data subject. This practise prevents citizens from taking action or filing complaints to obtain an adequate remedy, thereby breaching art. 8.º of the CFREU, which guarantees the "protection of personal data", and further contributes to non-compliance with art. 52.º of the CFREU, which enshrines the principles of proportionality and necessity, particularly since the EO requires that DPRC regulations be assessed solely under US law[55], thus precluding application of the proportionality and necessity tests established under EU law.[56]

---

[53] Ashley Gorski, *The Biden Administration's SIGINT Executive Order, Part II: Redress for Unlawful Surveillance*, *Just Security*, 2022.

[54] Ivan Hmelina, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, University of Zagreb – Faculty of Law, 2022, p. 26-27.

[55] Par. 128 of the TADPF.

[56] Elizabeth Goitein, *The Biden Administration's SIGINT Executive Order, Part I: New Rules Leave Door Open to Bulk Surveillance*, *Just Security*, 2022.

3.5.3 Failure to Regulate

The TADPF was developed in response to the shortcomings and gaps identified in the adequacy decisions following the Schrems judgements. By addressing areas that previously lacked guidance, the framework provides a higher level of protection for data subjects' personal data. The TADPF is presented as a solution to resolve the longstanding challenges in transatlantic data transfers that persisted over the past decades. The two-tier redress mechanism is expected to provide a structured system for resolving a wide range of complaints and surveillance- related issues that might occur in the near future. Yet, uncertainty remains as to whether the framework will effectively monitor, analyse, and address all such challenges. Even so, it introduces tools and instruments that allow decisions to be reviewed and adjusted if necessary, limiting the likelihood of repeating the shortcomings identified in the Schrems judgments.

The first review of the adequacy decision was conducted one year after it came into force to verify whether legal safeguards, oversight mechanism, and redress procedures had been fully implemented and were effective in practice. The Commission, in consultation with the EDPB and EU member states, will determine the frequency of subsequent reviews, which will occur at least every four years. In theory this review policy provides a practical mechanism to address any regulatory shortcomings or procedural issues that may arise, though it remains to be seen whether it will do so effectively in practise.

4. Conclusion

Over the past decades, the American data protection model has consistently struggled to ensure sufficient protection to data subjects' rights, particularly in cross-border personal data transfers. The Schrems judgments seem to have initiated a movement to supervise these transfers and protect citizens' fundamental rights against surveillance

practices. After the failure of both the Safe Harbour and the Privacy Shield adequacy decisions, the EDPB (combined with the US Government), the European Commission, and the European Parliament, searched for a long-term alternative to regulate international data transfers.

The EU and US wanted to remove the uncertainty, higher costs, and challenges that both businesses and the world were facing after the invalidation of the Privacy Shield. Despite the discrepancy of views regarding data protection, the goal was to create a practical framework enabling companies to implement adequate standards, thereby ensuring that citizens' personal data was not being compromised.

The creation of the TADPF represented another strategic push for the US to adopt measures according to European principles,[57] viewing the regulation of personal data as a means to reach a compromise between EU standards and those of other countries. The elaboration of the adequacy decision introduced additional mechanisms to legitimize transatlantic data transfers. This allowed self-certified companies that bind to the EU-US TADPF to receive EU citizen's personal data without having to assure additional safeguards.

The adequacy decision was developed based on EU law, specifically on the GDPR and the CJEU's rulings in the Schrems judgments, and is intended to be considered along with the EO 14086, which serves as a complementary legislation.

The TADPF most innovative addition was the redress mechanisms. The first-tier mechanism involves investigation and review by the CLPO to determine whether an individual's rights were violated by intelligence agencies and whether appropriate remediation was provided in response to a qualifying complaint. The second-tier mechanism allows the DPRC to review CLPO determinations and assess whether the appropriate remediation has been implemented.

---

[57] Paul J. Watanabe, *An Ocean Apart: The Transatlantic Data Privacy Divide and the Right to Erasure*, *Southern California Law Review*, 2016, p. 1139.

The role of the DPRC however, remains controversial, as its procedural rules cannot be evaluated under international law, since the EO explicitly stipulates that only American law may govern its assessment. Also, the President's direct influence on the Courts decision-making process exemplified by the unrestricted power to remove judges, in coordination with the Department of Justice, reveals a lack of impartiality in this supposedly independent authority. Such powers highlight an absence of transparency and independence in the functioning of the DPRC.[58]

Nonetheless, as mentioned by the EU Justice Commissioner Reynders in a press conference, "with the adoption of the Adequacy Decision, personal data can now flow freely and safely from the EU to the US without further conditions or authorizations," regarding potential challenges the Commissioner stated that "the Commission is very confident to try to, not only implement such an agreement but also to defend all procedures that it will have to face."

With this, although it is difficult to view the framework as a definitive solution for regulating international data transfers between the EU and the US, it may represent the most effective option for ensuring compatibility and facilitating communication between different data protection systems. When combined with other legal provisions and formal mechanisms, it is likely to offer real protection for international data transfers if its safeguards are properly implemented.[59] Furthermore, by increasing transparency in their activities, governmental organizations can enhance the likelihood that fundamental rights and freedoms are respected and ultimately guaranteed.[60]

Recent developments, notably the establishment of the TADPF,

---

[58] Elizabeth Goitein, *The Biden Administration's SIGINT Executive Order, Part I: New Rules Leave Door Open to Bulk Surveillance*, *Just Security*, 2022.

[59] Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, *German Law Journal*, 2017, p. 33.

[60] Paul Breitbarth, *A Risk-Based Approach to International Data Transfers*, *European Data Protection Law Review*, 2021, p. 549.

may pave the way to a new American norm[61]. Still, after an extensive analysis of legislative efforts, case laws and procedural rules, it seems unlikely that either the US or EU law can be resolved through a clear--cut approach. Nevertheless, the two systems are gradually moving towards a mutually accepted reasoning. It is possible that American and European Court's will converge in their assessments when evaluating data protection cases involving similar facts.[62]

The TADPF enforcement mechanisms may prove sufficient to guarantee the protection of personal data transfers.[63] The future of international data protection law could be successfully shaped through sustained EU–US engagement grounded in harmonization, coordination, cooperation, and transparency. By rethinking privacy in light of innovative structures, data protection law can evolve to meet global challenges. Undoubtedly, the TADPF adequacy decision represents a fresh start for resolving data protection and privacy conflicts.[64] After all, "privacy is important inasmuch as it protects the liberty that is its foundation, and there is no reason and no need to protect privacy if liberty is not in danger."[65]

Considering the rapid pace at which technological developments are shaping society, data protection and its regulation must be contemplated as a living instrument. The issues and primary concerns at stake today might not be relevant in a few years. Nonetheless, the demand for more robust data protection standards is expected to continue rising.

---

[61] Shannon Togawa Mercer, *The Limitation of European Data Protection as a Model for Global Privacy Regulations*, *Cambridge University Press*, 2020, p. 20-25.

[62] Erdem Büyüksağiş, *Towards a Transatlantic Concept of Data Privacy*, *Fordham Intellectual Property, Media & Entertainment Law Journal*, vol. 30, 2019, pp. 139-221.

[63] Daniel R. Leathers, *Giving Bite to the EU-US Data Privacy Safe Harbor: Model Solutions for Effective Enforcement*, *Case Western Reserve Journal of International Law*, vol. 41, 2009, p. 242.

[64] Paul M. Schwartz and Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, *Georgetown Law Journal*, vol. 106, 2017, p. 179.

[65] Avner Levin and Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, *University of Ottawa Law & Technology Journal*, vol. 2, 2005, p. 359-395; and Emmanuel Pernot-Leplay, *EU Influence on Data Privacy Laws: Is the US Approach Converging with the EU Model?*, *Colorado Technology Law Journal*, vol. 18.1, 2020, p. 36.

Ultimately, data protection is a concern that goes beyond the legal domain and as recognition of its importance grows, it may pave the way for the creation of a global regulatory framework that not only aligns EU and US laws but also promotes convergence with the rest of the world.[66]

[66] Emmanuel Pernot-Leplay, *EU Influence on Data Privacy Laws: Is the US Approach Converging with the EU Model?*, *Colorado Technology Law Journal*, vol. 18.1, 2020, p. 48.

II – COMENTÁRIOS DE JURISPRUDÊNCIA/ /NOTAS DE INVESTIGAÇÃO

AI and healthcare
A case of an omelette without eggs?

Francisco Arga e Lima

Introduction

The adoption of artificial intelligence ("AI") in the healthcare sector has the potential to improve medical diagnosis and treatment, thereby improving public health efforts, equitable access to care and ultimately contributing to the advancement of the public good.

However, the training of these AI models depends on personal data gathered, for example, during patient interactions with healthcare services. The processing of this information is subject to heightened protection under the General Data Protection Regulation ("GDPR"), creating significant limitations to AI developers in processing it in a way that respects the principle of lawfulness.

It is with these limitations in mind that this essay aims to bring clarity on a possible way forward for AI developers to lawfully process health data in the training process of their models.[1]

Health data and the GDPR

In order to have a complete overview of the steps AI developers need to adopt, it is important to clarify what makes data personal, as well as the concrete limitations derived from the principle of lawfulness to the processing of health data.

[1] In this regard, we will limit ourselves to Article 9(2) and 6(4) of the GDPR, assuming AI developers act as controllers. Considerations over applicable legal bases under Article 6(1) of the GDPR will, therefore, not be the main scope of this essay.

1. Personal data and health data

The GDPR defines personal data in Article 4(1) as all forms of data, whether objective or subjective,[2] whose content, purpose or effect has a direct or indirect connection to an individual.[3] Importantly, this individual needs to be identified or, at least, identifiable. Here, the GDPR adopts a contextual approach, where the main criteria for identifiability are the means – i.e. additional information held by third parties – reasonably likely to be used to identify the data subject.[4] Within this broad concept, Article 4(15) of the GDPR sets out a specific classification for data concerning health, which is to be interpreted as including more than purely medical data, i.e. hospital admission records, appointment schedules, invoices for healthcare services, and social security numbers.[5] Recital 35 GDPR also broadens its temporal dimension, encompassing personal data about past, present, and future health conditions.

An important requirement for the definition of personal and health data is, therefore, the need for the information to relate, at the very least, to an identifiable individual. This brings us to the distinction between personal data and non-personal data – in particular anonymised data – important since the GDPR does not apply to situations where the re-identification of the data subject becomes practically impossible or excessively difficult. Two caveats must, however, be made.

First, assessing anonymisation involves evaluating whether reasonable means (i.e. financial, technical, and human resources) exist to either (1) re-identify individuals from data held by a controller or (2)

---

[2] CJEU, Case C-434/16, Nowak, para. 34; CJEU, Case C-413/23 (Opinion Advocate-General), EDPB v. SRB, para. 29.

[3] CJEU, Case C-434/16, Nowak, para. 35; CJEU, Case C-413/23 (Opinion Advocate-General), EDPB v. SRB, para. 30; CJEU, Joined cases C-92/09 and C-93/09, Schnecke, para. 53.

[4] CJEU, Case C-582/14, Breyer, para. 43 and 46.

[5] EUROPEAN DATA PROTECTION SUPERVISOR, Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the Application of Patients' Rights in Cross-Border Healthcare (2009), para. 15.

access the information necessary to re-identify the data subject.[6] In this context, a line has to be drawn between anonymised data and pseudonymised data. According to guidance from the European Data Protection Board ("EDPB"), pseudonymisation involves replacing identifying information with pseudonyms.[7] Still, pseudonymised data are viewed as personal data since the pseudonymisation process is reversible,[8] through (1) the identification of the data subject, (2) reconnection of pseudonymised data to the original data, or (3) recreation of original data via additional information held by the controller.[9] By contrast, anonymisation is not reversible through reasonably available methods.[10] Thus, for personal data to be considered anonymised, controllers must assess what trumps their anonymisation efforts, considering not only their capabilities but also third-parties' and technological progress.[11]

Second, while anonymised data itself escapes the GDPR's scope, the anonymisation process does not.[12] In this regard, anonymisation operations, generally further processing activities, must respect Article 6(4) of the GDPR. This is in most cases not too high of a standard to achieve, as confirmed by the Article 29 Working Party ("WP29").[13]

---

[6] CJEU, Case C-582/14, Breyer, para. 46; Recital 26 GDPR.

[7] TOSONI, L.; "Article 4(5). Pseudonymisation". In: The EU General Data Protection Regulation (GDPR): A Commentary. Kuner, C., Bygrave, L. A., Docksey, C. (eds). Oxford: Oxford University Press (2020), p. 135; ARTICLE 29 WORKING PARTY, Opinion 05/2014 on Anonymisation Techniques (2014), p. 20; CJEU, Case C-413/23 (Opinion Advocate-General), EDPB v. SRB, para. 47.

[8] EUROPEAN DATA PROTECTION BOARD, Guidelines 01/2025 on Pseudonymisation (2025), p. 11.

[9] Idem. See also CJEU, Case C-413/23 (Opinion Advocate-General), EDPB v. SRB, para. 47-57.

[10] ARTICLE 29 WORKING PARTY, Opinion 05/2014 on Anonymisation Techniques (2014), p. 24.

[11] CJEU, Case C-582/14, Breyer, para. 43.

[12] ARTICLE 29 WORKING PARTY, Opinion 05/2014 on Anonymisation Techniques (2014), p. 7.

[13] Idem.

2. The principle of lawfulness and health data

When the development of AI models requires the processing of personal data, the applicability of the GDPR and the need for a legal basis is, therefore, unequivocal. Hence, the path forward will depend on whether AI training is the initial or a subsequent processing purpose.[14]

2.1. Personal data is collected for AI training purposes

If personal data is initially collected for AI training, given the sensitivity inherent to health data, developers will require an exception under Article 9(2) of the GDPR to apply.[15] Generally, two options are put forward.

Firstly, Article 9(2)(a) of the GDPR allows the processing of health data based on the explicit consent of the data subject.[16] Despite being theoretically possible to obtain it, consent has clear practical problems, due to, i.e. information and explicitly requirements, as well as the need to ensure a proper right to withdraw consent.[17]

The second option comes through Article 9(2)(e) of the GDPR, that allows for the processing of special categories of data if the data subject had manifestly made them public. However, here we also have practical difficulties, since controllers will need to demonstrate the data subject's intentionality in doing so, which is hard to achieve at scale. In fact, it must be evident that the data subject intended to make this information public on a case-by-case basis, considering i.e. the medium used

---

[14] EUROPEAN DATA PROTECTION BOARD, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, p. 6.

[15] GEORGIEVA, L., KUNER, C.; "Article 9. Processing of special categories of personal data". In: The EU General Data Protection Regulation (GDPR): A Commentary. Kuner, C., Bygrave, L. A., Docksey, C. (eds). Oxford: Oxford University Press (2020), p. 376-377.

[16] Idem.

[17] Idem.

to disclose the information, its standards settings, accessibility, etc.[18]

Given these challenges, the GDPR provides another route. This comes through Article 9(2)(j), where the GDPR allows for the processing of health data for scientific research purposes.[19] Three cumulative conditions determine the applicability of this exception: (1) the processing purposes must relate to scientific research, excluding, i.e. the subsequent commercial exploitation of the AI model;[20] (2) it must be based in EU or national law; and (3) the processing must be limited to what is strictly necessary, with suitable safeguards to mitigate risks towards data subjects.[21]

2.2. AI training is a subsequent data processing purpose

If AI training is a subsequent purpose from the one for which health data was initially collected, the GDPR allows it if it is compatible with the initial purpose.[22]

Here, a joint reading of Articles 5(1)(b), 6(4), and 9(2)(j) of the

---

[18] EUROPEAN DATA PROTECTION BOARD, Guidelines 8/2020 on the Targeting of Social Media Users (2020), p. 34–36.

[19] VERHENNEMAN, G.; "AI and Healthcare Data". In: The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence. Smuha, N. A. (ed). Cambridge: Cambridge University Press (2025) Cambridge, p. 312; KOTSCHY, W.; "Article 6. Lawfulness of processing". In: The EU General Data Protection Regulation (GDPR): A Commentary. Kuner, C., Bygrave, L. A., Docksey, C. (eds). Oxford: Oxford University Press (2020), p. 342.

[20] SVANBERG, C. W.; "Article 89. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes". In: The EU General Data Protection Regulation (GDPR): A Commentary. Kuner, C., Bygrave, L. A., Docksey, C. (eds). Oxford: Oxford University Press (2020), p. 1246.

[21] GEORGIEVA, L., KUNER, C.; "Article 9. Processing of special categories of personal data". In: The EU General Data Protection Regulation (GDPR): A Commentary. Kuner, C., Bygrave, L. A., Docksey, C. (eds). Oxford: Oxford University Press (2020), p. 381.

[22] An important discussion is whether compatible further processing still requires a new legal basis under Article 6 and Article 9 of the GDPR, if applicable. Although this is a central topic also for the training of AI in healthcare, since the common denominator for Article 6(4) and Article 9(2) is scientific research, we find that this discussion does not bear significant consequences for the discussion in this essay. See also VERHENNEMAN, G.; "AI and Healthcare Data". In: The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence. Smuha, N. A. (ed). Cambridge: Cambridge University Press (2025) Cambridge, p. 312;

GDPR leads us to conclude that this can be the case for scientific research. However, the assessment under Article 6(4) GDPR is still required,[23] with special attention to the sensitive nature of health data, as required by Article 6(4)(c) of the GDPR.[24] Additionally, and under Article 89(1) of the GDPR, this requires additional safeguards to be put in place (i.e. pseudonymisation and anonymisation) to minimise risks towards data subjects.[25]

2.3 Scientific research under EU law

We thus arrive at scientific research as a common denominator for the processing of health data for AI training purposes, which is broadly defined by the GDPR as including technological development and privately funded research.[26-27] This way, to qualify as scientific research, the activity must align with two core elements:

a. Firstly, there must be a systematic activity based on the collection and analysis of structured data aimed at increasing a *corpus* of knowledge.[28] Additionally, the EDPS, looking at the

---

[23] KOTSCHY, W.; "Article 6. Lawfulness of processing". In: The EU General Data Protection Regulation (GDPR): A Commentary. Kuner, C., Bygrave, L. A., Docksey, C. (eds). Oxford: Oxford University Press (2020), p. 342.

[24] ARTICLE 29 WORKING PARTY, Opinion 03/2013 on Purpose Limitation (2014), p. 25.

[25] KOTSCHY, W.; "Article 6. Lawfulness of processing". In: The EU General Data Protection Regulation (GDPR): A Commentary. Kuner, C., Bygrave, L. A., Docksey, C. (eds). Oxford: Oxford University Press (2020), p. 342-343.

[26] Recital 159 GDPR; SVANBERG, C. W.; "Article 89. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes". In: The EU General Data Protection Regulation (GDPR): A Commentary. Kuner, C., Bygrave, L. A., Docksey, C. (eds). Oxford: Oxford University Press (2020), p. 1249.

[27] Notwithstanding the GDPR's broad definition, Member States may define additional conditions for processing special categories of data. This means that the conclusions we arrive at will need to be analysed in line with national derogations and definitions of scientific research. See also VERHENNEMAN, G.; "AI and Healthcare Data". In: The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence. Smuha, N. A. (ed). Cambridge: Cambridge University Press (2025) Cambridge, p. 312.

[28] EUROPEAN DATA PROTECTION SUPERVISOR, A Preliminary Opinion on data pro-

definition provided by the Copyright in the Digital Single Market Directive ("CDSMD"), frames scientific research as a methodological pursuit of knowledge with public benefits.[29]

b. Secondly, scientific research requires the adoption of established scientific methods, i.e. the observation of phenomena, hypothesis creation and testing to ascertain their validity, openness to scholarly critique, and transparency of the conclusions arrived at.[30]

How to process health data for AI training in the healthcare sector

Based on this, we find room to conclude that AI training may be conceptualised as scientific research. In fact, it can be argued that an AI model is in itself a means that allows the increase of insights and the available *corpus* of knowledge since it leads to the creation and analysis of information through the rules and patterns it generalises from its training – a systematic and methodological process of arriving at the desired result: a functional AI model.

The Hamburg Regional Court in Kneschke v. LAION arrived at a similar conclusion, albeit when looking at the CDSMD, where it acknowledged the collection of training data as scientific research, establishing that:[31]

a. The concept of research includes preliminary steps and not solely direct knowledge creation, as long as they intend to lead to knowledge advancement.
b. The definition does not hinge upon the success of the research

tection and scientific research (2020), p. 9-10.

[29] Idem. See also Article 3 CDSMD.

[30] EUROPEAN DATA PROTECTION SUPERVISOR, A Preliminary Opinion on data protection and scientific research (2020), p. 10.

[31] LG Hamburg, Urteil vom 27.09.2024 – 310 O 227/23, para. 113.

but rather rests on methodological and systematic intent to achieve these objectives.

Therefore, AI training can be considered as scientific research when that training contributes systematically, methodologically, and transparently to societal knowledge and technological advancement, which seems to be the case with models aimed at being deployed in the healthcare space to i.e. render better diagnosis and medical treatment to patients.

However, to process health data based on scientific research purposes, the conditions described above need to be complied with, namely limiting the data processing to what is strictly necessary, with appropriate data minimization and anonymisation processes to mitigate the risks towards data subjects.

With this in mind, there are three main phases of minimisation and anonymisation AI developers need to consider.

1. Data collection

The healthcare sector processes personal data for multiple purposes, including to validate therapies, diagnosis and other healthcare practices. This information is typically collected and generated through various interactions with patients and kept in electronic health records ("EHRs"), which are essential sources for AI training datasets.[32] However, while unique patient identification is vital to healthcare services, patient names and other identification elements are typically unnecessary in the context of AI training. This means that all personal data that is not necessary to train the AI model must be removed or anonymised, ideally before being collected by the AI developer.

Consequently, to go in line with GDPR standards, developers will need to ensure they collect anonymised datasets from their suppliers to

[32] VERHENNEMAN, G.; "AI and Healthcare Data". In: The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence. Smuha, N. A. (ed). Cambridge: Cambridge University Press (2025) Cambridge, p. 308-310.

the extent possible for the purposes pursued and given the practical difficulties of anonymising EHRs.[33] Indeed, fully anonymising i.e. free-text clinical reports, may prove difficult, leading to residual personal data remaining within the dataset. In such cases, AI developers must also implement additional safeguards in a second phase to manage residual risks of re-identification.

2. Data pre-processing

After the data collection phase, developers will need to pre-process the collected information and remove any unnecessary personal data by using appropriate anonymisation processes. Here, two primary methods can be deployed:

a. Randomisation: This approach modifies data attributes, altering their accuracy to obscure the link to data subjects. One of the main randomisation techniques is noise addition, which adjusts data values just enough to retain the same distribution without allowing re-identification.[34]
b. Generalisation: Its purpose is to dilute data's specificity, adjusting magnitudes or broadening its attributes. Aggregation, for example, aims to combine data subjects into sufficiently large groups to effectively prevent identification at an individual level.[35]

After adopting an anonymisation process, developers will need to test and ensure it is effective, considering both the technical feasibility and expertise required to reverse it.[36] This must be done taking into

[33] Idem.
[34] ARTICLE 29 WORKING PARTY, Opinion 05/2014 on Anonymisation Techniques (2014), p. 12.
[35] Idem., p. 16-17.
[36] Idem., p. 9.

account risks of singling out,[37] linkability,[38] and inference,[39] as mentioned by the WP29.[40] The results of this assessment will inherently vary according to factors such as dataset attributes (i.e. their uniqueness), limitations on the access to the training datasets, availability of additional data allowing re-identification and the effort, cost, and required technological expertise necessary to reverse the anonymisation, which the developer needs to consider.[41]

This means that developers needing to anonymise personal data must combine different anonymisation strategies. Neither randomisation nor generalisation alone offer complete protection, so incorporating different methods is required for an efficient anonymisation process.[42] Moreover, developers should exclude rare or unique attributes to the extent that it doesn't undermine the training of the model, as well as ensure the underlying personal data is properly deleted.[43]

3. Model training

When personal data is necessary for the model's training, developers must adopt adequate safeguards to minimise its inherent risks, particularly those linked to the memorisation and output of health data.

In fact, the EDPB concluded that AI models trained on personal data cannot automatically be considered anonymous. Instead, given the high likelihood of extraction and inference, a case-by-case risk

---

[37] Risk of individual records being isolated within the dataset.

[38] Risk of linking multiple records related to one data subject within the same database or across separate databases.

[39] Risk of deducing sensitive attributes with significant probability from other information available within the dataset.

[40] ARTICLE 29 WORKING PARTY, Opinion 05/2014 on Anonymisation Techniques (2014), p. 11-12.

[41] CJEU, Case C-479/22 P, OC, para. 50; EUROPEAN DATA PROTECTION BOARD, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models (2024), p. 16.

[42] ARTICLE 29 WORKING PARTY, Opinion 05/2014 on Anonymisation Techniques (2014), p. 23.

[43] Idem., p. 9 and 25.

assessment must be undertaken by the developer to reach that conclusion.[44] This assessment should include considerations on the training data's characteristics, the model's architecture, training procedures, contextual use once deployed, cost, effort, and available technological resources.[45] Importantly, developers must determine whether third parties can reasonably identify data subjects from interactions with the model or access to it, if it is i.e. open-sourced.[46]

Therefore, AI developers must pay particular attention to the following when training their models on health data:[47]

a. Data Protection Impact Assessment ("DPIA"): Given the substantial risks connected with health data, conducting a DPIA is not just mandatory but also allows developers to systematically identify, evaluate and mitigate risks towards data subjects.
b. Privacy by design and by default: Developers should evaluate the impact different design and training choices have on the identifiability of data subjects from the model's parameters and output. Additionally, the EDPB recommends training methods involving i.e. regularisation, which improves model generalisation and reduces risks linked to overfitting. Privacy-preserving technologies such as differential privacy should be evaluated and applied when suitable.
c. Data sources and preparation: Developers must ensure only the strictly necessary personal data is used to train the model. Thus, and following the steps outlined in this essay, they must adopt relevant criteria when selecting the training data, assess the adequacy of data sources with the training objective, and exclude

[44] EUROPEAN DATA PROTECTION BOARD, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models (2024), p. 14-16

[45] Idem.; CJEU, Case C-479/22 P, OC, para. 50-51.

[46] EUROPEAN DATA PROTECTION BOARD, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models (2024), p. 16 et seqs.

[47] Idem.

unnecessary or inadequate sources. Additionally, they should adhere to the data pre-processing methodologies discussed previously, using anonymised or at least pseudonymised data whenever possible.

d. Testing for vulnerabilities and residual risks: Testing should be conducted throughout the training stage to address common and the most critical privacy attacks and risks, including attribute inference, membership inference, model inversion, memorisation, reconstruction, exfiltration, and regurgitation of training data.

Conclusion

This essay aimed to outline a three-phase approach enabling AI developers in the healthcare sector to lawfully process health data to train AI models as scientific research. Initially, they must obtain anonymised datasets, thus avoiding the application of the GDPR from the start. To the extent that this is not possible, developers must anonymise or remove any remaining personal data before training the model that is not needed at the training stage. If it is, developers must adopt a third layer of protection, by mitigating risks to data subjects through the pseudonymisation of personal data, and the adoption of an architecture and training process that limits the memorisation and output of personal data and is resilient to common and severe attacks.

While this essay aims to provide another route for AI developers to process special categories of data in this sector, other obligations will also need to be accounted for, such as the respect towards data subject rights, namely when it comes to the right to be informed and to be forgotten, whose practical implementations are far from easy to achieve.

When Rights Collide: GDPR and the Duty of Disclosure in Civil Proceedings
Commentary to the decision of the Swedish Supreme court, case Ö 1750-20

Moa Hedlund

1. Introduction

Courts play a significant role in shaping the future of data protection across the EU and Swedish courts are not an exception. In case Ö 1750-20, the Swedish Supreme Court addressed the issue of disclosing a staff register containing personal data within civil litigation, focusing on the balance between evidentiary needs and the right to the protection of personal data under EU law.

This paper aims to discuss the case in relation to the General Data Protection Regulation (GDPR) and the obligation to produce documents[1] in judicial proceedings. The comments on the ruling will primarily focus on the assessment of balancing opposing interests within GDPR-related issues as well as the fact that the right to personal data tends to conflict with other fundamental rights.

2. Facts and background

The case arose from a dispute between Per Nycander AB (Nycanders) and Norra Stockholm Bygg AB (Fastec) regarding a construction project. Nycanders hired Fastec to conduct construction work.

[1] This can either be called "*duty of disclosure*" or "*obligation to produce a document*" see https://www.domstol.se/globalassets/filer/gemensamt-innehall/for-professionella-aktorer/svensk-engelsk_ordlista_2019.pdf, page 35.

The persons working on the building site concerned recorded their presence by means of an electronic staff register. This register contained personal data, including names and personal identification numbers of workers. After the project was completed, a financial dispute emerged. Nycanders alleged that Fastec had overbilled them for work that was either not performed or carried out to a lesser extent than invoiced. To support its claim, Nycanders sought access to the electronic staff register maintained by Entral AB (Entral), a third party responsible for recording worker attendance on-site.

Before the court, Nycander requested that Entral be ordered to provide Fastec's staff register for a specific period, preferably in its entirety or, alternatively, with the personal identity numbers redacted. Nycander argued that Entral possessed the staff register and that it could serve as crucial evidence in determining Fastec's claim, as the recorded data would help verify the hours worked by Fastec's employees. Fastec objected to the disclosure, arguing that it would violate the General Data Protection Regulation (GDPR), in particular art. 5(1)(b) and infringe on the workers' privacy rights.

The tingsrätt (District Court) ordered Entral to produce in an unredacted state Fastec's staff register for the staff concerned by the building site at issue in the main proceedings during the relevant period. The Svea hovrätt (Svea Court of Appeal, Stockholm, Sweden) upheld the decision of the District Court and dismissed Fastec's objection that the obligation to produce the document was in breach of GDPR. The decision was appealed to the Supreme Court in Sweden.

3. The Supreme Court´s decision

First, the supreme court held that according to Swedish law, skatteförfarandelagen (2011:1244), there must be an electronic staff register in construction work containing necessary identification information for the employees. Furthermore, Chapter 38, Section 2, first

paragraph in rättegångsbalken (1942:740), states that anyone who possesses a written document that can be assumed to have significance as evidence is obliged to produce the document. The duty is based on the fact that in the administration of justice there is a fundamental requirement for the possibility of a complete investigation. Moreover, the court stated that when assessing whether a party should be required to produce a document, a balance must be struck between the relevance of the evidence and the opposing party's interest in not disclosing it. However, the interests of third parties in the document's content are generally not considered, except in cases covered by specific exceptions. If the requested document contains personal data, as in the disputed staff ledger, the issue of how Sweden's obligation to produce documents aligns with the EU General Data Protection Regulation arises, requiring an assessment of legal obligations versus data protection rights.

The court then referred to the following relevant provisions in GDPR. Under Article 6(1)(c) GDPR, processing personal data is lawful if necessary to fulfil a legal obligation. Article 6(3) requires that such obligations be based on EU or national law, serving a legitimate public interest in a proportionate manner. Article 6(4) states that if data is processed for a purpose other than originally collected and not based on consent or legal necessity under EU or national law, its compatibility must be assessed. Article 23(1) allows restrictions to protect judicial independence and legal proceedings. The Supreme Court in Sweden then decided to refer the following questions to the European Court of Justice (ECJ) for a preliminary ruling**: (i)** "*Does Article 6(3) and (4) of the GDPR also impose a requirement on national procedural legislation relating to the obligation to produce documents*?" **(ii)** "*If Question 1 is answered in the affirmative, does the GDPR mean that regard must also be had to the interests of the data subjects when a decision on [production] must be made which involves the processing of personal data? In such circumstances, does EU law establish*

any requirements concerning how, in detail, that decision should be made?"[2]

In the judgment of the ECJ on 2 March 2023 in the case Norra Stockholm Bygg AB, C-268/21, the court clarified that art. 6(3) and 4 in the GDPR must be interpreted as meaning that the provision applies, in the context of court proceedings, to the production as evidence of a staff register containing personal data. Art. 5 and 6 must be interpreted as meaning that, when assessing whether the production of a document containing personal data must be ordered, the national court is required to have regard to the interests of the data subjects concerned and to balance them according to the circumstances of each individual case and taking into account the requirements of the principle of proportionality and the requirements arising from the principle of data minimisation.

With support from this, the Supreme Court issued a decision as follows: the right to effective judicial protection and a fair trial requires that the parties have access to the documents necessary to prove their case. The client is deemed to have a legitimate interest in obtaining the contractor's personnel ledger through disclosure. This interest should carry significant weight in the assessment. In accordance with the preliminary ruling, consideration must be given to the interests of the registered personnel. The Supreme Court then states that the personal data in the personnel ledger mainly consists of identity information in the form of names and personal identification numbers. Furthermore, these details were provided to also be accessible to the client during the execution of the contract (even though the specific contract had been completed several years earlier).

The dispute concerns whether the contractor is entitled to certain compensation, and the registered individuals themselves are not otherwise significantly affected. Therefore, the court stated that the interest of the registered individuals in having their personal data protected from

[2] See Judgment of the European Court of Justice (ECJ) on 2 March 2023, C-268/21, paragraph 24.

disclosure is considered to carry less weight. However, special consideration must be given specifically to personal data in the form of personal identification numbers or similar. Since the client has not provided a detailed explanation of why these details are necessary, the disclosure order should, in accordance with the principle of data minimization, be limited so that the contractor must provide the personnel ledger with the registered individuals' personal identification numbers, coordination numbers, or similar numbers redacted.

Thus, The Supreme Court ruled that Entral must provide the staff register but with person identifiable information redacted.

4. Comments and analysis

It is interesting to discuss whether the access to evidence in a civil judicial process should triumph the right to the protection of personal data, which was the case in Ö 1750-20.[3] To begin with, the purpose of data protection legislation is to provide fundamental safeguards for individuals' personal data. This is reflected in a set of requirements aimed at increasing awareness of data processing and protecting individual privacy. Those handling personal data must carefully consider how it is collected, transferred, and used. Individuals should have clarity on what data is processed and for what purpose. Lawful processing must therefore be meaningful, accurate, secure, and limited in scope. The lawfulness of processing data is laid down in art. 6 GDPR. Any processing of personal data, including such that are carried out by courts, must meet the criterions of lawfulness set by this provision.[4]

In case Ö 1750-20, the personal data would be processed for another purpose other than that for which those data have been collected for. As the ECJ stated in their ruling, this is not allowed as a starting

[3] However, one must consider that the personal information actually was redacted.
[4] Judgment of the European Court of Justice on 2 March 2023, C-268/21, paragraph 29.

point. However, in order for the further processing that takes place on the basis of the obligation to produce documents to be lawful, it requires that it is a necessary and proportionate measure in a democratic society and protect one of the objectives set out in art. 23 (1) GDPR. Such an objective is, for example, the protection of the independence of the judiciary and legal action. It was the consideration above in relation to the duty of disclosure that the Supreme Court had to deal with in its assessment of the clients request for access to the personal register. In the light of ECJ´s response, the Supreme Court also had to balance the client's interest in obtaining the register file, and the individual's interest in the protection of their personal data. The Supreme Court initially stated that the ability to obtain the staff register from the contractor through disclosure constitutes a legitimate interest, and that this interest should carry significant weight in the assessment. This legitimate interest was then weighed against the privacy interests of the personnel whose data was subject to the disclosure request. The Supreme Court did not consider the requested information to be particularly sensitive in terms of personal integrity. The proportionality assessment was made and led to the conclusion that "the registered individuals' interest in having their personal data protected from disclosure is considered to carry less weigh."

In my opinion, the Supreme Court's assessment is very brief regarding the balancing of the opposing interests involved. The Supreme Court established that GDPR did not prevent the disclosure of the staff register in this specific case, as the requested personal data was not of such a nature that it would, in itself, constitute a significant intrusion into the employees' privacy. This assessment was based on the fact that the personal data, such as names and personal identification numbers, were intended to be used in this context and that access to this information was of essential importance to the legal process in the dispute. However, there is room for criticism. Such an interpretation poses a risk of undermining data protection when another legal function, such as a dispute, is deemed to outweigh individual privacy. The question that

arises is whether there is truly a proportional balance between these legal interests. Are all pieces of evidence truly of such a nature that they necessitate the disclosure of detailed personal data in order to ensure justice, or is there room to consider alternative approaches that better protect personal privacy?

Criticism can therefore be directed at the court for not fully weighing the potential risk that the disclosure of personal data, even in a legal context, could have grave consequences for individual privacy. It is possible that some employees did not intend for their personal data to be used in this manner, making it particularly problematic that such information is released without sufficient safeguards. One could argue that data protection should be more restrictive when it comes to the disclosure of personal data in all types of legal proceedings, even if this might lead to certain complications in the legal process. However, in case Ö 1750-20, as the disclosure request did not clarify why access to personal data in the form of personal identification numbers, coordination numbers, or foreign equivalents was necessary for evidentiary purposes, the Supreme Court found reason to limit the obligation to produce the document by redacting such data. In other words, considerations were made in accordance with the principle of data minimisation stated in art. 5 GDPR.

Furthermore, the right to protection of personal data is stipulated in art. 8 of the Charter of Fundamental Right of the European Union. Also, even if it is not explicitly protected in art. 8 of the European Convention on Human rights, it falls within its scope. The fact that personal data within the EU is protected as a fundamental right result in conflicts between this right and other opposition fundamental rights and freedoms. Case law from ECJ shows examples where the right to personal data has had to be balanced against other rights.[5] Case Ö 1750-20 is also a perfect example of when the right to protection of personal data

[5] See for example ECJ cases: C-131/12 (Google Spain), C-101/01 (Lindqvist) and C-461/10 (Bonnier Audio).

interferes with other fundamental rights. In particular, when the right to personal data conflicts with the right to a fair trial and right to effective remedies as the court also noted. Since all of these rights can be restricted, their has to be a balance between them.[6] This is what the Supreme Court of Sweden is trying to do in case Ö 1750-20. The court ruled that the right to a fair trail was more important in this case. The fact that they decided that the personal data should be redacted makes the judgment reasonable in my opinion. However, if the court would have concluded that the personal data would continue to be public, I would have strongly questioned the Supreme Courts decision.

Historically, Swedish courts have only considered the opposing interests of the applicant and the respondent when assessing a disclosure request, without considering the privacy interests of third parties.[7] An example of this is another case from the Supreme Court of Sweden, NJA 1982 s. 650, where the court did not comment at all on the fact that the application of obligation to produce document concerned a large number of personal data. However, Ö 1750-20, can be considered a step in the right direction. When the court chose to request a preliminary ruling to the ECJ, it indicated that the legal situation was unclear and that more detailed guidance was needed to determine whether the GDPR should take precedence over the need for evidence in civil litigation. The more apparent conclusion is that an assessment of a request for disclosure involves a balancing of the duty to disclose and the individual's privacy interest when the subject of disclosure includes personal data. Through the Supreme Court's decision, it has been clarified that the right to obtain documents through disclosure constitutes a legitimate interest that carries significant weight in the balance against the individual's interest in protecting their personal data.

---

[6] See ECJ case C-268/21, paragraph 46.

[7] Delphi,"*edition av handlingar som innehåller person personuppgifter",* https://www.delphi.se/sv/publikationer/dataskydd-integritet/edition-av-handlingar-som-innehaller--personuppgifter/ (17 January 2024).

5. Summary and final reflections

In summary, case Ö 1750-20 highlights a fundamental and challenging issue for the modern legal system: how to balance the protection of personal data with the legal need to provide evidence and ensure a fair trial. While the court prioritized the relevance of the personal data to the legal proceedings and deemed its disclosure permissible, the case raises important questions about the long-term impact of granting excessive weight to legal interests without fully safeguarding the right to protection of personal data. Finally, the principles established by the ECJ in case C-268/21 are not limited to the Swedish disclosure procedure but will have significant implications for the procedural rules on evidence collection in all EU member states.

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