

UNIVERSIDADE
AUTÓNOMA
DE LISBOA



DEPARTAMENTO DE DIREITO
MESTRADO EM DIREITO
ESPECIALIDADE EM CIÊNCIAS JURÍDICAS
UNIVERSIDADE AUTÓNOMA DE LISBOA
“LUÍS DE CAMÕES”

DECISÕES AUTOMATIZADAS: UM CONTRIBUTO JURÍDICO

Dissertação para a obtenção do grau de Mestre em Direito

Autora: Fernanda Maibon Sauer

Orientador: Professor Doutor Artur Micael Flamínio da Silva

Número da candidata: 20161191

Outubro de 2022

LISBOA

Aos meus pais, Sonia e João Guilherme,
provando que o fruto não cai longe da árvore.

À Anna Laura, meu fruto,
razão e fonte inesgotável do mais profundo afeto.

Ao meu amor,
por sê-lo.

“O problema fundamental em relação aos direitos do homem, hoje, não é tanto o de justificá-los, mas o de protegê-los”.

Norberto Bobbio – *A era dos Direitos* (2004, p. 16)

“A utilização da informática e as conquistas da ciência e da tecnologia devem visar à realização do bem comum e a satisfação dos direitos e das garantias individuais”.

René Ariel Dotti – *A liberdade e o direito à intimidade*
(1980, p. 149)

AGRADECIMENTOS

O trabalho de pesquisa para conclusão de um mestrado exige esforço, muitas horas e dias de estudos. No meu caso, isso aconteceu durante a pandemia da Covid-19. Além das dificuldades comuns a qualquer mestrando, me vi diante de outras tantas, impostas pela situação e suas consequências. Mesmo assim, ver o trabalho concluído é a prova de que sempre valeu a pena seguir em frente.

Nessa jornada não posso deixar de agradecer a todos os meus colegas de curso, especialmente Daniel Blume, Thiago Bhranner G. Costa, Alessandra Balestieri e Fernanda Fragoso, pelas trocas de conhecimento e impressões, bem como aos docentes e colaboradores da UAL, pelo carinho e pela acolhida, aos quais faço referência nas pessoas dos Professores Doutores Pedro Trovão do Rosário, Miguel Santos Neves, Manuel Monteiro Guedes Valente, Geraldo Prado, Jónatas Machado e Armindo Saraiva. Agradeço também à Professora Patricia Cardoso Dias, pelas conversas sobre a escolha do tema e sugestões na restrição do objeto, ainda na etapa do projeto.

Ao meu orientador, Professor Doutor Artur Flamínio da Silva, que é estudioso do tema na área do Direito Administrativo, meu sincero agradecimento pelas indicações bibliográficas, revisão e o preciso direcionamento do texto.

Aos amigos que se viram privados de minha presença e companhia.

À família pela compreensão diante do meu afastamento nessa reta final.

Muito obrigada.

RESUMO

A falta de transparência e a opacidade no funcionamento dos mecanismos de Inteligência Artificial geram insegurança e caminham em sentido contrário à transparência almejada pelo legislador do RGPD. As interpretações segundo as quais não há um direito à explicação (ou informação) nas decisões individuais automatizadas, as quais o titular não poderá se recusar a se submeter, são contrárias à tutela que impõe no domínio da proteção da privacidade e de dados pessoais num Estado de Direito Democrático. Diante do cenário no qual se inserem as novas tecnologias e em especial as decisões individuais automatizadas, há necessidade de se conhecer a respeito da existência ou não de um direito à explicação, de seu conteúdo e limites, assim como se esse direito está em conformidade com o sistema legislativo vigente relativamente à proteção da privacidade e proteção de dados pessoais e os valores fundamentais do Estado de Direito Democrático.

Palavras chaves: Decisões Automatizadas. RGPD. Ética.

ABSTRACT

The lack of transparency and the opacity in the functioning of Artificial Intelligence mechanisms generate insecurity and go against the transparency desired by the RGD legislator. Interpretations according to which there is no right to explanation (or information) in automated individual decisions to which the data subject cannot refuse to submit, are contrary to the protection that it imposes in the field of protection of privacy and personal data in Democratic Rule of Law. Faced with this scenario in which new technologies are inserted and, in particular, automated individual decisions, there is a need to know about the existence or not of a right to explanation, its content and limits, as well as whether this right is in accordance with the current legislative system regarding the protection of privacy and protection of personal data and the fundamental values of the Democratic Rule of Law.

Keywords: Automated Decisions. GDPR. Ethics.

SUMÁRIO

INTRODUÇÃO	10
1 DO DIREITO À RESERVA SOBRE A INTIMIDADE DA VIDA PRIVADA, AO DIREITO À PRIVACIDADE E À AUTODETERMINAÇÃO INFORMACIONAL E PROTEÇÃO DE DADOS PESSOAIS.	14
1.1 Caraterização e conceito de reserva sobre a intimidade da vida privada.....	14
1.2 Conteúdo do direito à reserva sobre a intimidade da vida privada no ordenamento jurídico português e brasileiro	21
1.3 Proteção da intimidade da vida privada: tutela internacional e regional	33
1.4 A relevância proteção da privacidade e o direito à reserva sobre a intimidade da vida privada e a necessidade de tutela	40
1.5 O direito à autodeterminação informacional e à proteção de dados pessoais.....	50
2 DA CONFORMIDADE ENTRE O REGIME DE PROTEÇÃO DE DADOS PESSOAIS, AS DECISÕES AUTOMATIZADAS E A DEFINIÇÃO DE PERFIS	56
2.1 Princípios relativos à proteção de dados pessoais e a licitude dos fundamentos para as operações de tratamento de dados	56
2.1.1 Princípios relativos à proteção de dados pessoais	56
2.1.2 Da licitude dos fundamentos para as operações de tratamento	64
2.2 Aproximação conceptual do RGPD: definição de perfis e decisões automatizadas.....	69
2.2.1 Definição de perfis	70
2.2.2 Decisões automatizadas.....	71
2.3 Da especificidade da tutela relativa a categorias especiais de dados previstos no n.º 4.º do artigo 22.º do RGPD.....	72
2.3 Direitos dos titulares dos dados	75
2.3.1 Direito a ser informado – alínea f) do n.º 2 do art.º 13.º; alínea g) do n.º 2 do art.º 14.º e alínea h) do n.º 1 do art.º 15.º do RGPD.....	75
2.4 Das disposições específicas do artigo 22.º do RGPD relativas às decisões automatizadas.....	82
2.4.1 Da decisão tomada exclusivamente com base no tratamento automatizado	82
2.4.2 Efeitos na esfera jurídica do titular dos dados.....	83
2.4.3 Exceções à proibição	84

2.4.3.1	Execução de um contrato	84
2.4.3.2	Autorizada pelo Direito da União ou do Estado-Membro	85
2.4.3.3	Consentimento explícito	86
2.4.4	Garantias adequadas	86
3	INTELIGÊNCIA ARTIFICIAL E DIREITO: DEMARCAÇÃO DE	
	FRONTEIRAS NA TRANSPOSIÇÃO DE CARACTERÍSTICAS DA	
	INTELIGÊNCIA HUMANA PARA PROCESSOS AUTOMATIZADOS.....	88
3.1	Inteligência artificial – Sistemas de inteligência artificial: distinção de figuras afins: <i>machine learning</i> e <i>deep learning</i>	88
3.2	<i>Robots advisors</i> : raciocínio/processamento de informação e tomada de decisões	94
3.3	Enquadramento jurídico-ético para sistemas de inteligência artificial	98
3.3.1	Os direitos fundamentais como direitos de caráter moral e jurídico com exigência de tutela reforçada	99
3.3.2	Princípios éticos aplicados à inteligência artificial	100
3.3.2.1	Respeito pela autonomia humana	101
3.3.2.2	Prevenção de danos e responsabilidade	102
3.3.2.3	Equidade	102
3.3.2.4	Informação e esclarecimento	103
3.3.3	A vinculatividade a inteligência artificial aos direitos fundamentais.....	104
3.3.3.1	A dignidade da pessoa humana.....	104
3.3.3.2	Liberdade	104
3.3.3.3	Igualdade, não discriminação e solidariedade	104
3.3.3.4	Privacidade e governança dos dados pessoais	105
3.4	A proposta de Regulamento da Inteligência Artificial	106
	CONCLUSÃO	111
	REFERÊNCIAS	114
	Fontes Documentais	114
	Bibliografia.....	120

LISTA DE SIGLAS E ABREVIATURAS

FRA	European Union Agency for Fundamental Rights
GT 29	Grupo de Trabalho do Artigo 29.º para Proteção de Dados
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
IA	Inteligência Artificial
RGPD	Regulamento Geral de Proteção de Dados

INTRODUÇÃO

Estamos diante da quarta revolução industrial.¹ O uso de Inteligência Artificial (IA) e a aplicação de algoritmos cada vez mais complexos e assertivos não são exatamente uma novidade, em que pese seus possíveis usos sejam ainda pouco conhecidos.

Com efeito, a aplicação de sistemas de IA assumiu uma importância incontestável no quotidiano das pessoas comuns, considerando que “o crescimento exponencial do tratamento automatizado de dados, espoletando pelos avanços tecnológicos das últimas décadas, coloca-nos, a todos, numa posição de enorme fragilidade: as informações pessoais hoje armazenadas, pelos mais distintos responsáveis pelo tratamento, públicos e privados, são hoje superiores às informações que nós próprios detemos sobre nossa vida”².

Nosso estudo envolve a análise da aplicação da IA para produção de decisões individuais automatizadas, incluindo a definição de perfis e eventuais falhas no juízo de adequação das decisões automatizadas, bem assim como a exceção prevista na alínea b) do n.º 2 do art.º 22.º do Regulamento Geral de Proteção de Dados (RGPD) e se esta se poderá considerar conforme com a proteção da privacidade e de dados pessoais estabelecidos pelo RGPD e, em última análise, com o Estado de Direito Democrático.

Nesse sentido, ao lado do desenvolvimento tecnológico têm se debruçado os estudiosos do Direito para garantir que esse avanço extraordinário não importe na perda de direitos e garantias (fundamentais) tão caros à preservação da dignidade humana e do Estado Democrático, ao mesmo passo e na medida em que as tecnologias em desenvolvimento se mantenham criando facilidades antes inimagináveis a serviço de seu criador. Não por acaso o artigo 1.º do RGPD traz os seus dois grandes propósitos, quais sejam, “a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação de dados”^{3,4}.

¹ SHWAB, Klaus – **A quarta Revolução Industrial**. São Paulo: Edipro, 2016.

² CORDEIRO, António Barreto Menezes – **Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020, p. 29.

³ UNIÃO EUROPEIA. Parlamento e Conselho – Regulamento n.º 679, 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). **Jornal Oficial da União Europeia** [Em linha]. L 119, n.º 2 (04 maio 2016). [Consult. 10 nov. 2019]. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:32016R0679>.

⁴ No mesmo sentido é o artigo 1.º da Lei n.º 58/2019, de 8 de agosto de 2019 (Lei de Execução do RGPD). (PORTUGAL. Assembleia da República – Lei n.º 58/2019, de 8 de agosto. Lei da Proteção de Dados Pessoais. Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Diário da República** [Em linha]. N.º 151, Série I (08 ago. 2019), p. 3-40. [Consult. 13 set. 2022]. Disponível em:

Para Gustavo Schainberg S. Babo, “os governos e as empresas cada vez mais utilizam algoritmos para aumentar a consistência das decisões, economizar dinheiro ou apenas gerenciar processos complicados. As decisões baseadas no aprendizado de máquina podem ser incrivelmente úteis e têm um impacto profundo em nossas vidas. A confiança e a responsabilidade são conceitos necessários que devem existir entre essas diversas aplicações dos algoritmos na sociedade. Para isso, vários debates são movimentados sobre ética, automação e futurismo, para que os pontos positivos dos algoritmos sejam explorados ao máximo. Contudo, os temores sobre os impactos da Inteligência Artificial no futuro estão distraindo os pesquisadores dos riscos reais dos sistemas implantados, como os vieses discriminatórios dos algoritmos utilizados. A natureza onipresente desse problema significa que precisamos de soluções sistemáticas urgentes”⁵.

Os algoritmos treinam e se desenvolvem a partir de dados já existentes e, para que aprendam com eficiência, precisam ser alimentados com uma grande quantidade de dados. Nesse contexto, considerando a pré-existência desses dados, é possível que os algoritmos tendam a replicar ou até a exacerbarem padrões históricos discriminatórios e indesejáveis. Ao contrário do que possa parecer, ao invés de a automatização nos levar a decisões mais objetivas e mais justas, uma vez que o sistema ou a máquina não poderiam ser parciais, a experiência recente nos mostrou que essa ideia está longe da realidade e desafia até mesmo o conceito de *neutralidade*⁶.

Nos Estados Unidos, por exemplo, foi possível observar a face mais perversa envolvendo tais riscos no que diz respeito à utilização de sistemas de IA de reconhecimento facial no direito penal. Um homem foi preso por dez dias depois que o sistema de reconhecimento facial chamado ClearView o teria identificado como sendo a pessoa na fotografia de um documento falso que estava na posse de um assaltante de uma loja em Nova Jersey. Ele recusou o acordo com a justiça que o levaria à cadeia por seis anos e foi a julgamento. Durante o julgamento, por insistência da defesa, o juiz exigiu que os procuradores apresentassem outras evidências além do reconhecimento pelo sistema de IA, mas não havia outras evidências e foram obrigados a retirar o caso. No processo o advogado

https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=3118A0002&nid=3118&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=

⁵ BABO, Gustavo Schainberg S. – **Discriminação Algorítmica: Origens, Conceitos e Perspectivas Regulatórias** [Em linha]. Belo Horizonte, MG: DTIBR, 15 jun. 2020. [Consult. 30 jul. 2020]. Disponível em: <https://www.dtibr.com/post/discrimina%C3%A7%C3%A3o-algor%C3%ADmica-origens-conceitos-e-perspectivas-regulat%C3%B3rias-parte-1>.

⁶ COSTA, Inês da Silva – A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas. **Revista Eletrônica de Direito** [Em linha]. Vol. 24, n.º 1 (fev. 2021), p. 34-82, p. 37. [Consult. 06 jun. 2022]. Disponível em: https://cije.up.pt/client/files/0000000001/4-ines-costa_1677.pdf.

do acusado alegou que ele só foi preso e processado por preconceito racial, já que é afro-americano. Há um histórico de falhas em sistemas de reconhecimento facial nos Estados Unidos, muito embora vários estados daquele país ainda utilizem ferramentas similares com essa tecnologia^{7,8}.

Em *The Black Box Society*⁹, Frank Pasquale expõe como interesses poderosos abusam do sigilo/segredo de empresa para obterem lucro com a obscuridade de seus sistemas de IA (os “black boxes” que dão nome ao título) e explica maneiras de controlá-los. Expõe que algoritmos podem construir ou arruinar reputações, decidir o destino de empreendedores ou até mesmo devastar a economia. Envoltas em segredo e complexidade, as decisões automatizadas até então consideradas neutras se mostram discriminatórias, como no *credit scoring*¹⁰.

Neste nosso trabalho procuramos, essencialmente, dar um contributo na demonstração de que a falta de clareza e opacidade quanto ao funcionamento dos mecanismos já conhecidos da Inteligência Artificial geram insegurança e caminham num sentido inverso da transparência almejada pelo legislador do RGPD. Além disso, pretendemos analisar se as interpretações segundo as quais não há um direito à explicação (informação) nas decisões individuais automatizadas, as quais o titular não poderá se recusar a se submeter, são, efetivamente, contrárias à tutela que se impõe no domínio da proteção da privacidade e de dados pessoais num Estado de Direito Democrático.

⁷ Para a notícia completa a respeito, confira: RIGEUS, Rafael – Reconhecimento facial falha e homem inocente passa 10 dias na cadeia. **Olhar Digital** [Em linha]. São Paulo, 30 dez. 2020. [Consult. 12 set. 2022]. Disponível em: <https://olhardigital.com.br/2020/12/30/noticias/reconhecimento-facial-falha-e-homem-inocente-passa-10-dias-na-cadeia/>.

⁸ Em outro caso, em 2020 no estado de Michigan, outro homem afrodescendente foi preso injustamente por falha no sistema de reconhecimento facial. A notícia informa que: “um debate nacional está sendo travado sobre o racismo na aplicação da lei. Em todo o país, milhões estão protestando não apenas contra as ações de policiais individuais, mas também contra o preconceito nos sistemas usados para vigiar comunidades e identificar pessoas para serem processadas. Os sistemas de reconhecimento facial são usados pelas forças policiais há mais de duas décadas. Estudos recentes do M.I.T. e o Instituto Nacional de Padrões e Tecnologia, ou NIST, descobriram que, embora a tecnologia funcione relativamente bem em homens brancos, os resultados são menos precisos para outros dados demográficos, em parte devido à falta de diversidade nas imagens usadas para desenvolver os bancos de dados” (THE NEW YORK TIMES – **Wrongfully Accused by an Algorithm** [Em linha]. New York, 03 ago. 2020. [Consult. 12 set. 2022]. Disponível em: <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>).

⁹ PASQUALE, Frank. **The Black Box society: the secret algorithms that control money and information**. Cambridge: Harvard University Press, 2015, *passim*.

¹⁰ “A credit card company uses behavioral-scoring algorithms to rate consumers' credit risk because they used their cards to pay for marriage counseling, therapy, or tire-repair services. [...] But this account is misleading. Because human beings program predictive algorithms, their biases and values are embedded into the software's instructions, known as the source code and predictive algorithms.²⁰ Scoring systems mine datasets containing inaccurate and biased information provided by people” (CITRON, Danielle Keats; PASQUALE, Frank – The scored society: due process for automated predictions. **Washington Law Review** [Em linha]. Vol. 89 (2014), p. 1-33. [Consult. 12 set. 2022]. Disponível em: <https://core.ac.uk/download/pdf/327104566.pdf>).

Assim, iniciamos a investigação identificando as origens, o conteúdo e titularidade do direito à reserva sobre a intimidade da vida privada. Da mesma forma analisamos a proteção da privacidade e a relevância da sua tutela jurídica para a evolução dos mesmos direitos até o direito à autodeterminação informacional e à proteção de dados pessoais.

No segundo capítulo, analisamos se o regime de proteção de dados pessoais, as decisões automatizadas e a definição de perfis, especialmente no que se refere às categorias especiais de dados previstos no n.º 4 do art. 22.º do RGPD, o direito de ser informado e às demais disposições relativas às decisões automatizadas contidas no art. 22.º do RGPD, estão em conformidade com os princípios norteadores do RGPD.

No terceiro capítulo nos dedicamos a analisar a relação entre a utilização de mecanismos de Inteligência Artificial e seu encontro (ou possíveis dificuldades) com o Direito, analisando e demarcando os limites jurídicos-éticos da transposição das características da inteligência humana para processos automatizados.

Ao final, tendo em consideração que a transparência e a responsabilidade¹¹ são princípios norteadores do RGPD, esperamos alcançar o objetivo de apresentar o cenário no qual se inserem as novas tecnologias, em especial as decisões individuais automatizadas, a necessidade de se conhecer a respeito da existência ou não de um direito à informação, de seu conteúdo e limites, assim como se esse direito está em conformidade com o sistema legislativo vigente relativamente à proteção da privacidade e proteção de dados pessoais e os valores fundamentais do Estado de Direito Democrático.

Em suma, é nossa intenção que este trabalho possa contribuir, no intuito de corroborar a importância da discussão, para uma busca de soluções para os sucessivos problemas que vêm surgindo e que ainda surgirão, bem assim como apurar da “responsabilidade” do Estado em sua constante atualização e promoção de iniciativas tanto no âmbito internacional, quanto nacional, para proteção da vida privada e da privacidade, na mesma medida que da livre iniciativa e da liberdade e igualdade.

¹¹ Transparência e responsabilidade também são princípios afetos ao Direito Administrativo. Sobre o tema *vide* SILVA, Artur Flávio da – Inteligência Artificial e Direito Administrativo. **Direito Administrativo e Tecnologia**. Coimbra: Almedina, 2021. p. 11-14, 21-24.

1 DO DIREITO À RESERVA SOBRE A INTIMIDADE DA VIDA PRIVADA, AO DIREITO À PRIVACIDADE E À AUTODETERMINAÇÃO INFORMACIONAL E PROTEÇÃO DE DADOS PESSOAIS.

1.1 Caracterização e conceito de reserva sobre a intimidade da vida privada

Na busca pela caracterização e conceituação do direito à reserva da intimidade da vida privada, recorreremos à evolução do conceito de *privacidade*. Princípios por duas sentenças que seriam anteriores ao direito da privacidade (*privacy*)¹². A primeira delas seria de 1384, do caso *I. De S. Et uxor v. De S.*, França, e a segunda, de 1849, no caso *Prince Albert v. Strange*.

No primeiro caso, que remonta ao século XIV, marcado pela crise em toda a Europa pela decadência do Feudalismo, que apontava para o fim da Idade Média na Europa Ocidental, e, em Portugal, pela crise resultante da sucessão de D. Fernando, que havia deixado como sua herdeira Beatriz de Portugal, que, por sua vez, se casa com João I de Castela, o que implicaria na perda de independência e resultaria, como de fato resultou, no início da Dinastia de Avis. No caso concreto, o acusado, pretendendo comprar vinho na madrugada, bateu na porta da taberna de propriedade dos autores da reclamação e, como não atenderam, golpeou a machadadas o batente da janela da casa, sendo condenado a pagar indenização pelos “males” causados¹³¹⁴.

O segundo, ocorrido na Inglaterra Vitoriana durante a Revolução Industrial, foi do caso *Prince Albert v. Strange*, em que o autor era o Príncipe Albert, marido da Rainha Vitória, o qual obteve uma ordem da Corte para impedir que o senhor William Strange divulgasse/expusesse ou vendesse reproduções dos desenhos e gravuras que ele, o Príncipe, e a própria Rainha haviam feito para seu divertimento particular¹⁵.

¹² O conceito de privacidade teria surgido desde a Antiguidade Clássica, considerando que Aristóteles distinguia a *esfera privada* (“oikós”) da *esfera pública* (“polis”). “A *esfera privada* dizia respeito à família, às questões económicas, e biológicas, enquanto que a *esfera pública* dizia respeito à liberdade política dos cidadãos”. (cf.: CORREIA, Victor – Sobre o Direito à privacidade. **O Direito**. [Em Linha] Ano 146, n.º 1 (2014), p. 9-32, p. 9. [Consult. 17 jul. 2022]. Disponível em: https://www.academia.edu/6106718/Sobre_o_direito_%C3%A0_privacidade)

¹³ COELHO, Larissa A. – Investigação de “casamentos brancos” e a reserva da intimidade da vida privada: Uma análise do acórdão do Tribunal Central Administrativo Sul, de 17 de dezembro de 2009. **Revista Jus Navigandi**. Ano 16, n. 3012 (30 set. 2011) [Em linha] [Consult. 1 fev. 2022]. Disponível em: <https://jus.com.br/artigos/20110/investigacao-de-casamentos-brancos-e-a-reserva-da-intimidade-da-vida-privada/1>.

¹⁴ CABRAL, Rita Amaral – O direito à intimidade da vida privada. Breve reflexão acerca do art. 80º. Do Código Civil. **Separata dos estudos em memória ao prof. Dr. Paulo Cunha**, Lisboa: 1998, p. 383.

¹⁵ CARDOZO, Virgínia Fehlberg – **O direito à intimidade da vida privada: o problema do enquadramento jurídico constitucional das escutas telefónicas em processo penal** [Em linha]. Coimbra, 2016. Dissertação de Mestrado em Direito apresentado à Universidade de Coimbra, 2016. (polic.ª), p. 18. [Consult. 1 set 2020] Disponível em: <https://estudogeral.sib.uc.pt/bitstream/10316/41203/1/Virg%20adnia%20Fehlberg%20Cardozo.pdf>

Reconheceu-se, então, um direito de propriedade que impediu a reprodução¹⁶.

Até o século XIX, a privacidade não era tida como um direito autônomo e, assim como em Roma, sua proteção se dava de forma reflexa a partir da tutela da propriedade, da liberdade e até mesmo da honra.

Locke e Stuart Mill também se dedicaram ao estudo do que chamamos de privacidade. Locke desenvolveu a ideia de liberdade como a autonomia de dispor, como bem entender, de seus atos, bens e tudo mais que lhe pertença¹⁷. Em *Sobre a liberdade*, Stuart Mill defende que as condutas humanas capazes de gerar deveres e responsabilidades seriam aquelas que afetassem os demais seres humanos em sociedade. Assim, aquilo que só afetasse a esfera pessoal do indivíduo seria absolutamente independente, sendo este soberano sobre si, seu corpo e sua mente¹⁸.

No entanto, o caso que é certamente o mais comentado e descrito entre a doutrina jurídica dos estudiosos dos direitos de privacidade e proteção de dados é aquele ocorrido nos Estados Unidos da América do Norte, no final do século XIX (1890), com a publicação do “The Right To Privacy”, dos advogados Samuel Dennis Warren II e Louis Dembitz Brandeis, na *Harvard Law Review*, como a primeira tentativa, ou pelo menos a mais conhecida, de se buscar estabelecer os limites para interferência na vida privada e de se estabelecer o direito à privacidade como direito autônomo. Warren, assim como Brandeis¹⁹, graduado em Direito da Universidade de Harvard, nascido em Boston em uma família de posses, passou a ter seu nome ligado às notícias sensacionalistas de que teria um caso com a filha de um político conhecido da época, logo após seu casamento. O trabalho passou a ser reconhecido como o responsável pela fixação das bases jurídicas do “direito de seu deixado em paz” ou de “estar só” (*right to be left alone*).

A intimidade e a vida privada são valores que, após anos de proteção reflexa por outros institutos jurídicos, o Direito começa a tutelar autonomamente, a partir do final do século XIX^{20,21}. Para tanto, as discussões sobre a existência, o conceito e a estrutura jurídica

¹⁶ DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**. 2.^a ed. São Paulo: Revista dos Tribunais, 2019, p. 32, nota 12.

¹⁷ LOCKE, John – **Segundo tratado sobre governo civil: ensaio sobre a origem, os limites e os fins verdadeiros do governo**. Petrópolis: Vozes, 1999, *passim*.

¹⁸ MILL, John Stuart – **Sobre a liberdade**. São Paulo: Martins Fontes, 2000, *passim*.

¹⁹ Brandeis teria se tornado mais tarde juiz da Suprema Corte (Cf. CABRAL, Rita Amaral – O direito à intimidade da vida privada. Breve reflexão acerca do art. 80º. Do Código Civil. **Separata dos estudos em memória ao prof. Dr. Paulo Cunha**, Lisboa, 1998, p. 6).

²⁰ DRAY, Guilherme – O direito à reserva da intimidade da vida privada: o artigo 80.º do Código Civil de 1966. **Revista de Direito Civil**. Ano II, n.º 3 (2017). p. 673-699, p. 678.

da, então, nova categoria dos direitos da personalidade foi vital. Na verdade, foi o aumento da urbanização e a convivência nas áreas urbanas que fez com que um sentimento de indiferença em relação aos vizinhos crescesse, sendo considerado um dos fatores sociológicos que promoveram essa noção de privacidade, principalmente na segunda metade do século XIX²².

Nesse passo, até se chegar à noção atual de *privacidade*, o direito à reserva sobre a intimidade da vida privada era entendido por meio de uma noção negativa, de não intromissão na esfera da vida privada, de proteção da personalidade física. A noção, até então, segundo Danilo Doneda, era “marcada por um individualismo exacerbado e até egoísta, portava a feição do direito a ser deixado só”. Segundo o autor, “a esse período remonta o paradigma da privacidade como uma *zero-relationship*, pelo qual representaria, no limite, a ausência de comunicação entre uma pessoa e as demais”²³. Foi a partir do artigo da dupla Warren e Bradeis o marco inicial para um crescente entendimento de que a privacidade seria aspecto fundamental para o desenvolvimento e realização da personalidade humana²⁴.

Assim, o que o indivíduo fazia no âmbito privado em seu momento de descanso e recolhimento deveria ser respeitado, não sendo divulgado sem seu consentimento. Na época questionou-se sobre a natureza jurídica ou fundamento do direito que impediria a publicação de momentos de recolhimento ou privacidade. Algumas correntes surgiram na época. A primeira defendia que esse direito seria em verdade uma extensão do direito à propriedade. Outra corrente, em contraposição à ideia de um valor pecuniário que recai sobre o direito de propriedade, entendia que a proteção conferida aos sentimentos e emoções poderiam se materializar de diferentes formas merecendo o reconhecimento de um direito mais amplo, como o direito de “não ser molestado”²⁵.

Alexandre Sousa Pinheiro afirma que o artigo de Warren e Bradeis, “The Right To Privacy”, traz “problemas efetivos e desenvolve um ideário que fará o seu curso na doutrina e no direito positivo” e destaca: “(i) a necessidade de a *common law* se adaptar as novas realidades sociais; (ii) que se procura encontrar resposta para um instrumento

²¹ Para Luísa Neto no século XIX o fundamento para a tutela da intimidade e vida privada já começa a se aproximar da ideia de dignidade humana/personality (PRATA, Ana (coord.) – **Código Civil Anotado. Volume I (Artigos 1.º a 1250.º)**. Coimbra: Almedina, 2019, p. 122).

²² CARDOZO, Virgínia Fehlberg – **O direito à intimidade da vida privada: o problema do enquadramento jurídico constitucional das escutas telefónicas em processo penal** [Em linha]. Coimbra, 2016. Dissertação de Mestrado em Direito apresentado à Universidade de Coimbra, 2016. (polic.^a), p. 61. [Consult. 1 set 2020] Disponível em: <https://estudogeral.sib.uc.pt/bitstream/10316/41203/1/Virg%C3%ADnia%20Fehlberg%20Cardozo.pdf>.

²³ DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**. 2.^a ed. São Paulo: Revista dos Tribunais, 2019, p. 30.

²⁴ No mesmo sentido, *vide*: DRAY, Guilherme – O direito à reserva da intimidade da vida privada: o artigo 80.º do Código Civil de 1966. **Revista de Direito Civil**. Ano II, n.º 3 (2017). p. 673-699, p. 677.

²⁵ CARDOZO, Virgínia Fehlberg, *op. cit.*, p. 61.

tecnologicamente novo que pode afectar a personalidade do indivíduo (não propriamente câmeras inseridas em telefones móveis, mas as máquinas fotográficas *kodak*); (iii) a necessidade de construção de uma área de reserva integral do indivíduo, tendo-se para isso recorrido ao *right to be let alone*; (iv) a construção de um nível imaterial de tutela da personalidade; (v) a necessidade de definir ilícitos capazes de proteger os bens da personalidade em causa”²⁶. Por isso, o legado de Warren e Bradeis é inestimável, resultando na palavra *privacy*, muito embora o debate sobre privacidade já fosse presente na jurisprudência e doutrina da época²⁷.

Fato é que a partir daí se deu a evolução do direito à privacidade e à reserva da intimidade no século XX, culminando com sua menção expressa da Declaração Universal dos Direitos Humanos²⁸, de 1948, em seu artigo 12.^o²⁹.

Danilo Doneda aponta que há uma profusão de termos utilizados pela doutrina brasileira para tratar a privacidade. Podem ser mencionados os termos: *vida privada*, *intimidade*, *sigilo*, *recato*, *reserva*, *intimidade da vida privada*. Acrescenta que na doutrina estrangeira também demonstra a variedade de nomenclaturas, como o termo *privacy*, que foi consolidado com o “*The Right To Privacy*”, mas que muitas vezes está relacionado a um número de situações que não se relacionam, necessariamente, para um jurista de tradição *civil law*, com a privacidade. Mesmo a menção ao “direito de ser deixado só”, como sendo uma definição de Warren e Bradeis, não se afiguraria correta já que os autores não chegaram a afirmar que a expressão traduziria o conteúdo do direito à privacidade³⁰.

No mesmo sentido, Paulo Mota Pinto afirma que “definir com rigor ‘privacidade’ é uma tarefa que parece raiar os limites do impossível”, acrescentando que existem aqueles que afirmam ser um conceito “vazio” e “obscuro”, que, “por abranger tudo, acaba por não ter conteúdo, um conceito ao qual não se deveriam abrir as portas do mundo jurídico. A denunciada ‘miséria *privacy*’ resulta em grande parte dessa dificuldade de definição de um conceito que, por ser necessariamente indeterminado, acaba por se revelar afinal imprestável,

²⁶ PINHEIRO, José Alexandre Guimarães de Souza – **Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional** [Em linha]. Lisboa, 2012. Tese de doutorado em Direito (Ciências Jurídico-Políticas) apresentada à Universidade de Lisboa. (polic.^a), p. 350. [Consult. 10 out. 2021]. Disponível em: <https://repositorio.ul.pt/handle/10451/7407?locale=en>. ou Lisboa: AAFDL, 2015. ISBN 9786120002605.

²⁷ DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**. 2.^a ed. São Paulo: Revista dos Tribunais, 2019, p. 125.

²⁸ ONU. Organização das Nações Unidas – **Declaração Universal dos Direitos Humanos** [Em linha]. Paris, 10 dez. 1948. [Consult. 09 jun. 2022]. Disponível em: <https://brasil.un.org/sites/default/files/2020-09/por.pdf>.

²⁹ “Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei”.

³⁰ DONEDA, Danilo, *op. cit.*, p. 99-101.

como um verdadeiro ‘conceito elástico’³¹. Assim, não seria desejável se renunciar ao objetivo de uma definição de privacidade, pelo que se deve tentar determinar cuidadosamente o que caracteriza o interesse subjacente, uma vez que “grande parte dos problemas com o conceito de *privacy* têm a ver com um esclarecimento teleológico e conceitual insuficiente, ou, pelo menos, incapaz de resistir à tendência para se colocar sob a alçada da privacidade coisas que não têm a ver com ela”³².

Nesse aspecto, a privacidade resulta da visão individualista do Estado e da vida, colocando-a como uma categoria ampla que acaba por absorver em si inúmeros direitos que foram autonomizados como direitos da personalidade, tais como a inviolabilidade de domicílio à liberdade de pensamento e locomoção. Assim, a *privacy* acaba por ser o conteúdo do direito da personalidade, quase um megadireito, com grande extensão e pouca compreensão³³.

A definição e delimitação da privacidade não é um problema dogmático, refletindo um relevante conteúdo social e ideológico de modo que varia de sociedade para sociedade, tendo um conteúdo mais amplo ou mais restritivo de acordo com a evolução sociocultural³⁴. Mas a busca por um conteúdo comum é uma necessidade real, fruto do desenvolvimento tecnológico e grande incremento do fluxo de informações dos últimos anos, sendo uma realidade da vida moderna o processamento massivo de informações e os inúmeros problemas advindos desse processamento³⁵.

³¹ MOTA PINTO, Paulo – O direito à reserva da intimidade. **Boletim da Faculdade de Direito: Universidade de Coimbra**. Vol. LXIX (1993), p. 479-586, p. 504.

³² MOTA PINTO, Paulo – O direito à reserva da intimidade. **Boletim da Faculdade de Direito: Universidade de Coimbra**. Vol. LXIX (1993), p. 479-586, p. 504-506.

³³ ASCENSÃO, Jose de Oliveira – A Reserva da Intimidade da Vida Privada e Familiar. **Revista da Faculdade de Direito de Lisboa**. Vol. 43, n.º 1 (2002), p. 9-25, p. 15.

³⁴ Nesse sentido: “Existe uma variedade de expressões mas também de dimensões da vivência da privacidade, dado que os conteúdos e as regras da privacidade por um lado variam culturalmente, e por outro lado não cessam de evoluir historicamente. Aquilo que se entende por *privacidade* não é igual em todos os meios regionais, em todas as categorias sociais, em todos os países, e em todas as épocas. Além disso, mesmo que a privacidade diga respeito ao indivíduo, ela não se reduz ao indivíduo isolado, dado que existem normas da sociedade em geral, e de comunidades culturais específicas, que determinam o significado e o valor desse conceito. Por outro lado, alguns assuntos que outrora pertenciam à esfera privada hoje pertencem à esfera pública, e outros que outrora pertenciam à esfera pública hoje pertencem à esfera privada. A confusão não surge apenas em relação a duas épocas diferentes, mas na mesma época, como a atual, em que o espaço público invade o espaço privado, e o espaço privado invade o espaço público. Esta confusão decorre da conceção moderna da sociedade, que vê a política como um espaço de regulação também da esfera privada, e de regulação da vida doméstica, e que acarreta a dificuldade de distinção entre *público* e *privado*” (cf.: CORREIA, Victor – Sobre o Direito à privacidade. **O Direito**. [Em Linha] Ano 146, n.º 1 (2014), p. 9-32, p. 11. [Consult. 17 jul. 2022]. Disponível em: https://www.academia.edu/6106718/Sobre_o_direito_%C3%A0_privacidade).

³⁵ DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**. 2.ª ed. São Paulo: Revista dos Tribunais, 2019, p. 127-128.

No artigo já referenciado aqui, de Mota Pinto, o autor assevera que “o problema da privacidade e a sua solução [...] são dominados por uma tensão de base entre o social e o individual, tensão segundo se diz, muito em evidência nos tempos que correm. [...] A evolução técnica veio fornecer meios incomparavelmente mais eficazes de violação da intimidade das pessoas [...]. A própria noção de privacidade evoluiu, desenvolvendo-se uma maior sensibilidade dos indivíduos às ofensas ao domínio privado”³⁶.

David de Oliveira Festas afirma que o direito à reserva sobre a intimidade da vida privada tem forte dimensão ética e um âmbito de aplicação delimitado. Segundo ele,

[...] a compreensão do direito à reserva da intimidade da vida privada postula que este seja observado de três perspectivas: estrutural, teleológica e substancial. De uma perspectiva estrutural, o direito à reserva da intimidade da vida privada divide-se em dois direitos menores: o direito de impedir o acesso a informações relativas à vida privada; e o direito de impedir a divulgação dessas mesmas informações. Nesta dupla vertente, o direito à reserva da intimidade da vida privada, configura-se como um direito à informationelle Selbstbestimmung. De uma segunda perspectiva, teleológica, o direito à reserva da intimidade da vida privada visa a defesa de dois interesses: por um lado, o interesse de evitar a tomada de conhecimento e a divulgação de informação pessoal; por outro lado, sem se reconduzir ao right to be let alone, o direito à reserva da vida privada tutela também um interesse na subtracção à atenção dos outros. De uma terceira perspectiva, substancial, o âmbito de protecção do direito à reserva da vida privada pode ser delimitado de acordo com a teoria das três esferas³⁷.

A terceira perspectiva aludida é a teoria desenvolvida por Hubmann, dos círculos concêntricos, em que cada uma representa os diferentes graus de manifestação da privacidade: “vida privada”, “intimidade ou segredo” e, em torno delas, a esfera pessoal, que abrangeria a vida pública^{38,39}. A função do esquema concebido por Hubman é explicar os graus de privacidade. O maior círculo representa a vida privada e dentro dele estaria um círculo menor, que seria a intimidade, sendo ambos envolvidos pelo espaço de vida pública onde as

³⁶ MOTA PINTO, Paulo – O direito à reserva da intimidade. **Boletim da Faculdade de Direito: Universidade de Coimbra**. Vol. LXIX (1993), p. 479-586, p. 504-506.

³⁷ FESTAS, David de Oliveira – O direito à reserva da intimidade da vida privada do trabalhador no Código do Trabalho. **Revista da Ordem dos Advogados (ROA)** [Em linha]. Ano 64, Vol. I-II (nov. 2004), p. 1 [Em linha]. [Consult. 02 fev. 2022]. Disponível em: <https://portal.oa.pt/publicacoes/revista-da-ordem-dos-advogados-roa/ano-2004/ano-64-vol-i-ii-nov-2004/artigos-doutriniais/david-de-oliveira-festas-o-direito-a-reserva-da-intimidade-da-vida-privada-do-trabalhador-no-codigo-do-trabalho-star/>.

³⁸ Para Domingos Soares Farinho, a divisão da privacidade em esferas, sendo uma delas a do “segredo” seria desnecessária, já que este estaria incluído na esfera da intimidade (FARINHO, Domingos Soares – **Intimidade da Vida Privada e Media no Ciberespaço**. Coimbra: Almedina, 2006. p. 45). No mesmo sentido, vide CANOTILHO, José Joaquim Gomes; MOREIRA, Vital – **Constituição da República Portuguesa Anotada**. 4.ª ed., rev. Coimbra: Coimbra, 2014. Vol. 1, p. 468.

³⁹ Sobre a teoria das três esferas, vide: COSTA ANDRADE, Manuel da – **Liberdade de imprensa e inviolabilidade pessoal: uma perspetiva jurídico-criminal**. Coimbra: Coimbra, 1996, p. 95 *et seq.*

informações não têm restrição alguma. Essa teoria foi posteriormente abandonada pelo Tribunal Constitucional Alemão^{40,41}.

Nesse passo, “as conceituações unitárias pecam por desprezar alguns aspectos da privacidade ou por deixar de definir outros. Assim, apresentam-se muito amplas, em determinadas situações, e pouco abrangentes em outras, sempre deixando a desejar no sentido de abarcar as plurais facetas do enunciado normativo”. Por isso, “a privacidade não pode ser vista somente através da ótica da invasão (como decorre dos conceitos de direito de estar só e de resguardo contra interferências alheias), ela deve ser tida também como controle de dados pessoais e de acesso a tais dados. Contudo, entendê-la somente neste sentido, também, não é suficiente, visto que estaria deixando de lado as questões atinentes à tomada de decisões no âmbito da vida privada e da própria invasão dela. Por fim, entendê-la como segredo ou intimidade mostra-se ultrapassado, pois o fluxo de dados, hoje, é imenso e constante e as informações pessoais nem sempre são secretas, tampouco uma afronta direta à intimidade do indivíduo. Seu processamento e disseminação que, posteriormente e de forma estrutural e sistêmica, podem causar graves danos à pessoa”⁴², nos mais variados aspectos de sua vida.

Em que pesem os esforços para a definição filosófica, política e sociológica de *privacidade*, entendemos que não foi possível chegar a um conceito mínimo de precisão desejável para que possa servir a um sistema jurídico coeso⁴³.

⁴⁰ DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**. 2.^a ed. São Paulo: Revista dos Tribunais, 2019, p. 103.

⁴¹ “Inicialmente elaborada da Alemanha essa teoria foi aí objeto de inúmeras críticas e o mesmo tem sucedido em Portugal. [...]. E a verdade é que a teoria das três esferas tem sido utilizada na sua versão gradualista, e com terminologia variada, pelo Tribunal Constitucional Português. Neste sentido, o nível de intimidade dos dados ou informações é, de facto, um elemento a ponderar no juízo global de proporcionalidade, que quase sempre envolvem as questões relativas ao direito à reserva da vida privada e familiar. A complexidade do juízo de proporcionalidade neste domínio, adensa-se, pelo facto de serem concebíveis renúncias de âmbito alargado, à reserva da vida privada e familiar, como sucede, por exemplo, num concurso televisivo difundido como o Big Brother e pelo facto serem cada vez mais variados os meios tecnológicos de obtenção de informação sobre a vida privada das pessoas. [...] Independentemente da necessária e ineliminável tarefa de ponderação em concreto, não sofre, porém, contestação, pelo menos, que, não existindo, no nosso ordenamento, qualquer habilitação constitucional para circunscrever o direito à reserva da vida privada a uma esfera pessoal íntima, deve entender-se que a privacidade (privacy) tem âmbito mais vasto (MIRANDA, Jorge; MEDEIROS, Rui – **Constituição Portuguesa Anotada**. Lisboa: Universidade Católica, 2017. Vol. 1, p. 452-453).

⁴² FESTAS, David de Oliveira – O direito à reserva da intimidade da vida privada do trabalhador no Código do Trabalho. **Revista da Ordem dos Advogados (ROA)** [Em linha]. Ano 64, Vol. I-II (nov. 2004), p. 1 [Em linha]. [Consult. 02 fev. 2022]. Disponível em: <https://portal.oa.pt/publicacoes/revista-da-ordem-dos-advogados-roa/ano-2004/ano-64-vol-i-ii-nov-2004/artigos-doutriniais/david-de-oliveira-festas-o-direito-a-reserva-da-intimidade-da-vida-privada-do-trabalhador-no-codigo-do-trabalho-star/>.

⁴³ Nesse sentido, cf. CORREIA, Victor – Sobre o Direito à privacidade. **O Direito**. [Em Linha] Ano 146, n.º 1 (2014), p. 9-32, p. 12. [Consult. 17 jul. 2022]. Disponível em: https://www.academia.edu/6106718/Sobre_o_direito_%C3%A0_privacidade.

1.2 Conteúdo do direito à reserva sobre a intimidade da vida privada no ordenamento jurídico português e brasileiro

Segundo os ensinamentos do Professor Mota Pinto, ao buscarmos o conteúdo do direito à reserva da intimidade, devemos conduzir pelo interesse que esse direito visa proteger. Acrescenta, entretanto, que é possível aproveitar a sugestão semântica que nos dá a expressão *reserva sobre a vida privada* e, com isso, sugere que iniciemos com o significado do que é *vida privada* e apenas posteriormente partamos para o exame da palavra *intimidade*, para verificar se há algo a mais que agregue ao significado, para, por fim, chegar ao que consiste na reserva exigida⁴⁴.

Assim como a lei francesa, artigo 9 do Código Civil francês, a lei portuguesa utiliza a expressão *vida privada* para tutela da privacidade em contraposição ao que seria a *vida pública*⁴⁵. Nesse contexto, a vida pública diria respeito a um domínio público e “vida privada” diria respeito apenas aos particulares e abrangeria o “pequeno mundo do qual cada um é rei e senhor”⁴⁶. Haveria, então, uma certa relativização nesse aspecto, a depender das circunstâncias fáticas e das pessoas envolvidas⁴⁷, o que faria surgir novas hipóteses a ponto de “não sabermos em muitos casos se estamos perante a vida privada de outrem”. Por essa razão, esclarece o professor que se faz necessário o estabelecimento de uma diretriz geral, orientando-a com conformidade com critérios objetivos, os quais “só podem ser os que resultam das valorações sociais correntes sobre a questão, desde que harmonizáveis com princípios gerais do ordenamento jurídico nesta matéria e, portanto, que além de a própria noção da vida ser em certa medida dependente do indivíduo, é também função das valorações de cada formação social”⁴⁸, devendo este ser o critério geral.

Exemplificativamente, então, o conteúdo da vida privada seria a identidade da pessoa, marcas ou sinais de identidade, seu número de telefone e endereço, endereço de *e-mail*, dados

⁴⁴ MOTA PINTO, Paulo – O direito à reserva da intimidade. **Boletim da Faculdade de Direito: Universidade de Coimbra**. Vol. LXIX (1993), p. 479-586, p. 524-526.

⁴⁵ “[...] tem-se defendido, a propósito da primeira questão, que a vida privada é toda a vida que não é pública. A vida privada cessa onde começa a vida pública, incluindo, nomeadamente, aspectos relativos à vida doméstica, familiar, sexual e afetiva, bem como o estado de saúde das pessoas” (DRAY, Guilherme – O direito à reserva da intimidade da vida privada: o artigo 80.º do Código Civil de 1966. **Revista de Direito Civil**. Ano II, n.º 3 (2017). p. 673-699, p. 678-679).

⁴⁶ MOTA PINTO, Paulo – O direito à reserva da intimidade. **Boletim da Faculdade de Direito: Universidade de Coimbra**. Vol. LXIX (1993), p. 479-586, p. 524-526.

⁴⁷ N.º 2, do artigo 80.º. Do Código Civil.

⁴⁸ Nesse sentido: “As considerações anteriores não significam, obviamente, que no âmbito da vida privada que deve permanecer reservado seja, em qualquer caso, idêntico. Pelo contrário, para além desse alcance genérico do direito à reserva da intimidade da vida privada, tudo depende, em última análise, da adequada ponderação da diversidade de situações em que o problema se coloca e da própria condição das pessoas” (MIRANDA, Jorge; MEDEIROS, Rui – **Constituição Portuguesa Anotada**. Lisboa: Universidade Católica, 2017. Vol. 1, p. 454).

de saúde, preferência afetiva, hábitos sexuais, casamento e divórcio, afetos e ódios, a vida do lar. Independentemente do local, mesmo em local público, há aspectos que continuam sendo circunscritos à “vida privada”, como a discussão de um casal em um estabelecimento aberto ao público em geral. Há que se compreender que as palavras ali ditas e o conteúdo do diálogo diz respeito à esfera privada, assim como as correspondências e telecomunicações. O patrimônio e situação financeira da pessoa também integram a esfera da “vida privada”⁴⁹.

Mas que sentido deve ser dado à referência ao termo *intimidade* constante do n.º 1 do artigo 80.º do Código Civil português^{50,51}?

O termo *intimidade* serve ao propósito de delinear melhor o interesse em causa, donde estariam excluídos dos aspectos já aqui abordados, a proteção de outras questões da vida privada. Assim estaria protegida a intimidade da vida privada, mas não a liberdade da vida privada, no sentido de que somente os aspectos íntimos, ligados ao domínio mais particular das pessoas, estariam tutelados, aquele que “seria o que normalmente se exclui de todo o conhecimento alheio”⁵². Dessa forma, aspectos da vida não íntima, tais quais da vida profissional, não seriam considerados íntimos e, ainda, também seriam excluídos aqueles fatos que, apesar de comporem a vida privada, normalmente não se resguarda dos outros.

Por fim, o termo *reserva*, em “reserva sobre a intimidade da vida privada”, incluindo-se tanto fatos verdadeiros quanto falsos, na medida em que se tutela a privacidade, não estando em causa a reputação ou honra, de modo que é objeto de proteção mesmo o segredo da desonra, não sendo admitida a exceção da verdade⁵³. A tutela do direito sobre a “reserva sobre a intimidade da vida privada” engloba tanto a proibição da tomada de conhecimento e a divulgação da informação, que correspondem à tutela do segredo no sentido de não intrusão⁵⁴ (proibição de ações dirigidas à tomada de conhecimento) e da não difusão⁵⁵.

⁴⁹ MOTA PINTO, Paulo, *op. cit.*, p. 529-530.

⁵⁰ PORTUGAL. Ministério da Justiça – Decreto-Lei nº 47.344/66, de 25 de novembro (Código Civil português). **Diário do Governo** [Em linha]. Série I (25 nov. 1966), p. 1883-2086. [Consult. 10 abr. 2022]. Disponível em: <https://dre.pt/dre/detalhe/decreto-lei/47344-1966-477358>

⁵¹ “Artigo 80.º (Direito à reserva sobre a intimidade da vida privada). 1. Todos devem guardar reserva quanto à intimidade da vida privada de outrem. 2. A extensão da reserva é definida conforme a natureza do caso e a condição das pessoas (MOTA PINTO, Paulo; MONTEIRO, João Pinto – **Código Civil e legislação complementar e jurisprudência**. 2.ª ed. Lisboa: INCM, 2016, p. 86).

⁵² MOTA PINTO, Paulo – O direito à reserva da intimidade. **Boletim da Faculdade de Direito: Universidade de Coimbra**. Vol. LXIX (1993), p. 479-586, p. 531.

⁵³ *Ibid.*, p. 533.

⁵⁴ A “intrusão” pode acontecer pela captação de filmes e fotografias, retratos da vida íntima da pessoa, gravações de voz na vida privada, bem assim como casos de violação de domicílio, ou de correspondência e conversas telefônicas (*ibid.*, p. 535).

⁵⁵ A divulgação por relator verbais, de artigos de jornais e revistas, na internet, redes sociais e afins, por meio de radiodifusão ou televisão, comercialização de gravações, publicação de livros sobre a vida privada (*ibid.*, *loc. cit.*).

O núcleo fundamental do direito à reserva da vida privada, contido no artigo 80.º, n.º 1, é o direito de controle (autodeterminação) sobre a informação relativa à esfera da vida privada⁵⁶. Segundo Mota Pinto, inclusive em se tratando de direito à reserva, “é de aceitar a extensão da noção de ‘direito à autodeterminação informativa’ para além do domínio do tratamento de dados pessoais – como aspecto do ‘direito geral de personalidade’⁵⁷ –, e abrangendo a proteção perante a intrusão no domínio pessoal e a tutela perante a divulgação de afirmações pessoais e factos verdadeiros”⁵⁸.

No direito à reserva da vida privada não está apenas em causa a inviolabilidade física ou pessoal do titular, mas a sua autodeterminação informativa em relação à vida privada, o que, ainda de acordo com o autor, faria incorporar ao direito em questão um componente de liberdade, liberdade esta que integra o próprio bem protegido (informação privada, informação da vida privada)^{59,60}. O mesmo direito, tendo em consideração que a informação cujo controle nos referimos é apenas aquela relativa à vida privada do indivíduo, é conformado pela atuação deste, de modo que o consentimento com o ato violador é causa de exclusão de ilicitude. Ou seja, a atuação voluntária do titular do direito à reserva da intimidade no sentido de dispor dele implica na licitude do ato que de outro modo seria tido por violador (ilícito)⁶¹.

Os limites do direito à reserva da intimidade da vida privada se encontram previstos n.º 2, do artigo 80.º, do Código Civil, onde se estabelece que “a extensão da reserva definida conforme a natureza do caso e as condições das pessoas”⁶², por isso estão excluídos dos limites da reserva da intimidade da vida privada, que, por sua vez, se encontram tutelados no direito à liberdade (artigo 27.º, n.º 1, Constituição da República Portuguesa)⁶³.

⁵⁶ A Autodeterminação informacional e consequente obrigatoriedade da proteção de dados pessoais foi uma tendência europeia a partir da segunda metade do século XX. *Vide* comentários ao artigo 80.º em PRATA, Ana (coord.) – **Código Civil Anotado. Volume I (Artigos 1.º a 1250.º)**. Coimbra: Almedina, 2019, p. 123.

⁵⁷ Em referência ao direito geral de personalidade, confira-se CANOTILHO, José Joaquim Gomes; MOREIRA, Vital – **Constituição da República Portuguesa Anotada**. 4.ª ed., rev. Coimbra: Coimbra, 2014. Vol. 1, p. 463: “Na qualidade de expressão geral de uma esfera de liberdade pessoal, ele constitui um direito subjectivo fundamental do indivíduo, garantindo-lhe um direito à formação livre da personalidade de acção como sujeito autónomo dotado de autodeterminação decisória, e um direito de personalidade fundamentalmente garantidor da sua esfera jurídico pessoal e, em especial, da integridade desta”.

⁵⁸ MOTA PINTO, Paulo – A limitação voluntária do direito à reserva sobre a intimidade da vida privada. **Separata de Estudos em homenagem a Cunha Rodrigues** [Em linha]. Coimbra: Coimbra, 2001, p. 3. [Consult. 02 fev. 2022] Disponível em: <https://xdocs.com.br/doc/limitacao-do-direito-a-reserva-xn45y7x343oj>.

⁵⁹ *Ibid.*, p. 4.

⁶⁰ No mesmo sentido, MIRANDA, Jorge; MEDEIROS, Rui – **Constituição Portuguesa Anotada**. Lisboa: Universidade Católica, 2017. Vol. 1, p. 446.

⁶¹ MOTA PINTO, Paulo, *op. cit.*, p. 4.

⁶² PORTUGAL – **Constituição da República Portuguesa**. 2.ª ed. Lisboa: INCM, 2016, p. 36.

⁶³ A respeito do direito à reserva da intimidade da vida privada, Guilherme Dary: “O que mais importante se retira do preceito em causa é que todos devem guardar quanto à intimidade da vida de outrem (n.º 1), sendo

O perímetro da reserva ou limites da reserva sobre a vida privada e familiar contida no n.º 2 está definido em atenção à “natureza do caso” e à “condição das pessoas”, pelo que somente diante do caso concreto se poderia averiguar o que está ou não está compreendido no âmbito da reserva⁶⁴. A vida privada compreende, assim, um conjunto de atividades, atitudes e comportamentos que não têm relação com a vida pública, estando apartados dela e ligados à esfera individual e familiar do indivíduo. Não seria possível, a princípio, fazer-se uma enumeração exaustiva de seu conteúdo, nem o legislador teve tal pretensão, fazendo uso de uma cláusula geral⁶⁵.

A privacidade também é tutelada na esfera penal. O Código Penal define em um capítulo intitulado “Dos crimes contra a reserva da vida privada” (artigos 176.º ao 185.º), os crimes de introdução em casa alheia” (artigo 176.º) ou em outro local vedado ao público (artigo 177.º); a intrusão na vida privada através da interceptação de conversas ou comunicações, captação, registro ou divulgação de imagens e pela observação de pessoas (artigo 180.º), bem como a divulgação de fatos relacionados à intimidade da vida privada (art. 178.º). Também são incriminadas as condutas de violação de segredo de correspondência ou de telecomunicações (artigo 183.º), violação do segredo profissional (artigo 184.º), a gravação e a fotografia ilícitas (artigo 179.º) e, finalmente, no que toca à informática, a devassa por meio da informática (artigo 181.º)⁶⁶.

O direito à reserva da intimidade encontra-se previsto na Constituição da República Portuguesa, no art. 26.º, n.º 1, no qual se dispõe que “a todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação”⁶⁷, preceituando, no n.º 2, que a lei estabelecerá garantias contra a utilização abusiva, ou contrária à dignidade

certo que o teor o reconhecimento do direito em causa varia consoante a natureza do caso e a condição das pessoas (n.º 2). O direito à reserva da intimidade da vida privada não é, portanto, nem um direito absoluto, nem um direito uniformemente aplicável: a sua aplicação deve variar em função dos elementos materiais fornecidos pelo caso concreto, à luz de um sistema móvel” (DRAY, Guilherme – O direito à reserva da intimidade da vida privada: o artigo 80.º do Código Civil de 1966. **Revista de Direito Civil**. Ano II, n.º 3 (2017). p. 673-699, p. 678).

⁶⁴ GONZÁLEZ, José Alberto Rodríguez Lorenzo – **Código Civil Anotado. Parte Geral**. Lisboa: Quid Iuris, 2019. Vol. 1, p. 139.

⁶⁵ PRATA, Ana (coord.) – **Código Civil Anotado. Volume I (Artigos 1.º a 1250.º)**. Coimbra: Almedina, 2019, p. 123.

⁶⁶ No sentido de que a doutrina penalista portuguesa adotaria a teoria das três esferas, cf.: CORREIA, Victor – Sobre o Direito à privacidade. **O Direito**. [Em Linha] Ano 146, n.º 1 (2014), p. 9-32, p. 12. [Consult. 17 jul. 2022]. Disponível em: https://www.academia.edu/6106718/Sobre_o_direito_%C3%A0_privacidade.

⁶⁷ PORTUGAL. Assembleia da República – **Constituição da República Portuguesa de 1976** [Em linha]. Lisboa, 1976. [Consult. 10 nov. 2019]. Disponível em: <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>.

humana, de informações relativas às pessoas e famílias”, no n.º 3, que “a lei garantirá a dignidade pessoal e a identidade genética do ser humano, nomeadamente na criação, desenvolvimento e utilização das tecnologias e na experimentação científica” e, por fim, no n.º 4, “a privação da cidadania e as restrições à capacidade civil só podem efectuar-se nos caos e termos previstos em lei, não podendo ter como fundamento motivos políticos”⁶⁸.

Entre nós, importa-nos salientar a expressa referência constitucional “à protecção legal contra quaisquer formas de discriminação”, bem assim como a delegação à norma infraconstitucional dos meios de garantia dessa mesma protecção “contra a utilização abusiva, ou contrária à dignidade humana, de informações relativas às pessoas e famílias”, além da garantia “à dignidade pessoal [...] nomeadamente na criação, desenvolvimento e utilização das tecnologias e na experimentação científica”. Nesse sentido, observamos a preocupação do legislador constitucional com a protecção contra a discriminação, e a missão (delegada) à norma infraconstitucional no que toca à protecção das informações relativas às pessoas e famílias, contra sua utilização abusiva das novas tecnologias e violadora do valor maior constitucional, a dignidade humana.

Gomes Canotilho e Vital Moreira afirmam que do direito fundamental à reserva sobre a intimidade da vida privada e familiar “deverá delimitar-se com base no conceito de ‘vida privada’ que tenha como referência civilizacional sob três aspectos: (i) o respeito dos comportamentos; (ii) o respeito do anonimato; (iii) o respeito da vida em relação. Todas essas dimensões devem ser convocadas para eventuais renúncias à protecção da intimidade da vida privada (ex.: caso Big-Brother)”⁶⁹.

A partir da quarta revisão constitucional, em 1997, foi acrescentado no n.º 1 a referência aos direitos “ao desenvolvimento da personalidade” e “à protecção legal contra quaisquer formas de discriminação”, fazendo introduzir, ainda, o n.º 3. Além disso, a revisão constitucional de 2004 teria sido responsável por explicitar, no n.º 2, que “as garantias efetivas nele previstas valem não apenas contra a utilização, mas também contra a obtenção abusiva, ou contrária à dignidade humana, de informações relativas às pessoas e famílias”^{70,71}.

⁶⁸ PORTUGAL. Assembleia da República – **Constituição da República Portuguesa de 1976** [Em linha]. Lisboa, 1976. [Consult. 10 nov. 2019]. Disponível em: <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>.

⁶⁹ CANOTILHO, José Joaquim Gomes; MOREIRA, Vital – **Constituição da República Portuguesa Anotada**. 4.ª ed., rev. Coimbra: Coimbra, 2014. Vol. 1, p. 468.

⁷⁰ MIRANDA, Jorge; MEDEIROS, Rui – **Constituição Portuguesa Anotada**. Lisboa: Universidade Católica, 2017. Vol. 1, p. 440.

⁷¹ SOUZA, Marcelo Rebelo de; ALEXANDRINO, José de – **Constituição da República Portuguesa: comentada: introdução teórica e histórica, anotações, doutrina e jurisprudência, Lei do Tribunal Constitucional**. Lisboa: Lex, 2000, p. 109-111.

Assim como fizemos, os mesmos autores alertam para o fato de que “o artigo 26.º constitui expressão direta do postulado básico da dignidade humana”, bem como “que a Constituição consagra ao longo do artigo 1.º como valor básico logicamente anterior à própria ideia de Estado de Direito democrático e que constitui a referência primeira em matéria de direitos fundamentais. [...] Por ser impressão do postulado básico do respeito pela dignidade humana⁷², o princípio consignado neste artigo 26.º constitui ‘pedra angular’ na demarcação dos limites ao exercício de outros direitos fundamentais. [...] A especial força normativa dos direitos pessoais aqui consagrados é aliás confirmada pelo regime processual privilegiado que a Constituição impõe para a sua tutela e pelo fato de alguns deles não poderem ser sequer afetados pela declaração do estado de sítio ou do estado de emergência (artigo 19.º, n.º 6, da Constituição)”⁷³. Nesse contexto, afirmam que não seria de se admirar que no mesmo art. 26.º possam ser reconhecidos direitos da personalidade não tipificados na Constituição, como o direito à autodeterminação informacional, bem assim como à identidade pessoal, que é o que concretiza cada pessoa enquanto unidade individualizada e que se diferencia de todas as outras pessoas, ligando-se, por conseguinte, à proibição de discriminação constante do artigo 13.º, n.º 2, na medida em que as características identificadas nas pessoas são, geralmente, constitutivas da identidade pessoal⁷⁴.

O “direito ao desenvolvimento da personalidade” teria duas dimensões diferentes: o direito geral de personalidade e a liberdade geral de ação. O primeiro abrangeria o direito à palavra, ao silêncio, à resposta na comunicação social e à autodeterminação informativa. Por outro lado, da liberdade da ação, apresentaria o “ônus de fundamentar do poder legislativo: é o poder que terá de justificar a coerção e não as pessoas, a sua liberdade”^{75,76}.

Em seus comentários ao artigo 26.º os autores esclarecem que hoje se reconhece uma outra dimensão ao direito à reserva sobre a intimidade da vida privada, “traduzida na faculdade dos cidadãos de controlarem as informações que lhe dizem respeito”. Nesse

⁷² Nesse sentido, o professor Canotilho coloca como caráter fundamente da liberdade digna e da dignidade livre do homem, como princípio fundamental (CANOTILHO, José Joaquim Gomes – **“Brancos” e Interconstitucionalidade: Itinerários dos Discursos Sobre a Historicidade Constitucional**. Coimbra: Almedina, 2008, p. 175 *et seq.*).

⁷³ MIRANDA, Jorge; MEDEIROS, Rui – **Constituição Portuguesa Anotada**. Lisboa: Universidade Católica, 2017. Vol. 1, p. 443.

⁷⁴ *Ibid.*, p. 444.

⁷⁵ *Ibid.*, p. 446.

⁷⁶ Por sua vez, para Canotilho e Vital Moreira o direito ao desenvolvimento da personalidade pressuporia 3 elementos nucleares: (i) a possibilidade de interiorização autónoma” da pessoa ou direito a “auto-afirmação” em relação a si mesmo, contra quaisquer imposições heterónomas (de terceiros ou dos poderes públicos); (ii) o direito à criação ou aperfeiçoamento de pressupostos indispensáveis ao desenvolvimento da personalidade (CANOTILHO, José Joaquim Gomes; MOREIRA, Vital – **Constituição da República Portuguesa Anotada**. 4.ª ed., rev. Coimbra: Coimbra, 2014. Vol. 1, p. 464).

perspectiva, citam que a tutela constitucional da reserva sobre a intimidade da vida privada confere aos cidadãos a faculdade de conservar à esfera privada e reservada todos os dados pessoais que pertencem à sua vida privada e familiar, dispondo o titular do direito de impedir o acesso, emprego e revelação dos dados, caso não tenham sido previamente autorizados, bem como se beneficiando do direito de conhecimento, retificação, atualização e eliminação, reconhecendo, por fim, o direito à autodeterminação informacional emergente do referido dispositivo constitucional (do direito ao desenvolvimento da personalidade), o qual seria o direito que cada titular de dados (indivíduo) tem de dispor livremente dos respectivos dados e informações pessoais, bem como de determinar os termos de acessos e utilização por terceiros desses mesmos dados e informações. No mesmo sentido, ainda, disporia o n.º 2 do artigo 26.º, quando remete à lei, o estabelecimento de “garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias”⁷⁷.

Na expressão de Canotilho e Vital Moreira, está em causa uma tríplice referência civilizacional: o respeito dos comportamentos, o respeito do anonimato e o respeito da vida em relação⁷⁸.

Na análise constitucional também não podem nos escapar outros direitos fundamentais que também têm vieses de proteção da intimidade da vida privada, qual seja, o artigo 35.º, que se relaciona à correta utilização da informática e tem especial importância para o nosso tema, que trata das decisões automatizadas, na medida que dispõe expressamente sobre direitos dos titulares de dados pessoais, estabelecendo que “a lei definirá as condições aplicáveis ao tratamento automatizado” (n.º 2) e que “a informática não poderá ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expreso do titular, autorização prevista em lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis” (n.º 3).

A redação do artigo 35.º sofreu grandes alterações desde a sua inclusão no texto constitucional, notadamente para adequação do conteúdo às diretivas comunitárias que entraram em vigor sobre a matéria (Diretiva n.º 95/46/CE). O n.º 3 foi introduzido pela reforma de 1982 e sofreu alterações em 1997 com a inclusão do “consentimento expreso” do

⁷⁷ MIRANDA, Jorge; MEDEIROS, Rui – **Constituição Portuguesa Anotada**. Lisboa: Universidade Católica, 2017. Vol. 1, p. 452.

⁷⁸ CANOTILHO, José Joaquim Gomes; MOREIRA, Vital – **Constituição da República Portuguesa Anotada**. 4.ª ed., rev. Coimbra: Coimbra, 2014. Vol. 1, p. 464.

titular e autorização legal com “garantias de não discriminação” entre as causas de justificação para utilização de dispositivos informáticos para tratamento de dados pessoais⁷⁹.

A lei responsável pela transposição da Directiva 95/46/CE para o ordenamento português foi a Lei n.º 67/98⁸⁰, de 26 de outubro. Esta lei acabou revogada pela Lei n.º 58/2019⁸¹ (Lei de Execução do Regulamento Geral de Proteção de Dados), que assegura a execução, na ordem nacional portuguesa, do Regulamento (UE) 2016/679 do Parlamento e do Conselho ou Regulamento Geral de Proteção de dados ao qual nos referiremos apenas como Regulamento Europeu.

Jorge Miranda e Rui Medeiros afirmam que “não existe um consenso absoluto quanto ao modelo constitucional a seguir como forma de assegurar as faculdades individuais que integram o conteúdo essencial do direito à proteção de dados pessoais perante o uso das novas tecnologias e, em particular, da informática. Além da natureza fortemente ‘instável’ do objeto da regulação que torna precária a intervenção constitucional neste domínio, as opiniões e as legislações dividem-se entre a necessidade de garantir um direito fundamental autónomo, e a consideração do direito à proteção dos dados pessoais como parte integrante do âmbito de tutela de outro direito fundamental”⁸².

Para Cunha Rodrigues “a convivência entre a informática e a intimidade privada tornou-se de tal modo intensa que justificou uma série de recomendações e resoluções de instâncias internacionais que abrangem domínios tão diferentes como são os do emprego, da segurança social, da polícia, do marketing, da estatística, da proteção de utilizadores, dos bancos de dados médicos, do sector público e do sector privado. Curiosamente, em muitos casos, a tutela da privacidade associa-se à ideia de protecção da dignidade humana, dando razão aos que defendem que, neste domínio, só uma perspectiva integrada nos pode salvar do universo profetizado por Orwell”⁸³.

⁷⁹ MIRANDA, Jorge; MEDEIROS, Rui, *op. cit.*, p. 780.

⁸⁰ PORTUGAL. Procuradoria-Geral Distrital de Lisboa – Lei n.º 67/98, de 26 de outubro (Lei de Proteção da Dados Pessoais). **Diário da República** [Em linha]. N.º 247, Série I-A (26 out. 1998). [Consult. 17 jul. 2022]. Disponível em: <https://dre.pt/dre/legislacao-consolidada/lei/1998-34450175>.

⁸¹ *Id.* Assembleia da República – Lei n.º 58/2019, de 8 de agosto. Lei da Proteção de Dados Pessoais. Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Diário da República** [Em linha]. N.º 151, Série I (08 ago. 2019), p. 3-40. [Consult. 13 set. 2022]. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=3118A0002&nid=3118&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=.

⁸² MIRANDA, Jorge; MEDEIROS, Rui – **Constituição Portuguesa Anotada**. Lisboa: Universidade Católica, 2017. Vol. 1, p. 783.

⁸³ RODRIGUES, Cunha – Informática e a reserva da vida privada. Comunicação e Defesa do Consumidor. **Atas do Congresso Internacional organizado pelo Instituto Jurídico da Comunicação da Faculdade de Direito da Universidade de Coimbra, de 25 a 27 de novembro de 1993**. Coimbra, 1996. p. 287-292, p. 290.

No Brasil, a Constituição Federal de 1988 incluiu no rol dos direitos fundamentais elencados no artigo 5.º a proteção da intimidade e da vida privada.⁸⁴ Não da intimidade da vida privada” como fez a Constituição portuguesa, mas da “intimidade” e da “vida privada”, ambas expressões contidas no inciso X, fazendo notar que a proteção do indivíduo abrange esses aspectos, além da “honra” e da “imagem”, “cabendo ao intérprete a sua determinação”⁸⁵, opção que encontra justificativa no desenvolvimento legislativo, histórico e doutrinário. Além disso, a inviolabilidade de correspondência e do domicílio, onde se inclui o direito à privacidade, estão presentes em todas as constituições Brasileiras desde a Constituição do Império de 1824⁸⁶.

Por outro lado, Danilo Doneda esclarece que “a terminologia da Constituição brasileira deve, porém, ser lida em razão do contexto no qual se encontram os direitos fundamentais que visa proteger”, por isso considera “não ser frutífero insistir em uma conceptualística que intensifique as conotações e diferenças dos dois termos”, posto que “cada um deles possui campo semântico próprio”, acrescentando que “tais termos podem ser integrados através da atividade interpretativa e, nesse caso, autorizada doutrina reconhece a identidade dos dois termos e propõe a atuação de suas particularidades”⁸⁷. Por fim, o próprio autor acaba por escolher utilizar o termo *privacidade*, entendendo ser a opção mais razoável, por ser “específico o suficiente para que se distinga de outras locuções com as quais eventualmente deve medir-se, como a imagem, honra ou a identidade pessoal; e também é claro bastante para especificar seu conteúdo, efeito da sua atualidade”. A escolha, então, “não é consequência da fragilidade das demais”, uma vez que “se revela por si só mais adequada, justamente por unificar os valores expressos nos termos intimidade e vida privada”⁸⁸.

A aceitação do termo *privacidade* na doutrina brasileira pode ser constatada em René Ariel Dotti, em *Proteção da vida privada e liberdade de informação*⁸⁹, de 1980; Celso

⁸⁴ BRASIL. Presidência da República – **Constituição da República Brasileira de 1988 [Em linha]**. Brasília, 1988. [Consult. 10 nov. 2019]. Disponível em: <http://www.planalto.gov.br/ccivil/03/constituicao/constituicao.htm>.

⁸⁵ DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**. 2.ª ed. São Paulo: Revista dos Tribunais, 2019, p. 103.

⁸⁶ MARINELI, Marcelo Romão – **Privacidade e redes sociais virtuais**. Rio de Janeiro: Lumen Juris, 2017, p. 94.

⁸⁷ DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**. 2.ª ed. São Paulo: Revista dos Tribunais, 2019, p. 104-105.

⁸⁸ *Ibid.*, p. 106.

⁸⁹ DOTTI, René Ariel – **Proteção da vida privada e liberdade de informação [Em linha]**. São Paulo: Revista dos Tribunais, 1980. [Consult. 01 maio 2022]. Disponível em: <http://localhost:8080/xmlui/handle/123456789/1303>.

Ribeiro Bastos, em 1989, em seu *Curso de Direito Constitucional*⁹⁰; Tércio Sampaio Ferraz, em 1993, em *Sigilo de dados: direito à privacidade e os limites à função fiscalizadora do Estado*⁹¹; José Adércio Leite Sampaio, em 1998, em *Direito à intimidade e à vida privada*⁹²; Caitlin Sampaio Mulholland, em 2018, em *Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18)*⁹³.

Como em Portugal, no Brasil, o princípio da dignidade humana é fundamento do Estado, servindo de “base valorativa para de sustentação de toda e qualquer situação jurídica de Direito Privado. Sua inclusão no texto constitucional representou a escolha sociocultural-jurídica por uma sociedade solidária e justa, proporcionadora do livre desenvolvimento pessoal de seus cidadãos”, sendo o Direito “chamado a dar concretude a este princípio através de uma atuação protetiva”⁹⁴.

Assim é que o artigo 21 do Código Civil brasileiro de 2002 dispõe que “a vida privada da pessoa natural é inviolável e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma”⁹⁵. A Lei de Acesso à Informação (Lei n.º 12.527/2011) estabelece a proteção às informações que estiverem em poder do Estado relacionadas à intimidade, vida privada, honra e imagem das pessoas, estabelecendo um limite de 100 anos para o acesso às informações pessoais (art. 31.º, § 1.º, inciso D), as quais só poderão ser divulgadas com consentimento expresso do titular. A Lei do Cadastro Positivo (Lei 12.414/2011) disciplina a formação e a consulta de bancos de dados com informações sobre o adimplemento de obrigações de pessoas naturais para a formação de histórico de crédito, nas condições previstas na mesma lei⁹⁶.

⁹⁰ BASTOS, Celso Ribeiro – **Curso de Direito Constitucional**. 17.ª ed. São Paulo: Saraiva, 1989. Vol. 2, p. 63.

⁹¹ FERRAZ, Tércio Sampaio – *Sigilo de dados: direito à privacidade e os limites à função fiscalizadora do Estado*. **Revista da Faculdade de Direito de São Paulo**. Vol. 88 (jan./dez. 1993), p. 439-459.

⁹² SAMPAIO, José Adércio Leite – **Direito à intimidade e à vida privada**. Belo Horizonte: Del Rey, 1998.

⁹³ MULHOLLAND, Caitlin Sampaio – *Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18)*. **Revista de Direitos e Garantias Fundamentais**. Vol. 19, n.º 3 (2018), p. 159-180. [Consult. 10 abr. 2022]. Disponível em: <https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603/pdf>.

⁹⁴ *Id.* – **Mercado, Pessoa Humana e Tecnologias: a Internet das Coisas e a proteção do direito à privacidade** [Em linha]. Rio de Janeiro: PUC-RJ, ago. 2021. [Consult. 07 maio 2022]. Disponível em: <https://www.jur.puc-rio.br/wp-content/uploads/2021/08/CAITLIN-SAMPAIO-Mercado-Pessoa-Humana-e-Tecnologias.pdf>.

⁹⁵ BRASIL. Presidência da República – Lei n.º 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União** [Em linha]. Seção 1 (11 jan. 2002), p. 1. [Consult. 10 abr. 2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm.

⁹⁶ “Art. 3º, § 1º Para a formação do banco de dados, somente poderão ser armazenadas informações objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado” (*id.* – Lei n.º 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. **Diário Oficial da União** [Em linha]. Seção 1 (10 jun. 2011), p. 2. [Consult. 20 jul. 2022].

O Código de Defesa do Consumidor (Lei n.º 8.078/1990) dispõe sobre o direito de acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre suas respectivas fontes (art. 43.º, *caput*), prevendo que as informações devem ser verdadeiras, claras e objetivas (art. 43.º, § 1.º); que a abertura do cadastro ou registro deve ser comunicado por escrito ao consumidor quando não solicitada por ele (art. 43.º, § 2.º); que o consumidor poderá exigir a correção de informação inexata a seu respeito, devendo o “arquivista” comunicar aos destinatários das informações incorretas a sua correção em 5 dias (art. 43.º, § 3.º). Por sua vez, a Lei n.º 12.965/2014 (Marco Civil da Internet) disciplinou princípios, garantias, direitos e deveres dos usuários da rede e abordou de maneira sistemática e específica as relações jurídicas estabelecidas na internet. Previu entre os direitos dos usuários da internet a (i) inviolabilidade da intimidade e da vida privada (art. 7.º, I); (ii) a preservação do sigilo das comunicações privadas transmitidas ou armazenadas (art. 7.º, II, III); (iii) a proteção contra o fornecimento de dados pessoais coletados pela internet a terceiros sem prévio consentimento do titular (art. 7.º, VII); (iv) o direito a informações claras e completas sobre o tratamento de dados pessoais (art. 7.º, VIII); e (v) a prerrogativa do consentimento expresso e destacado sobre o tratamento destes (art. 7.º, XI).

Por fim, no Brasil, em 2018, foi promulgada a Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018), primeiro compêndio legislativo brasileiro especificamente direcionado para a disciplina da proteção de dados pessoais no Brasil, possibilitando o surgimento de um ambiente de equilíbrio entre a proteção de direitos fundamentais de liberdade e de privacidade dos indivíduos e do livre desenvolvimento da personalidade da pessoa natural, de um lado, e o grande fluxo livre de dados pessoais que alimentam o comércio nacional e internacional, do outro. Seu principal objetivo foi trazer segurança jurídica estabelecendo padrões para o tratamento de dados pessoais, alinhando-se a parâmetros internacionais – faz-se referência aqui ao Regulamento Europeu⁹⁷ –, promovendo a livre iniciativa e desenvolvimento tecnológico⁹⁸.

Não menos importante foi a inclusão do “direito à proteção de dados pessoais, inclusive em meios digitais” (inciso LXXIX) pela Emenda Constitucional n.º 115, de 10 de

Disponível em: http://www.planalto.gov.br/ccivil_03/ato2011-2014/2011/lei/112414.htm. ISSN 1677-7042).

⁹⁷ UNIÃO EUROPEIA – Regulamento (EU) 2016/679 (General Data Protection Regulation - GDPR). **Jornal Oficial da União Europeia**. L119. (04 maio 2016), p. 1-88.

⁹⁸ Art. 1º e Art. 2º (BRASIL. Presidência da República – Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União** [Em linha]. N.º 157, Seção 1 (15 ago. 2019), p. 59-215. [Consult. 20 jul. 2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/113709.htm).

fevereiro de 2022⁹⁹, ao rol dos direitos e garantias fundamentais do art. 5.º da Constituição da República de 1988. Ela também teve a importante função de estabelecer a competência privativa da União Federal sobre proteção de dados pessoais, buscando evitar que Estados e Municípios – como já vinha ocorrendo – começassem a legislar sobre a matéria de modo a evitar o conflito com o regramento federal.

Tendo sido positivado em nível constitucional 46 anos depois de Portugal, o direito à proteção de dados pessoais já vinha sendo reconhecido em âmbito doutrinário e jurisprudencial, cabendo a referência à paradigmática decisão¹⁰⁰ da Ministra Rosa Weber, do Supremo Tribunal Federal, em que, em sede de liminar do bojo na Ação Direta de Inconstitucionalidade (ADI) n.º 6.387 MC-Ref/DF, publicada em 28 de abril de 2020, declarou o reconhecimento do direito à proteção de dados pessoais como direito fundamental autônomo¹⁰¹.

⁹⁹ BRASIL. Presidência da República – Emenda Constitucional n.º 115 de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial da União** [Em linha]. N.º 30, Seção 1 (11 fev. 2022), p. 2. [Consult. 24 jul. 2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm.

¹⁰⁰ Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165>.

¹⁰¹ “**14.** Entendo que as condições em que se dá a manipulação de dados pessoais digitalizados, por agentes públicos ou privados, consiste em um dos maiores desafios contemporâneos do direito à privacidade. A Constituição da República confere especial proteção à intimidade, à vida privada, à honra e à imagem das pessoas ao qualificá-las como invioláveis, enquanto direitos fundamentais da personalidade, assegurando indenização pelo dano material ou moral decorrente de sua violação (**art. 5º, X**). O assim chamado direito à privacidade (right to privacy) e os seus consectários direitos à intimidade, à honra e à imagem emanam do reconhecimento de que a personalidade individual merece ser protegida em todas as suas manifestações. A fim de instrumentalizar tais direitos, a Constituição prevê, no **art. 5º, XII, a inviolabilidade do “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 penal”. **15. O art. 2º da MP n. 954/2020** impõe às empresas prestadoras do Serviço Telefônico Fixo Comutado – STFC e do Serviço Móvel Pessoal – SMP o compartilhamento, com a Fundação Instituto Brasileiro de Geografia e Estatística – IBGE, da relação de **nomes, números de telefone e endereços** de seus consumidores, pessoas físicas ou jurídicas. Tais informações, relacionadas à **identificação – efetiva ou potencial – de pessoa natural**, configuram **dados pessoais** e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (**art. 5º, caput**), da privacidade e do livre desenvolvimento da personalidade (**art. 5º, X e XII**). Sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional. Decorrências dos direitos da personalidade, o respeito à **privacidade** e à **autodeterminação informativa** foram positivados, no art. 2º, I e II, da Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da **proteção de dados pessoais**. No clássico artigo *The Right to Privacy*, escrito a quatro mãos pelos juízes da Suprema Corte dos Estados Unidos Samuel D. Warren e Louis D. Brandeis, já se reconhecia que as mudanças políticas, sociais e econômicas demandam incessantemente o reconhecimento de novos direitos, razão pela qual necessário, de tempos em tempos, redefinir a exata natureza e extensão da proteção à privacidade do indivíduo. Independentemente do seu conteúdo, mutável com a evolução tecnológica e social, no entanto, permanece como denominador comum da privacidade e da autodeterminação o entendimento de que a privacidade somente pode ceder diante de justificativa consistente e legítima. Em seus dizeres, “*a invasão injustificada da privacidade individual deve ser reprimida e, tanto quanto possível, prevenida*”. **16. Cumpre, pois, equacionar se a MP n. 954/2020 exorbitou dos limites traçados pela Constituição ao dispor sobre a disponibilização dos dados pessoais de todos os consumidores dos serviços STFC e SMP, pelos respectivos operadores, a entidade integrante da Administração indireta**” (grifos da autora).

Nesta senda, parece-nos ser relevante a reprodução das palavras de Ingo Wolfgang¹⁰², a respeito da emenda e às discussões a respeito da conveniência da promulgação da emenda constitucional (que posteriormente foi aprovada, superando-se a discussão), em que faz referência à supracitada decisão liminar no sentido de que

[...] uma das perguntas que se colocava, pouco tempo faz, dizia respeito à necessidade e mesmo conveniência da aprovação e promulgação da PEC 17/19, de modo a incorporar um direito fundamental à proteção de dados pessoais ao catálogo de direitos e garantias da nossa CF. Tal questionamento, por sua vez, assume ainda maior relevo com a edição e iminente entrada em vigor da nova Lei Geral de Proteção de Dados Pessoais do Brasil — LGPD (Lei nº 13.709/2018, porquanto, embora tal legislação não sirva de base e justificação constitucional direta para o reconhecimento de um direito fundamental à proteção de dados pessoais, o conteúdo e o alcance da regulação legal (infraconstitucional) carece de limitação a partir do marco normativo constitucional, ainda mais levando em conta o leque de direitos fundamentais e mesmo outros bens e interesses de estatura constitucional por ela protegidos, mas também limitados. À míngua, portanto, de expressa previsão de tal direito, pelo menos na condição de direito fundamental explicitamente autônomo, no texto da CF, e a exemplo do que ocorreu em outras ordens constitucionais, o direito à proteção dos dados pessoais pode (e mesmo deve!) ser associado e reconduzido — exatamente como o fez o STF — a alguns princípios e direitos fundamentais de caráter geral e especial, como é o caso do princípio da dignidade da pessoa humana, do direito fundamental (também implicitamente positivado) ao livre desenvolvimento da personalidade, do direito geral de liberdade, bem como dos direitos especiais de personalidade mais relevantes no contexto, quais sejam — aqui nos termos da CF — os direitos à privacidade e à intimidade, e um direito à livre disposição sobre os dados pessoais, o assim designado direito à livre autodeterminação informativa. [...] o fato é que sua positivação formal, em sendo o caso, carrega consigo uma carga positiva adicional, ou seja, agrega (ou, ao menos, assim o deveria) valor positivo substancial em relação ao atual estado da arte no Brasil¹⁰³.

1.3 Proteção da intimidade da vida privada: tutela internacional e regional

A necessidade de tutela da privacidade há muito passou a ser universalmente sentida¹⁰⁴, pelo que cuidamos aqui das referências que entendemos mais significativas.

Iniciando pelos Estados Unidos, já citado anteriormente quanto ao conceito e conteúdo do direito à intimidade e o termo *privacy*, foi lá que o desenvolvimento de novas tecnologias — sempre elas — e a expansão do jornalismo sensacionalista nos finais do século XIX fizeram sentir a necessidade de tutela de forma mais acentuada, especialmente considerando os

¹⁰² Consultor Jurídico é Revista Eletrônica sobre Justiça e Direito criada em 1997. Disponível em: https://www.conjur.com.br/a/quem_somos.

¹⁰³ SARLET, Ingo Wolfgang – A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I. **Consultor Jurídico** [Em linha]. (11 mar. 2022). [Consult. 24 jul. 2022]. Disponível em: <https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protacao-dados-pessoais-direito-fundamental>.

¹⁰⁴ Para um panorama comparativo, com citação das doutrinas americana, italiana, alemã, francesa e espanhola, fazemos referência ao trabalho de Manuel Iglesias Cubría, catedrático de direito civil na Universidade de Oviedo, *El derecho a la intimidad* (IGLESIAS CUBRÍA, Manuel – **El Derecho a La Intimidad**. Discurso Inaugural del año académico 1970-1971 [Em linha]. Oviedo: Universidad de Oviedo, 1970). [Consult. 10 abr. 2022]. Disponível em: <https://core.ac.uk/download/pdf/71852292.pdf>).

valores que enformam e enformavam aquela sociedade, centrada na defesa do indivíduo, das liberdades individuais e de seu espaço próprio. Foram Samuel Warren e Louis Brandeis, em seu *The right to privacy*, que aproximaram o “direito de ser deixado só” da tutela da personalidade; desde então, o direito à privacidade ganhou a tutela generalizada da doutrina e jurisprudência¹⁰⁵.

Em 1965, o Tribunal do Estado de Connecticut reconheceu pela primeira vez a possibilidade de se proibir o uso de contraceptivos, no caso *Griswold v. Connecticut*^{106,107}, com fundamento na constituição americana. O citado caso aproximou o direito à privacidade da tutela de liberdades individuais e passou a ser invocado com sucesso em alguns casos para sustentar o afastamento de outras restrições legais, como a proibição de abortar, da eutanásia, do uso de cabelos compridos por certos profissionais, da posse de material obsceno, de práticas homossexuais e o porte de drogas leves. Assim, a *privacy*, antes ligada diretamente à informação sobre a pessoa, começa a se identificar com todos os direitos fundamentais e tem a ver com a liberdade dos indivíduos¹⁰⁸.

Em 1974 foi publicado o “Privacy Act”, que nada mais é do que a primeira lei de privacidade norte-americana que estabelece um código de práticas de informações justas que rege a coleta, a manutenção, o uso e a disseminação de informações sobre a pessoa natural, que são mantidas em sistemas de registros por órgãos federais. Um “sistema de registros” referido é um grupo de registros sob o controle de uma agência do qual as informações são recuperadas pelo nome do indivíduo ou por algum identificador atribuído ao indivíduo¹⁰⁹. A Lei de Privacidade em questão exige que as agências divulguem seus sistemas de registros por meio de publicação no Registro Federal. Ela foi responsável pelo primeiro ato dirigido diretamente contra as instituições públicas e em proteção dos cidadãos e de suas garantias individuais de liberdade contra o Poder Público naquele país.

¹⁰⁵ MOTA PINTO, Paulo – O direito à reserva da intimidade. **Boletim da Faculdade de Direito: Universidade de Coimbra**. Vol. LXIX (1993), p. 479-586, p. 512.

¹⁰⁶ Referência do caso no sítio eletrônico de “Justia”, que é um fórum de advogados que sintetiza, comenta e analisa casos julgados pelas Cortes Norte Americana – (US SUPREME COURT – *Griswold v. Connecticut*, 381 U.S. 479 (1965)). **Justia**, 2022 [Em linha] [Consult. 10 abr. 2022]. Disponível em: <https://supreme.justia.com/cases/federal/us/381/479/>.

¹⁰⁷ Livre tradução do resumo do caso citado no sítio apontado na nota anterior: “Os apelantes, o Diretor Executivo da Planned Parenthood League of Connecticut, e seu diretor médico, um médico licenciado, foram condenados como cúmplices por fornecer informações e conselhos médicos a pessoas casadas sobre como evitar a concepção e, após exame, prescrever um dispositivo ou material contraceptivo para uso da esposa. Um estatuto de Connecticut torna crime qualquer pessoa usar qualquer droga ou artigo para evitar a concepção. Os apelantes alegaram que o estatuto acessório, conforme aplicado, violou a Décima Quarta Emenda. Um tribunal de apelação intermediário e o mais alto tribunal do Estado confirmaram a sentença”.

¹⁰⁸ MOTA PINTO, Paulo, *op. cit.*, p. 515.

¹⁰⁹ THE UNITED STATES. Department of Justice – **Privacy Act of 1974** [Em linha]. Washington, D.C., 1974. [Consult. 29 maio 2022]. Disponível em: <https://www.justice.gov/opcl/privacy-act-1974>.

Na Alemanha, Mota Pinto esclarece que a esfera íntima e a esfera do segredo das pessoas já possuía alguma “tradição” e teria sido “desentranhada do direito geral da personalidade”¹¹⁰, ocasião em que, a partir de então, após o reconhecimento do “direito geral de personalidade” pelo Supremo Tribunal Federal, passou-se a se recorrer a ele para a tutela da intimidade. O professor faz referência aos primeiros casos apontados na Alemanha. O primeiro, relacionado a fotografias não permitidas de Otto von Bismarck depois de morto, em julho de 1898, onde estaria mais em causa o direito à imagem do que o direito à privacidade. Acrescenta que, antes mesmo desse caso e antes da publicação da Warren e Bradeis, o direito à privacidade já havia sido tratado na Alemanha em 1880, muito embora não o tenha sido sob essa designação, por Josef Kohler, que tratava do “direito individual, que protege os segredos da vida interna de publicidade não autorizada”.

Em matéria de proteção de dados pessoais, a primeira lei sobre a matéria, que surgiu em 1977, foi substituída por outra, que entrou em vigor em 1979, qual seja, a Lei Federal de Proteção de Dados (Bundesdatenschutzgesetz, BDSG), que já passou por diversas revisões, inclusive para se adequar à Diretiva 95/46/CE¹¹¹. Cada estado federal na Alemanha conta com leis próprias de proteção de dados pessoais, as quais visam regulamentar o processamento e o uso de dados pelas autoridades públicas estaduais.

Na Itália, após alguns debates doutrinários nos anos 50, o “*diritto allá riservatezza*” se impôs e hoje não é contestado. Segundo Mota Pinto, Adriano de Cupis, em conhecida obra sobre direitos da personalidade, teria o compreendido como um direito que se manifestaria no direito ao segredo, distinguindo os diversos tipos de segredo. Somente em 1963 a Corte de Cassação Italiana veio a reconhecer um “direito absoluto de personalidade”, fundado no art. 2.º da Constituição, e a basear nele o direito à “*reservatezza*”; a partir dos anos 1970, a jurisprudência do país começou a se mostrar mais firme no reconhecimento do direito, que em 1975 já era reconhecido com direito autônomo^{112,113}.

Na França, o direito ao respeito à vida privada foi uma criação jurisprudencial. Uma lei de 1970 veio alterar o Código Civil francês para albergar a proteção à privacidade. No início, o respeito à vida privada, por vezes se confundindo com o direito à imagem, como o caso da atriz Rachel (“*affair Rachel*”), em que foi fotografada em seu leito de morte, ainda no

¹¹⁰ MOTA PINTO, Paulo – O direito à reserva da intimidade. **Boletim da Faculdade de Direito: Universidade de Coimbra**. Vol. LXIX (1993), p. 479-586, p. 512.

¹¹¹ Versão em inglês da BDSG pode ser acessada em: www.gesetze-imInternet.de/englisch_bdsge/.

¹¹² MOTA PINTO, Paulo, *op. cit.*, p. 518.

¹¹³ MIGLIETTI, Lucia – Profili storico-comparativi del diritto alla privacy. **Diritti Comparati: comparare i diritti fondamentali in Europa** [Em linha]. (04 dic. 2014). [Consult 10 abr. 2022]. Disponível em: <https://www.diritticomparati.it/profili-storico-comparativi-del-diritto-alla-privacy/>.

século XIX. Os primeiros casos em que o segredo da vida privada parece ser tratado autonomamente surgiram a partir de 1950, como é o caso de Brigitte Bardot. A atriz tinha 17 anos quando estrelou um filme em que aparecia de biquíni em cena, o que provocou a ira de seu pai, que, por sua vez, ajuizou procedimento judicial para impedir a exibição, mas perdeu a ação¹¹⁴.

O Direito sobre a reserva da intimidade da vida privada está consagrado em diversos documentos internacionais, notadamente europeus. É o caso da Declaração Universal dos Direitos do Humanos de 1948 (artigo 12.º)¹¹⁵, primeiro instrumento internacional a tutelar a intimidade da vida privada autonomamente, preceituando que “ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques, toda a pessoa tem direito a protecção da lei”, em prescrição que deve ser articulada com o princípio da dignidade, “inerente a todos os membros da família humana (fórmula extraída do primeiro considerando) e nos direitos fundamentais do homem, na dignidade e no valor da pessoa humana (quinto considerando)”¹¹⁶.

A mesma Declaração Universal dos Direitos humanos, ao tratar dos direitos do homem face ao desenvolvimento tecnológico, no artigo 27.º, proclama que “toda a pessoa tem o direito de tomar parte livremente na vida cultural da comunidade, de fruir as artes e de participar no progresso científico e nos benefícios que deste resultam”¹¹⁷.

¹¹⁴ Sobre o processo judicial: “O auge dos atritos envolvendo Brigitte e sua família aconteceria na ocasião do lançamento de seu primeiro filme. A produção se chamava ‘Manina, la fille sans voile’ e não economizava na sensualidade, trazendo fartas cenas de Bardot de biquíni, na praia, em cenas ousadas. Quando o filme foi lançado, o clã Bardot perdeu a paciência e tentando preservar sua ‘reputação moral’ resolveu tomar medidas duras, levando todos, de produtores ao diretor Vadim, aos tribunais. Tentando a todo custo proibir a exibição do filme os advogados da família Bardot alegavam que a produção ia contra todos os valores morais e religiosos do povo francês, contra a ética, contra o pudor e chegava ao ponto de acusar os realizadores de anti-cristãos e lascivos pois estariam pisando nos dogmas religiosos mais vitais ao sentimento da nação francesa! [...] Após uma longa batalha judicial o tribunal deu ganho de causa para os produtores do filme. [...] Por que proibir a beleza feminina afinal? O caso fez jurisprudência na justiça francesa e em vários outros países o exemplo foi seguido. Não havia como proibir uma obra de cinema apenas por uma questão moral de foro íntimo, pois a decência varia de pessoa para pessoa. O que pode ser considerado imoral para alguns pode não ser para outros. Na nova década não havia mais espaço para moralismos caducos e retrógrados como aquele. O biquíni de Bardot enfim vencera e ela, linda e graciosa, iria a partir daí iniciar um reinado nas telas mundiais que duraria vários anos para deleite de todos os cinéfilos ao redor do mundo” (PIPOCA 3D – Brigitte Bardot – **sensual e no tribunal** [Em linha]. 2022. [Consult. 23 jul. 2022]. Disponível em: <https://www.pipoca3d.com.br/2015/02/brigitte-bardot-sensual-e-no-tribunal.html>).

¹¹⁵ ONU. Organização das Nações Unidas – **Declaração Universal dos Direitos Humanos** [Em linha]. Paris, 10 dez. 1948. [Consult. 09 jun. 2022]. Disponível em: <https://brasil.un.org/sites/default/files/2020-09/por.pdf>.

¹¹⁶ PINHEIRO, José Alexandre Guimarães de Souza – **Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional** [Em linha]. Lisboa, 2012. Tese de doutorado em Direito (Ciências Jurídico-Políticas) apresentada à Universidade de Lisboa. (polic.º), p. 626. [Consult. 10 out. 2021]. Disponível em: <https://repositorio.ul.pt/handle/10451/7407?locale=en> ou Lisboa: AAFDL, 2015. ISBN 9786120002605.

¹¹⁷ ONU. Organização das Nações Unidas – *op. cit.*

Posteriormente, em novembro de 1950, foi adotada pelo Conselho da Europa a Convenção Europeia de Direitos Humanos¹¹⁸, que entrou em vigor em setembro de 1953; foi o primeiro texto com carácter vinculante após a proclamação da Declaração Universal dos Direitos Humanos, instituiu no n.º 1 do artigo 8.º o direito à reserva da intimidade da vida privada ao estabelecer que “qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência”¹¹⁹.

Em 1966, temos o Pacto Internacional de Direitos Civis e Políticos, que estabeleceu que “ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em se domicílio ou em sua correspondência, nem de ofensas ilegais a sua honra e reputação” (art. 17.º, § 1 e § 2)¹²⁰.

Em 23 janeiro de 1970, previa a Resolução n.º 428 da Assembleia Consultiva da Europa o conceito de *direito à vida privada* (§ C, n.º 16)¹²¹. Além do conceito nela estabelecido, a mesma resolução apontou os conflitos então existentes entre a liberdade de informação e de expressão e o direito à privacidade protegido no artigo 8.º da Convenção de Direitos Humanos, afirmando que o exercício do primeiro não poderia ser permitido para destruir a existência do último (“the exercise of the former right must not be allowed to destroy the existence of the latter” – § C, n.º 15).

Em particular, a resolução ainda teve mais um mérito, pois ressaltou os problemas então emergentes das tentativas de se obter informação por equipamentos modernos, tais como as escutas telefônicas, microfones ocultos e o uso de computadores, os quais infringiriam o direito à privacidade, acrescentando que onde os bancos de dados fossem estabelecidos o indivíduo não poderá ser completamente exposto pela acumulação de informações relacionadas à sua vida privada, bem como que, nesse contexto, os bancos de

¹¹⁸ TRIBUNAL EUROPEU DOS DIREITOS DO HOMEM. Council of Europe – **Convenção Europeia de Direitos Humanos** [Em linha]. Strasbourg, 2002. [Consult. 17 jul. 2022]. Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/convention_por.pdf.

¹¹⁹ *Ibid.*

¹²⁰ *Id.* Assembleia Geral – **Pacto Internacional de Direitos Civis e Políticos** [Em linha]. New York, 16 dez. 1966. [Consult. 17 jul. 2022]. Disponível em: https://www.cne.pt/sites/default/files/dl/2_pacto_direitos_civis_politicos.pdf.

¹²¹ “16. The right to privacy consists essentially in the right to live one's own life with a minimum of interference. It concerns private, family and home life, physical and moral integrity, honour and reputation, avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs, protection against misuse of private communications, protection from disclosure of information given or received by the individual confidentially. Those who, by their own actions, have encouraged indiscreet revelations about which they complain later on, cannot avail themselves of the right to privacy” (COUNCIL OF EUROPE. Parliamentary Assembly – **Resolution 428. Declaration on mass communication media and Human Rights** [Em linha]. New York, 23 Jan. 1970. [Consult. 17 jul. 2022]. Disponível em: <https://pace.coe.int/en/files/15842>).

dados deveriam ser restritos ao mínimo necessário de informação para cumprir aos propósitos da tributação, regimes de pensão, regimes de seguridade social e assuntos similares¹²².

A partir do meio da década de 1970, os Ministros do Conselho da Europa adotaram várias resoluções que faziam referência ao artigo 8.º da Convenção Europeia de Direitos Humanos, diante dos avanços tecnológicos e da crescente necessidade de que fossem adotadas regras mais específicas para salvaguardar os indivíduos por meio da proteção de seus dados. Em 1981, então, foi concluída a Convenção 108 – Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal¹²³ –, primeiro instrumento internacional vinculativo ao domínio da proteção de dados; trata, especialmente, da “recolha e tratamento automatizado de dados de forma leal e lícita, armazenados para finalidades determinadas e legítimas, não podendo ser utilizados para fins incompatíveis com essas finalidades nem conservados por tempo superior ao necessário”¹²⁴. Além disso, prevê “garantias relativas à recolha e tratamento de dados pessoais, a Convenção proíbe, na ausência de garantias jurídicas adequadas, o tratamento de dados sensíveis, tais como dados sobre a raça, a opinião política, a saúde, as convicções religiosas, a vida sexual ou o registo criminal de uma pessoa”¹²⁵.

Todos os Estados-Membros da União Europeia ratificaram a Convenção 108; em 1999, foi alterada para permitir a adesão da União Europeia; e, em 2001, foi adotado protocolo que estabelece, entre outras questões, a criação obrigatória das autoridades nacionais de proteção de dados. A adoção das Resoluções n.º (73) 22¹²⁶, n.º (73) 23¹²⁷ e n.º

¹²² “18. *Another particular problem arises from attempts to obtain information by modern technical devices (wire-tapping, hidden microphones, the use of computers etc.), which infringe the right to privacy. Further consideration of this problem is required.* 19. *Where regional, national or international computer-data banks are instituted the individual must not become completely exposed and transparent by the accumulation of information referring even to his private life. Data banks should be restricted to the necessary minimum of information required for the purposes of taxation, pension schemes, social security schemes and similar matters*” (COUNCIL OF EUROPE. *Parliamentary Assembly – Resolution 428. Declaration on mass communication media and Human Rights* [Em linha]. New York, 23 Jan. 1970. [Consult. 17 Jul. 2022]. Disponível em: <https://pace.coe.int/en/files/15842>).

¹²³ PORTUGAL. Ministério Público – **Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal** [Em linha]. Estrasburgo, 28 jan. 1981. [Consult. 17 jul. 2022]. Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/convencao_protecao_pessoas_tratamento_automatizado_dados_caracter_pessoal.pdf.

¹²⁴ EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS; EUROPEAN COURT OF HUMAN RIGHTS; COUNCIL OF EUROPE – **Manual da Legislação Europeia sobre Protecção de Dados** [Em linha]. Luxemburgo: Serviço das Publicações da União Europeia, 2014, p. 16. [Consult. 17 jul. 2022]. Disponível em: http://publications.europa.eu/resource/ellar/af9d0b3f-82be-11e5-b8b7-01aa75ed71a1.0017.03/DOC_2

¹²⁵ *Ibid.*, loc. cit.

¹²⁶ COUNCIL OF EUROPE – **Resolution (73) 22 of the Committee of Ministers to Members States on the protection of the privacy of individuals Vis-a-vis electronic data banks in the private sector** [Em linha]. Luxembourg, 26 Sept. 1973. [Consult. 17 jul. 2002]. Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502830>.

(74) 29¹²⁸ é considerada pela doutrina como início do movimento legislativo europeu e inspiradora de princípios albergados pelo vigente Regulamento Europeu de Proteção de Dados¹²⁹.

Não menos importante, temos as Diretrizes sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais da OCDE, adotada pelos países membros em 1980. O trabalho sobre privacidade e fluxos de dados transfronteiriços na OCDE começou no início dos anos 70. Com uma crescente divergência nas legislações nacionais que criavam riscos para o livre fluxo de informações entre os países membros, a OCDE comprometeu-se a desenvolver diretrizes em 1978. Tais diretrizes foram desenvolvidas em estreita cooperação com o Conselho da Europa, que preparava o que se tornaria a Convenção n.º 108. A privacidade diz respeito aos valores essenciais dos Estados, e os países da OCDE procuraram garantir certos padrões mínimos para a proteção da privacidade e das liberdades individuais em relação aos dados pessoais. Ao desenvolver um consenso em torno de um conjunto de princípios fundamentais para proteger os indivíduos, esperava-se diminuir a necessidade de regulamentação das exportações/transmissões de dados pessoais e minimizar os problemas relacionados ao conflito de leis.

Contudo, diante das diferenças entre os Estados, principalmente de cada lado do Atlântico, a resolução desse impasse não estaria na direção de um tratado internacional, mas na adoção de princípios gerais, os quais, se introduzidos no âmbito interno, esperava-se que contribuíssem para a redução dos obstáculos à circulação de dados, cumprindo com os objetivos institucionais da OCDE. Para os países membros não europeus, a adoção de um tratado europeu para proteger a privacidade era um encargo burocrático pesado demais, com custo elevado de implementação e que, na verdade, configuraria um mecanismo de fomento à tecnologia de informação na Europa, sob a roupagem de normas que visariam à proteção de dados.

Como bem destacado por Marcelo Varella, “as *soft norms* devem ser avaliadas não sob a ótica de seu conteúdo normativo, mas como uma etapa entre a inexistência de um quadro

¹²⁷ COUNCIL OF EUROPE – **Resolution (73) 23 of the Committee of Ministers to Members States on harmonization measures in the field of legal data processing in the Member States of the Council of Europe** [Em linha]. Luxembourg, 26 Sept. 1973. [Consult. 17 jul. 2022]. Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680502830.

¹²⁸ *Id.* – **Resolution (74) 29 of the Committee of Ministers to Members States on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector** [Em linha]. Luxembourg, 20 Sept. 1974. [Consult. 17 July 2022]. Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804d1c51.

¹²⁹ UNIÃO EUROPEIA – Regulamento (EU) 2016/679 (General Data Protection Regulation - GDPR). **Jornal Oficial da União Europeia**. L119. (04 maio 2016), p. 1-88.

normativo por falta de contexto político de positivação de normas rígidas e a existência de um direito obrigatório, cuja efetividade tem maiores chances de ocorrer pelo consenso alcançado entre as partes. De fato, é melhor ter a aprovação de uma norma *soft* sobre um tema controverso que a não aprovação de uma norma rígida sobre o mesmo tema. O ‘tudo ou nada’ no direito internacional pode significar a postergação da regulação sobre determinado tema por muitos anos ou mesmo a não regulação. O excesso de *soft norms* não parece ser de forma alguma um obstáculo à evolução jurídica, mas um método para tornar possível essa evolução”¹³⁰.

Mesmo que parte da doutrina não seja muitas vezes convergente em relação à autuação dos instrumentos de *soft law*, na prática internacional e ao menos para fins do tema aqui explorado, verifica-se a sua indelével contribuição para a mitigação de riscos e danos aos seres humanos.

1.4 A relevância proteção da privacidade e o direito à reserva sobre a intimidade da vida privada e a necessidade de tutela

A tutela da privacidade e da reserva sobre a intimidade da vida privada ao longo dos tempos e nos países de tradição democrática representou a garantia de tutela de um conjunto de valores fundamentais do indivíduo, nos quais se destacam os direitos de liberdade e privacidade, alicerçados no valor fundamental da dignidade humana.

Assim o reconhecem Guilherme Gray e Felipa Urbano Calvão. O primeiro, enfatizando que o livre desenvolvimento da personalidade e a liberdade de autodeterminação são determinantes para a permanente proteção do indivíduo contra as ameaças e desafios decorrentes da sociedade tecnológica e novas técnicas de acesso e armazenamento (entre nós, incluiríamos o processamento) de dados pessoais¹³¹. A segunda, tratando da vertente do direito à proteção de dados pessoais, assevera que o objetivo não há de ser apenas a tutela da privacidade, mas também da garantia da liberdade¹³².

Stefano Rodotà também reconhece que as novas formas ou “dimensões de coleta e tratamento de informações provocam a multiplicação de apelos à privacidade e, ao mesmo tempo, aumentam a consciência da impossibilidade de confinar as novas questões que surgem dentro do quadro institucional tradicionalmente identificado por esse conceito”. Hoje o

¹³⁰ VARELLA, Marcelo Dias – **Direito internacional público**. 7.^a ed. São Paulo: Saraiva, 2017.

¹³¹ DRAY, Guilherme – O direito à reserva da intimidade da vida privada: o artigo 80.º do Código Civil de 1966. **Revista de Direito Civil**. Ano II, n.º 3 (2017). p. 673-699, p. 699.

¹³² CALVÃO, Felipa Urbano – O direito fundamental à proteção de dados pessoais e a privacidade 40 anos depois. **Jornadas nos quarenta anos da constituição da República portuguesa: impacto e evolução**. Porto: Universidade Católica, 2017. p. 85-101, p. 89.

problema não seria em adaptar à noção de privacidade antiga e nascida em outra época, em outro lugar e circunstâncias às questões e problemas atuais respeitando as razões de sua origem, mas sim de considerar uma importante mudança qualitativa dessa noção, vislumbrando os problemas da privacidade inseridos dentro do quadro da organização do poder, no âmbito do qual a infraestrutura da informação representa, modernamente, um dos componentes fundamentais¹³³.

Para Victor Correia, a tutela da privacidade é, por exemplo, a limitação do acesso à informação. A vigilância das informações acontece por meio da utilização de bancos de dados pessoais para inquirir e vigiar as ações e comunicações das pessoas, sem que saibamos exatamente o que eles revelam sobre nós, quais dados são utilizados, para qual finalidade e de que forma. O problema não estaria relacionado com a vigilância, mas especialmente com a impotência e vulnerabilidade criada por essa utilização, que acaba por excluir o vigiado do processo criativo. Assim, “o problema da vigilância dos dados e da privacidade põe um problema relativamente ao modo como as pessoas são tratadas pelas instituições, criando um desequilíbrio entre o poder dos indivíduos e o da entidade que recolhe esses dados. Esta situação coloca sobretudo questões sobre poderes estatais, institucionais, e sociais, que jogam com os nossos dados pessoais, como por exemplo a sua reutilização para uma finalidade diferente daquela para a qual foram recolhidos, sem o consentimento das pessoas. Trata-se de um défice democrático, numa relação de forças desigual”¹³⁴.

Nesse sentido, é necessária uma conceção de democracia de privacidade, de modo que ela é importante para a democracia do mesmo modo que a democracia é importante para o direito à privacidade, posto que, se assim entendidas, “ambas constituem um compromisso perante outros direitos, como o direito à liberdade e à igualdade, e o direito à privacidade assume-se então como algo necessário para assegurar que estes direitos são de facto democráticos”¹³⁵.

De fato, o uso massificado de informações e as formas automatizadas de tratamento delas por parte de instituições públicas e privadas, tendência que é inevitável diante dos claros ganhos em eficiência e precisão¹³⁶, devem ser examinados de forma realista e combinada com

¹³³ RODOTÁ, Stefano – **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008, p. 23.

¹³⁴ CORREIA, Victor – Sobre o Direito à privacidade. **O Direito**. [Em Linha] Ano 146, n.º 1 (2014), p. 9-32, p. 25-28. [Consult. 17 jul. 2022]. Disponível em: https://www.academia.edu/6106718/Sobre_o_direito_%C3%A0_privacidade

¹³⁵ *Ibid.*

¹³⁶ FERREIRA, Diogo Figueiredo Perfeito Dias – Trabalhador, reserva da intimidade da vida privada e “redes sociais”: nótulas reflexivas sobre este delicado problema laboral. **Estudos Laborais** [Em Linha]. Ano 80,

as transformações provocadas no uso do poder por essas instituições. Somente dessa forma será possível sanar e equilibrar eventual conflito entre a tutelas dos direitos e liberdades individuais e a eficiência administrativa e empresarial.

Mais uma vez nos parece valiosa a lição de Stefano Rodotà quando afirma que “identificando as raízes do poder fundado na disponibilidade das informações e seus reais detentores, será possível não somente projetar formas de contrapoder e de controle, como também aproveitar possibilidades oferecidas pela tecnologia da computação para tentar produzir formas diversas de gestão do poder, capazes de oferecer às liberdades individuais possibilidades de expansão antes impensáveis. Enquanto se luta contra os riscos de uma ‘poluição dos direitos civis’, até mesmo a utopia está a nosso alcance. Nada impede que se trabalhe buscando definir uma estratégia cujo ponto de chegada consista na proliferação de processos decisórios racionalizados, tornados transparentes com o auxílio do computador, com um consequente controle social sobre os participantes do processo, de modo a alcançar uma participação no próprio processo”¹³⁷.

Felipe Urbano Calvão, traçando um panorama sobre os novos desafios da privacidade 40 anos após a Constituição da República portuguesa, no âmbito de uma análise ao artigo 35.º, afirma que está em causa a proteção dos cidadãos contra pretensões de vigilância dos Estados e das empresas, visto que a alteração do contexto tecnológico alterou a realidade social no que toca o tratamento massificado de dados pessoais¹³⁸.

A informatização da informação proporcionou o salto quantitativo e qualitativo. O quantitativo, baseado no enorme volume de dados e o poder de processá-los em muito menos tempo, e o qualitativo, considerando a aplicação de técnicas (como a definição de perfis¹³⁹ e

Vol. III/IV (jul./dez. 2020), p. 585-611, p. 592-593. [Consult. 17 jul. 2022] Disponível em: <https://portal.oa.pt/media/132093/diogo-figueiredo-perfeito-dias-ferreira.pdf>.

¹³⁷ RODOTÁ, Stefano – **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008, p. 24-25.

¹³⁸ CALVÃO, Felipa Urbano – O direito fundamental à proteção de dados pessoais e a privacidade 40 anos depois. **Jornadas nos quarenta anos da constituição da República portuguesa: impacto e evolução**. Porto: Universidade Católica, 2017. p. 85-101, p. 91.

¹³⁹ A definição de perfis ou *profiling*, segundo Danilo Doneda, consiste na elaboração de perfis de comportamento de um indivíduo (ou grupos de indivíduos) a partir de informações disponibilizadas por ele próprio ou colhidas de outras fontes. “Com ela os dados são tratados com auxílio de métodos estatísticos e de técnicas de inteligência artificial, com o fim de obter uma metainformação que consistiria numa síntese de hábitos, preferências pessoais e outros registros da vida desta pessoa” (DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**. 2.ª ed. São Paulo: Revista dos Tribunais, 2019, p. 151). Para Felipa Urbano Calvão, a criação de perfis standatiza as pessoas, havendo um risco de identidades inexatas, assentes em informações ou interpretações de dados falsas, ou até de usurpação de identidade (CALVÃO, Felipa Urbano, *op. cit.*, p. 95).

mineração de dados¹⁴⁰) cada vez mais sofisticadas de processamento a fim de obter resultados cada vez mais relevantes.

A possibilidade de tratamento de grandes quantidades de informações decorre também do aumento da capacidade de seu armazenamento em diversos tipos de memória, “desde os idos tempos dos cartões perfurados até os atuais métodos massificados de coleta, armazenamento e processamento [...], apontando para um futuro marcado pela nanotecnologia e capacidade sempre crescente de armazenamento”¹⁴¹.

Deste modo, aumenta-se exponencialmente a quantidade de informação disponível sobre a pessoa em circulação em várias bases de dados (autorizadas ou não), o que pode vir a influenciar diretamente na sua vida presente e futura, limitando sua liberdade (de escolha, de ir e vir, de manifestação livre de opinião, etc.) e causando reflexos em sua segurança, por exemplo. Mais relevante é notar que o elemento essencial a várias das modalidades diferentes de técnicas de tratamento de dados é a de que informações pessoais fornecidas pelos indivíduos podem se distanciar bastante das finalidades para as quais elas foram originalmente fornecidas¹⁴².

Os dados pessoais se tornaram verdadeiros intermediários entre o indivíduo e a sociedade, agindo como prepostos “nem sempre autorizados e capazes – e é justamente isto que pode gerar como efeito a perda de controle da pessoa sobre o que se sabe em relação a si mesma o que, em última análise, representa uma diminuição na sua própria liberdade”¹⁴³.

Mudaram-se os hábitos de vida, as necessidades e os interesses públicos e privados. Em prol da eficiência de gestão das empresas e órgãos públicos que justificam a utilização das tecnologias com os riscos a elas inerentes, da centralização das informações como condição de gestão eficiente, o que também importa em riscos pela concentração de dados num mesmo sistema¹⁴⁴.

¹⁴⁰ O mesmo Doneda esclarece que mineração e dados ou data mining consiste “na busca de correlações, recorrências, formas, tendências e padrões significativos a partir de quantidades muito grandes de dados, com o auxílio de instrumentos estatísticos e matemáticos. Assim, a partir de uma grande quantidade de informação em estado bruto e não classificada, torna-se possível identificar informações de potencial interesse” (DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**. 2.^a ed. São Paulo: Revista dos Tribunais, 2019, p. 154).

¹⁴¹ *Ibid.*, loc. cit.

¹⁴² *Ibid.*, p. 157.

¹⁴³ *Ibid.*, p. 158.

¹⁴⁴ “Invoca-se a necessidade de segurança, em resposta às ameaças do terrorismo e da criminalidade organizada sobretudo numa lógica preventiva que implica a vigilância generalizada dos cidadãos, com tecnologia (vg. Reconhecimento facial) que permite detetar ou seguir qualquer um a multidão, a análise preditiva de comportamentos assente essencialmente em data mining e criação de perfis. [...] Afirma-se ainda a necessidade de uma sempre crescente transparência na administração da coisa pública, que reclama ou justifica crescente transparência da informação detida pelos organismos públicos, como meio de prevenir abusos de poder [...]” (CALVÃO, Felipa Urbano – O direito fundamental à proteção de dados pessoais e a

O tema central do nosso trabalho é para nós o que de mais extraordinário surgiu com a desenfreada evolução tecnológica: a Inteligência Artificial (IA). É certo que a IA evoluiu e se beneficiou, através dos tempos, de novas descobertas em diferentes áreas do conhecimento, como tecnologias da informação de comunicação e com a grande produção e disponibilidade de dados, pelo que as grandes questões atuais remetem a desafios relativamente à imitação de alta complexidade do cérebro humano.

O primeiro desafio consistiria em como fazer com que um sistema de IA se mantenha aprendendo e como poucos exemplos como o cérebro humano. O segundo desafio seria atender à proposta de que a área de IA vá além das soluções de problemas, mas “que ela também seja capaz de trazer dados que possam elucidar como suas soluções são auferidas. Essa área é conhecida como Explainable Artificial Intelligence (XAI)”¹⁴⁵. O professor ainda ressalta que a necessidade de uma IA explicável tem sido posta em diversos usos e aplicações da IA, que vão desde diagnósticos de saúde, carros autônomos e veículos aéreos não tripulados (os conhecidos drones), que têm sido automatizados por modelos de IA, e afirma que um passo importante teria sido dado em 2016 com o advento do RGPD, que teria “postulado direitos explícitos aos cidadãos europeus em solicitar o detalhamento de decisões auferidas por máquinas sobre seus dados”¹⁴⁶, citando o considerando 71.^{o147} do Regulamento

privacidade 40 anos depois. **Jornadas nos quarenta anos da constituição da República portuguesa: impacto e evolução.** Porto: Universidade Católica, 2017. p. 85-101, p. 93-94).

¹⁴⁵ SILVA, Nilton Correa – Inteligência Artificial. In MULHOLLAND, Caitlin; FRAZÃO, Ana (coord.) – **Inteligência Artificial e Direito: ética, regulação e responsabilidade.** São Paulo: Thompson Reuters Brasil, 2019. p. 35-52, p. 36-37.

¹⁴⁶ *Ibid.*, p. 37.

¹⁴⁷ “(71) O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito por via eletrónico ou práticas de recrutamento eletrónico sem qualquer intervenção humana.

Esse tratamento inclui a definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar.

No entanto, a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se expressamente autorizada pelo direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento, incluindo para efeitos de controlo e prevenção de fraudes e da evasão fiscal, conduzida nos termos dos regulamentos, normas e recomendações das instituições da União ou das entidades nacionais de controlo, e para garantir a segurança e a fiabilidade do serviço prestado pelo responsável pelo tratamento, ou se for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento, ou mediante o consentimento explícito do titular.

Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, **de obter uma explicação sobre a decisão tomada** na sequência dessa avaliação e **de contestar a decisão.**

Essa medida não deverá dizer respeito a uma criança.

na parte em que enuncia que, “em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão”¹⁴⁸.

Já há algum tempo organizações dos mais diferentes setores vêm investindo pesadamente em IA no intuito de se tornarem cada vez mais competitivas, e os usos principais da IA hoje se relacionam à organização de dados, do auxílio à tomada de decisão e da automação da decisão¹⁴⁹. Em relação às conquistas em automação de decisões, que estão cada vez mais apropriadas e confiáveis, podemos citar as decisões relacionadas a vendas, pois permite que grandes empresas utilizem suas bases de dados para, com ajuda da IA, cruzá-las com dados disponíveis na internet para criar listas de prospecção. Agentes virtuais poderão lidar com queixas de consumidores e tomar decisões para dar solução aos problemas trazidos por eles; professores robôs poderão atuar como moderadores de grupos de estudos.

A IA já faz parte de nossa vida quando interagimos com a Siri (assistente inteligente da Apple), Alexa (a assistente da Amazon), por exemplo, que no âmbito da tecnologia é conhecida como a Internet das Coisas (*Internet of things*). Os assistentes possuem vozes femininas e simpáticas, nos dão respostas rápidas, selecionam ou buscam nossa música preferida, executam pequenas tarefas se conectadas em aparelhos de automação doméstica e podem fazer muito mais do imaginamos, até mesmo o que não desejamos.

Trata-se exatamente o que aconteceu nos idos de 2015, quando uma notícia publicada no sítio eletrônico do “*The Daily Beast*” com a manchete “*Your Samsung SmartTV Is Spying on You, Basically: watch your mouth*”¹⁵⁰, mostrou não só as capacidades de uma simples

A fim de assegurar um tratamento equitativo e transparente no que diz respeito ao titular dos dados, tendo em conta a especificidade das circunstâncias e do contexto em que os dados pessoais são tratados, o responsável pelo tratamento deverá utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos.

A decisão e definição de perfis automatizada baseada em categorias especiais de dados pessoais só deverá ser permitida em condições específicas” (grifos nossos).

¹⁴⁸ UNIÃO EUROPEIA – Regulamento (EU) 2016/679 (General Data Protection Regulation - GDPR). **Jornal Oficial da União Europeia**. L119. (04 maio 2016), p. 1-88.

¹⁴⁹ STEIBEL, Fabro; VICENTE, Victor Freitas; JESUS, Diego Santos Vieira de – Possibilidade e potenciais da utilização da Inteligência Artificial. In MULHOLLAND, Caitlin; FRAZÃO, Ana (coord.) – **Inteligência Artificial e Direito: ética, regulação e responsabilidade**. São Paulo: Thompson Reuters Brasil, 2019. p. 35-52, p. 58.

¹⁵⁰ SHANE, Harris – **Your Samsung SmartTV Is Spying on You, Basically** [Em linha]. New York, 14 Apr. 2017. [Consult. 07 maio 2022]. Disponível em: <https://www.thedailybeast.com/your-samsung-smarttv-is-spying-on-you-basically>.

Smart TV, mas os perigos e desafios à privacidade, que estavam, literalmente, vivendo conosco. Determinadas Smart TVs estavam ouvindo e gravando as conversas no ambiente em que estavam instaladas, por meio de um microfone embutido nos controles remotos, e compartilhando essas informações com parceiros comerciais para definições de perfis de consumo. A captação das conversas era uma opção que já vinha habilitada de fábrica; se o consumidor desejasse, deveria desabilitá-la. O problema reside no fato de que essa informação não era suficientemente clara e/ou o consumidor desconhecia por completo as potencialidades dessa colheita de informações, ou mesmo a respeito da colheita das informações, de modo que a referida “opção” raramente era desabilitada. Não pretendemos aqui nos debruçar sobre as minúcias do caso, mas demonstrar que os riscos à tutela da privacidade são reais e muito próximos de nós. Não pretendemos frear o desenvolvimento, mas nos socorrer às bases de tutela dos Direitos e garantias que possuímos para nos proteger de abusos e das falhas que podem advir do desenvolvimento sem controle.

Caitlin Sampaio Mulholland, oportunamente, analisou o mesmo episódio e colocou a questão da necessária regulação e proteção do indivíduo de forma consistente e eficiente, com foco na dignidade humana, apontando o Regulamento Europeu como o então novo e adequado instrumento ao cumprimento desse objetivo: “questiona-se se é necessária – e, em sendo –, qual o tipo de regulação que deveria ser adotada no Brasil para delimitar o âmbito de proteção do direito de privacidade e dos dados dos consumidores destes bens conectados. Aos poucos, vão surgindo iniciativas regulatórias que indicam a necessidade de tutelar de maneira mais consistente e eficiente os dados pessoais, como desenvolvimento da cláusula geral de proteção da pessoa humana. Neste sentido, a União Europeia conta com um novo regulamento de proteção de dados, após mais de duas décadas de vigência da Diretiva 95/46, que é o Regulamento Geral de Proteção de Dados – conhecida também como GDPR (General Data Protection Regulation) – que tem a missão de proteger de forma ampliada e geral os dados pessoais, focada em iniciativas de boas práticas empresariais e compliance, que serão, por sua vez, fiscalizadas por meio de autoridades centrais de garantia e proteção de dados”¹⁵¹.

Também nos parece caber aqui a citação do caso, em especial, que levou Cathy O’Neil, a escrever *Algoritmos de Destruição em Massa: como o big data aumenta a desigualdade e ameaça à democracia*. Na verdade, na introdução deste texto, a autora expõe o caso que a levou a escrever. Conta que desde muito pequena sempre foi atraída e fascinada

¹⁵¹ MULHOLLAND, Caitlin Sampaio – **Mercado, Pessoa Humana e Tecnologias: a Internet das Coisas e a proteção do direito à privacidade** [Em linha]. Rio de Janeiro: PUC-RJ, ago. 2021. [Consult. 07 maio 2022]. Disponível em: <https://www.jur.puc-rio.br/wp-content/uploads/2021/08/CAITLIN-SAMPAIO-Mercado-Pessoa-Humana-e-Tecnologias.pdf>.

por números e que isso a fez uma “nerd da matemática”. A matemática se expandia e se desenvolvia no mundo, o que a levou a se formar em matemática e a abandonar seu cargo como professora no departamento de matemática de Columbia University para trabalhar como analista para o D. E. Shaw¹⁵², um fundo multimercado de ponta. Narra que a empolgação inicial ruiu com a percepção de que “a matemática não só estava emaranhada nos problemas mundiais, como era também o combustível de muitos deles”¹⁵³ e que “a matemática podia combinar-se com a tecnologia para multiplicar o caos e a desgraça, dando eficiência e escala a sistemas que agora entendo defeituosos”^{154,155}.

O’Neil cita o exemplo do caso de 2007, quando o novo prefeito de Washington, D.C., estava determinado a reverter o quadro de baixo rendimento dos alunos nas escolas municipais e contratou uma nova reitora para as escolas, que, por sua vez, implementou um plano para erradicar professores de baixo rendimento, uma vez que, em teoria, os estudantes não estariam apreendendo o suficiente porque os professores não faziam bem o seu trabalho. Essa tendência teria se espalhado pelo país e, segundo a autora, para um engenheiro de sistemas a avaliação de professores fazia todo sentido. “Livrar-se dos piores e posicionar os

¹⁵² “We are the D. E. Shaw group, a global investment and technology development firm. Academic culture. Real-world challenges. The excitement of a startup with the resources of an industry leader. Whatever brings you here, this is a place where extraordinary and diverse minds come together. To discover. To create. To build” (DESHAW&CO [Em linha] New York, NY, 2022. [Consult. 7 jun. 2022]. Disponível em: <https://www.deshaw.com/>)

¹⁵³ O’NEIL, Cathy – **Algoritmos de Destruição em Massa: como o big data aumenta a desigualdade e ameaça à democracia**. São Paulo: Rua do Sabão, 2020, p. 6.

¹⁵⁴ *Ibid.*, p. 7.

¹⁵⁵ E a autora continua: “Se tivéssemos sido lúcidos, teríamos todos dado um passo atrás para conseguir entender como a matemática fora mal utilizada e como poderíamos prevenir uma catástrofe similar no futuro. Ao invés disso, na esteira da crise, novas técnicas matemáticas estavam bombando, expandindo-se para novos territórios. Petabytes de dados eram processados 24 horas por dia, 7 dias por semana, muitos deles raspados de redes sociais ou sites de e-commerce. **E cada vez mais o foco não era nos movimentos dos mercados financeiros globais, mas nos seres humanos. Em nós. Matemáticos e estatísticos estavam estudando os nossos desejos, movimentações e poder de compra.** Eles previam nossa credibilidade e calculavam nosso potencial enquanto estudantes, trabalhadores, amantes e criminosos. Esta era a economia do Big Data, os **imensos volumes de dados**, e ela prometia ganhos espetaculares. Um programa de computador poderia vasculhar milhares de currículos ou pedidos de empréstimo em um segundo ou dois e ordená-los em listas impecáveis, com os candidatos mais promissores no topo. Isso não apenas economizava tempo, mas também era vendido como algo imparcial e objetivo. Afinal, não envolvia humanos preconceituosos cavoucando resmas de papel, apenas máquinas processando números frios. Contudo, eu via problemas. As aplicações matemáticas fomentando a economia dos dados eram baseadas em escolhas feitas por seres humanos falíveis. Algumas dessas escolhas sem dúvida eram feitas com as melhores das intenções. Mesmo assim, muitos desses modelos programavam preconceitos, equívocos e vieses humanos nos sistemas de software que cada vez mais geriam nossas vidas. Como deuses, esses modelos matemáticos eram opacos, seus mecanismos invisíveis a todos exceto os altos sacerdotes de seus domínios: os matemáticos e cientistas da computação. Suas decisões, mesmo quando erradas ou danosas, estavam para além de qualquer contestação. E elas tendiam a punir os pobres e oprimidos da sociedade enquanto enriquecia ainda mais os ricos. Criei um nome para esses modelos nocivo: Armas de Destruição Matemáticas, ou ADMs” (*ibid.*, p. 8).

melhores onde podem fazer um bem maior”¹⁵⁶. A ferramenta IMPACT foi usada no final de alguns anos letivos e foi responsável pela demissão de centenas de professores que teriam baixo rendimento, até que uma professora que era muito bem avaliada por diretores e pais de alunos recebeu uma avaliação lastimável no IMPACT. Perguntava-se como poderia alguém tão bem avaliado receber uma avaliação ruim de uma máquina tão eficiente? O problema era o novo sistema de pontuação conhecido como “modelagem de valor agregado, que pretendia medir a eficácia da professora ao ensinar matemática e habilidades linguísticas. Aquela pontuação, gerada por um algoritmo, representava metade da avaliação final, e prevaleceu sobre os comentários positivos dos gestores e da comunidade escolar. O distrito não tinha outra opção a não ser demiti-la [...]. Isso não parecia ser algum tipo de caça às bruxas ou ajuste de contas. De fato, há lógica na abordagem do distrito escolar. Gestores, afinal, podem muito bem ser amigos de professores terríveis. Maus professores podem parecer bons”. A professora em questão quis saber de onde vinham os números tão injustos, mas ninguém os compreendia. O distrito havia contratado a consultoria Mathematica Policy Research.

Inúmeros fatores podem influir no aprendizado, desde histórico socioeconômico, transtornos de aprendizado, fatores regionais e locais (pobreza, drogas), o que poderia afetar os resultados dos alunos e não ser atribuível ao educador, e os algoritmos tinham que dar conta desses fatores. Uma característica desses sistemas de algoritmos é que eles tendem a punir os pobres, a agravar desigualdades, já que são projetadas para avaliar grandes números de pessoas, especializando-se em volumes massivos e são baratas, sendo esse mais um atrativo. “Um escritório de advocacia de gabarito ou escolas particulares tenderão muito mais a recomendações e entrevistas cara a cara do que uma rede de fast-food ou distrito escolar com grana curta”¹⁵⁷.

Em dado momento a autora chega no ponto que nos causa inquietação e nos leva à investigação. Afirma que a professora demitida teve muita dificuldade em encontrar quem fosse capaz de explicar sua pontuação baixa, o que ela classifica como sendo “revelador” e afirma que “as sentenças das ADMS (Armas de Destruição Matemáticas) caem como mandamentos dos deuses algorítmicos”, posto que o modelo em si é uma “caixa-preta, cujo conteúdo é segredo corporativo ferozmente protegido”¹⁵⁸. Por anos os professores demitidos teriam cobrado detalhes sobre a composição das pontuações arbitrárias, mas lhe diziam que

¹⁵⁶ O’NEIL, Cathy – **Algoritmos de Destruição em Massa: como o big data aumenta a desigualdade e ameaça à democracia**. São Paulo: Rua do Sabão, 2020, p. 9.

¹⁵⁷ *Ibid.*, p. 15.

¹⁵⁸ *Ibid.*, *loc. cit.*

eram algoritmos muito complexos, o que desencorajava a maioria. Notem que estamos falando de professores, pessoas esclarecidas com nível superior.

A dificuldade em se descortinar e explicar os detalhes que levaram aos resultados apontados pelo sistema serve não só ao objetivo de que as consultorias cobrem menos pelos seus serviços (pois investem menos em algoritmos explicáveis), mas também serve ao objetivo de manter as pessoas avaliadas “no escuro”, que, diante disso, terão menos chances de “burlar o sistema” e terão que, simplesmente, “trabalhar mais duro, seguir regras e rezar para que o modelo registre e aprecie seus esforços. Mas se detalhes estão escondidos, também é mais difícil questionar ou contestar os resultados”¹⁵⁹.

Nesse sentido, a IA usará dados e lesará direitos de liberdade ao mudar hábitos pessoais e comportamentos, tornando o indivíduo refém de um sistema que lhe é imposto, aumentando a desigualdade, impondo a vontade da máquina sobre o homem, do poder econômico sobre a dignidade humana¹⁶⁰.

A falta de clareza e opacidade¹⁶¹ no funcionamento dos mecanismos já conhecidos da IA geram insegurança e caminham em sentido contrário à transparência almejada pelo legislador do RGPD. Além disso, as interpretações segundo as quais não há um direito à explicação (informação) nas decisões individuais automatizadas, as quais o titular não poderá se recusar a se submeter, nos parecem contrárias à tutela da privacidade que se impõe no domínio da proteção de dados pessoais num Estado de Direito Democrático.

Os riscos envolvidos quando se trata da aplicação de decisões automatizadas na Administração Pública e da falta de transparência das “black boxes” foram tratados por Artur Flamínio da Silva. Em função do princípio da transparência que é pressuposto essencial da atividade administrativa, a complexidade dos sistemas de IA, os quais, mesmo com a intervenção humana se tornam ininteligíveis, devem ser reconduzidos a verdadeiras “white boxes” (“casa de vidro tecnológica”), com acesso e conhecimento generalizado pelos

¹⁵⁹ O’NEIL, Cathy – **Algoritmos de Destruição em Massa: como o big data aumenta a desigualdade e ameaça à democracia**. São Paulo: Rua do Sabão, 2020, p. 16.

¹⁶⁰ Sobre os riscos, perigos e desvantagens da Informatização da Administração Pública (“Administração Pública Eletrônica”), bem como os limites que devem ser impostos à essa informatização, cf.: OTERO, Paulo – **Manual de Direito Administrativo**. Coimbra: Almedina, 2016. Vol. I, p. 488-496.

¹⁶¹ Sobre o fenômeno do “black box”, vide PASQUALE, Frank. **The Black Box society: the secret algorithms that control money and information**. Cambridge: Harvard University Press, 2015. Tratando também da opacidade dos sistemas de *Machine Learning*, vide DONEDA, Danilo; ALMEIDA, Virgílio Augusto Fernandes – O que é a governança de algoritmos? **Tecnopolíticas da Vigilância: perspectivas da margem**. São Paulo: Boitempo, 2018, p. 142-143.

cidadãos, estando e causa, ainda, questões relacionadas, eventualmente, à fundamentação das decisões automatizadas¹⁶².

De facto, não partilhamos nenhuma descrença relativamente à tecnologia e reconhecemos que o conhecimento e desenvolvimento da IA é estratégico. Bem desenvolvida e utilizada, pode diminuir a sobrecarga de trabalho humano, executar tarefas com imensa precisão e em velocidade infinitamente maior, além de poder contribuir com a diminuição das desigualdades sociais. No entanto, não podemos colher frutos positivos se o desenvolvimento técnico da IA não for acompanhando da análise de sua robustez, solidez, confiabilidade, levando em conta as dimensões éticas de desenvolvimento e seu impacto no mundo do Direito.

Sem referenciais éticos e jurídicos claros e aceites, estaremos diante do risco de que o desenvolvimento acelerado e descuidado das aplicações da IA acabem por fornecer elementos para justificação de diversos mitos – ou verdades parciais –, associados à sua aplicação, tais como a falta de transparência e obscuridade, insensibilidade, preconceito e aumento das desigualdades. Por isso, preferimos nos unir aos que discutem e pesquisam meios de tornar as aplicações de AI estruturadas em diretrizes éticas em parâmetros e propósitos de confiabilidade e transparência, robustez e respeito ao indivíduo¹⁶³.

1.5 O direito à autodeterminação informacional e à proteção de dados pessoais

No contexto do anteriormente referenciado, importa ter em conta que o artigo 35.º da Constituição portuguesa consagra o direito à autodeterminação informativa, que tem por finalidade a salvaguarda da vida privada dos indivíduos, proibindo as intromissões abusivas por meio da recolha e tratamento de dados pessoais informatizados, muito embora, como bem pondera Jorge Miranda, vá além da tutela da esfera íntima da vida de cada um¹⁶⁴.

Os direitos fundamentais se relacionam com o tratamento informático de dados, em sede de direitos, liberdades e garantias, como é o caso do direito à dignidade humana, do desenvolvimento da personalidade, da integridade pessoal e da autodeterminação informativa¹⁶⁵.

¹⁶² SILVA, Artur Flamínio da – Inteligência Artificial e Direito Administrativo. **Direito Administrativo e Tecnologia**. Coimbra: Almedina, 2021, p. 14-15.

¹⁶³ PEIXOTO, Fabiano Hartmann – **Inteligência Artificial e Direito: convergência ética e estratégica**. Curitiba: Alteridade, 2020, p. 10.

¹⁶⁴ MIRANDA, Jorge; MEDEIROS, Rui – **Constituição Portuguesa Anotada**. Lisboa: Universidade Católica, 2017. Vol. 1, p. 785.

¹⁶⁵ CANOTILHO, José Joaquim Gomes; MOREIRA, Vital – **Constituição da República Portuguesa Anotada**. 4.ª ed., rev. Coimbra: Coimbra, 2014. Vol. 1, p. 551.

Helena Moniz considera que, subjacente a todo o regime de direitos fundamentais, está a consagração de um direito à autodeterminação informacional, que funciona como instrumento de proteção de direitos fundamentais e que “se traduz, fundamentalmente, na faculdade de o particular determinar e controlar a utilização de seus dados pessoais”¹⁶⁶.

O direito à autodeterminação informativa constitui uma das expressões mais renomadas das discussões a respeito da proteção de dados pessoais. Suas primeiras expressões surgiram na Alemanha a partir da evolução das interpretações quanto ao direito geral da personalidade alemão e inspirou ou é fundamento de quase a totalidade das legislações que tutelam o direito à proteção de dados pessoais, como acontece na experiência europeia e brasileira.

Laura Schertel Ferreira Mendes trata do tema da autodeterminação informativa traçando a sua evolução no direito alemão no intuito de delimitar seu núcleo fundamental. De acordo com o Tribunal Constitucional alemão, a autodeterminação informativa se baseia principalmente em três propriedades: a primeira, no poder de decisão do indivíduo a respeito da colheita e utilização de seus dados pessoais; a segunda, decorrente da primeira, no sentido de que o direito à autodeterminação informativa não tem teor fixo ou definido, o que o “desviaria do modelo de esfera privada de atribuição de dados de uma esfera íntima”¹⁶⁷; e a terceira, que a referência pessoal do dado atua decisivamente sobre o teor da proteção, uma vez que cada registro pessoal é merecedor de tutela. Por conseguinte, “a decisão referente ao recenseamento contribuiu não apenas para fundamentar o direito à autodeterminação informativa, mas também para consolidar o direito geral da personalidade como conceito efetivo, flexível e de grande aplicação prática”¹⁶⁸.

O direito fundamental da proteção de dados se desenvolveu a partir de seu distanciamento de um âmbito fixo de proteção (esfera íntima ou privada) e teve sua base transferida a um poder de decisão e a instrumentos procedimentais, apresentando-se como a superação da esfera privada, marcado por um processo de abstração do seu âmbito de proteção¹⁶⁹. Da dimensão objetiva desse direito decorre “não apenas um dever de proteção

¹⁶⁶ MONIZ, Helena – Notas sobre a proteção de dados pessoais perante a informática. **Revista Portuguesa de Ciência Criminal**. Ano 7, Fasc. 2.º (abr./jun. 1997), p. 231-261, p. 246.

¹⁶⁷ MENDES, Laura Schertel Ferreira Mendes – Autodeterminação informativa: a história de um conceito. **Pensar – Revista de ciências jurídicas [Em linha]**. Vol. 25, n.º 4 (out./dez. 2020), p. 1-18, p. 12. [Consult. 22 abr. 2022]. Disponível em: <https://periodicos.unifor.br/rpen/article/view/10828>.

¹⁶⁸ *Ibid.*, loc. cit.

¹⁶⁹ *Ibid.*, p. 13.

contra o conhecimento não autorizado por terceiros, mas também um dever de proteção contra o consentimento meramente aparente (ou fictício) quanto ao tratamento de dados”¹⁷⁰.

Apesar de a decisão relativa ao caso do recenseamento apresentar uma concepção procedimental do direito à autodeterminação informativa, o Tribunal Constitucional alemão apresentou os riscos concretos à liberdade dos indivíduos e os limites substanciais do processamento de informações, revelando a tensão entre a noção de poder de decisão e o controle de dados e os riscos da informação: “trata-se da tensão entre o conceito puramente formal de privacidade, em que apenas a decisão e a vontade do interessado têm um papel a desempenhar, e outro conceito mais objetivo, no qual a situação objetiva de risco individual também ganha importância”¹⁷¹.

Menezes Cordeiro também faz referência ao acórdão da lei dos censos na Alemanha, assinalando que o Tribunal Constitucional alemão se beneficiou da intensa discussão jurídica anterior à própria decisão, quando a recondução do direito individual à proteção de dados ao universo da autodeterminação informativa já contava com consenso considerável, bem assim como o reconhecimento da insuficiência dos modelos clássicos da tutela da intimidade sobre a vida privada para regular o tema também serviu para que se buscasse “um novo ponto de partida”¹⁷². As linhas gerais do novo direito assentado pela Tribunal Constitucional foi o sentido de que trata-se de um direito que cabe ao próprio titular determinar em que termos e que dados seus serão divulgados e tratados; as restrições a este direito apenas poderiam ocorrer fundadas no interesse público e quando encontrassem fundamento constitucional suficiente, posto que o princípio constitucional da proporcionalidade deve ser respeitado e, por fim, que a utilização de dados pessoais deve ser limitada em lei. Além disso, o desenvolvimento posterior do direito à autodeterminação informativa viria a demonstrar sua amplitude e transversalidade¹⁷³.

À luz da aplicação do RGPD, a sustentação de um direito à autodeterminação informacional de forma apartada dos direitos da personalidade seria pouco convincente, posto que o tratamento de dados em atividades exclusivamente domésticas ou pessoais é perfeitamente válido e lícito, contrastando com o direito à imagem, por exemplo; e, ao

¹⁷⁰ *Ibid.*, p. 15.

¹⁷¹ MENDES, Laura Schertel Ferreira Mendes – Autodeterminação informativa: a história de um conceito. **Pensar – Revista de ciências jurídicas [Em linha]**. Vol. 25, n.º 4 (out./dez. 2020), p. 1-18, p. 12. [Consult. 22 abr. 2022]. Disponível em: <https://periodicos.unifor.br/rpen/article/view/10828>, p. 16-17.

¹⁷² CORDEIRO, António Barreto Menezes – **Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020, p. 257-258.

¹⁷³ *Ibid.*, p. 259.

contrário do que acontece com os direitos da personalidade, o consentimento do titular corresponde a apenas uma das bases legais de licitude do tratamento¹⁷⁴.

Procurando definir a natureza jurídica do direito à autodeterminação informativa também, Menezes Cordeiro esclarece que a posição jurídica do titular de dados compreende todos os direitos que o RGPD lhe reconhece, os quais se encontram amparados no texto constitucional. Assim, aponta como diretrizes gerais: (i) tratar-se de posição jurídica complexa, uma vez que possui situações jurídicas ativas e passivas; (ii) parte da proteção vem da imposição de obrigações aos responsáveis pelo tratamento; (iii) não se trata de um direito absoluto; (iv) e deverá ser sempre avaliado considerando as suas vantagens sociais, numa concepção amplíssima e da livre fruição da informação (função social)¹⁷⁵.

O direito de proteção de dados pessoais é um dos mais relevantes reflexos da “Era Digital” no direito privado, emergindo do claro impacto social do tratamento dos grandes volumes de dados (Big Data), repercutindo desde os contratos laborais, contratos de *e-commerce* até suas repercussões nos direitos da personalidade. Não é por acaso que Yan Carrière e Vikram Haksar, técnicos do Fundo Monetário Internacional, questionam se “os dados são o novo petróleo?”, no documento intitulado “*The Economics and Implications of Data – An Integrated Perspective*”^{176,177}.

De facto, o direito à proteção de dados assumiu e vem assumindo uma importância incontestável; o crescimento exponencial do tratamento automatizado de dados colocou a todos em uma posição de extrema vulnerabilidade, uma vez que nossas informações estão armazenadas por diferentes responsáveis pelo tratamento de dados, no âmbito público e privado, em níveis superiores do que aqueles que detemos nós mesmos sobre nossas vidas. Em que pese a realidade descrita e a preocupação em torno do tratamento automatizado não seja recente e tenha evoluído através dos tempos, principalmente na Europa, fato é que o

¹⁷⁴ *Ibid.*, p. 260-261.

¹⁷⁵ CORDEIRO, António Barreto Menezes – **Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020, p. 260-261.

¹⁷⁶ Livre tradução: “A economia e implicações dos dados – uma perspectiva integrada” (CARRIERE-SWALLOW, Yan; HAKSAR, Vikram – **The Economics and Implications of Data: An Integrated Perspective** [Em linha]. Washington, D.C.: IMF, 23 Sept. 2019. (Departmental Paper, No. 13) ISBN 978-1513511436. [Consult. 21 abr. 2022]. Disponível em: <https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596>).

¹⁷⁷ HIRSH, Dennis D. – The Glass House Effect: Big Data, The New Oil, and The Power of Analogy. **Maine Law Review** [Em linha]. (12 fev. 2014), p. 1-28 [Em linha]. [Consult. 13 set. 2022]. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393792.

RGPD colocou a proteção de dados pessoais no centro das preocupações jurídicas, tanto no setor privado quanto público¹⁷⁸.

Como efeito, o RGPD foi responsável pela densificação dos direitos e deveres dos responsáveis pelo tratamento e seus suboperadores, bem como o reforço das autoridades de controle, além da expansão e modernização das legislações correlatas e âmbito internacional (*i.e.*, no Brasil). Os seus dois propósitos essenciais foram: a defesa dos direitos e liberdades fundamentais das pessoas singulares, notadamente por meio da proteção aos seus dados, bem como a promoção da livre circulação dos dados pessoais, respeitados os limites ali bem definidos. Não se pode negar, nesse sentido, que o surgimento do regramento relacionado aos dados pessoais não se justificou apenas para acautelar interesses individuais dos titulares de dados, considerando que estes já poderiam ser tutelados por meio das normas gerais relativas aos direitos da personalidade, mas, principalmente, para regular seu tratamento¹⁷⁹, objetivos estes que estão positivados no artigo 1.º do RGPD. Esse, aliás, também foi o propósito das diretrizes traçadas pela OCDE¹⁸⁰ para proteção da privacidade e a transmissão de dados pessoais¹⁸¹.

Para Danilo Doneda o estabelecimento de regime de proteção de dados pessoais, com todas as suas implicações, atinge interesses bastante distintos, ideologias opostas, e que, por essa razão, requer certo grau de elaboração conceitual a fim de abranger de forma adequada as

¹⁷⁸ CORDEIRO, António Barreto Menezes, *op. cit.*, p. 29.

¹⁷⁹ CORDEIRO, António Barreto Menezes – **Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020, p. 33.

¹⁸⁰ OECD. Organisation for Economic Co-operation and Development – **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data** [Em linha]. Paris: OECD, 2013. [Consult. 22 abr. 2020]. Disponível em: <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>.

¹⁸¹ Nossas pesquisas nos levaram ao discurso do Sr. Michael Kirby, em março de 2010, que foi Presidente do grupo de peritos da OCDE que desenvolveram as diretrizes sobre privacidade entre 1978 e 1980. Em seu discurso Michael Kirby declara que o que motivou o interesse da OCDE e a criação do grupo e peritos está no título do grupo: “barreiras transfronteiriças de dados e à proteção da privacidade”. Ou seja, foram as “barreiras” à circulação de informação que motivo os trabalhos do grupo. A OCDE era uma organização preocupada com a eficiência econômica e com o compartilhamento geralmente livre de informações essenciais para o bom funcionamento da governança democrática e das economias de mercado. Foi o potencial das restrições sobre a transmissão de dados transfronteiriços, de regulamentos e até mesmo tratados dentro da comunidade global de livres mercados a impor “barreiras” sobre o livre fluxo de dados que atraiu o interesse da OCDE. Melhor dizendo, a preocupação da OCDE era de que a resposta das nações europeias (e das instituições regionais europeias) aos desafios da transmissão de dados transfronteiriços e as políticas de privacidade pudessem potencialmente erguer barreiras jurídicas e econômicas, pelo que era essencial fornecer exceções efetivas (KIRBY, Michael – **30 Years After: the Impact of the OECD Privacy Guidelines** [Em linha]. Paris: OECD, 10 Mar. 2010. [Consult. 01 ago. 2022]. Disponível em: <http://www.oecd.org/internet/ieconomy/30yearsaftertheimpactoftheoecdprivacyguidelines.htm>).

questões que pretende englobar. Não se trata da luta da proteção de dados contra o livre acesso e circulação de informação, ou vice-versa¹⁸².

A disciplina de proteção de dados é cercada de aparentes paradoxos: ora se protege e se tutela a confidencialidade de dados, ora se busca promover a transparência; ora se visa evitar a colheita e armazenamento, ora se defende as benesses do tratamento automatizado de grandes volumes de dados. Existe toda sorte de argumentos econômicos, técnicos e pragmáticos que procuram apontar as supostas incoerências do sistema de proteção de dados. Mas essas tensões não enfraquecem a disciplina. Longe disso. Na verdade, reforçam a necessidade de um equilíbrio a ser realizado entre o Direito e a tecnologia.

Alicerça-nos, mais uma vez, Danilo Doneda, para quem “na verdade, no mais das vezes, são determinadas consequências das tecnologias que devem ser submetidas a ajustes, eventualmente até com o auxílio da própria tecnologia. Os meios de atuação são vários e devem ser considerados com ousadia para que sejam eficazes e capazes de promover a personalidade perante as posições tanto da tecnologia como do mercado”¹⁸³.

Existem ainda dois pontos em relação à disciplina dos sistemas de proteção de dados pessoais, que é preciso destacar. O primeiro, o de que o objetivo da disciplina é a proteção do indivíduo, o ser humano, e nisso se encontra a sua unidade. O segundo, que a proteção de dados deve se valer da utilização integrada de diversos instrumentos de tutela, e que a maleabilidade e a facilidade de adaptação a novos cenários e à inovação em razão do desenvolvimento das novas tecnologias é uma característica dos instrumentos normativos de índole “soft”, como são as normas deontológicas, códigos de autorregulação, diretrizes principiológicas, etc.¹⁸⁴

Nesse contexto, em seguida, passamos a analisar o regime de proteção de dados trazido pelo RGPD, as decisões automatizadas e a definição de perfis e sua conformidade, não só com o regulamento, mas também com os valores e princípios fundantes do Estado de Direito Democrático.

¹⁸² DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**. 2.^a ed. São Paulo: Revista dos Tribunais, 2019, p. 325.

¹⁸³ DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**. 2.^a ed. São Paulo: Revista dos Tribunais, 2019, p. 327.

¹⁸⁴ *Ibid.*, p. 328-329.

2 DA CONFORMIDADE ENTRE O REGIME DE PROTEÇÃO DE DADOS PESSOAIS, AS DECISÕES AUTOMATIZADAS E A DEFINIÇÃO DE PERFIS

2.1 Princípios relativos à proteção de dados pessoais e a licitude dos fundamentos para as operações de tratamento de dados

Cientes de que os dois grandes propósitos do RGPD são: (i) tutelar os direitos e as liberdades fundamentais das pessoas singulares, especificamente a proteção de dados; e (ii) promover a livre circulação dos dados pessoais (art. 1.º, 2 e 3)¹⁸⁵, toda lógica do sistema se encontra funcionalizada nesses dois grandes objetivos. Dessa forma, os considerados e os princípios, esses últimos positivados no artigo 4.º e vinculantes, assumem função primordial na interpretação do RGPD, razão pela qual são objeto do nosso estudo nesse tópico, assim como as bases legais para o tratamento lícito de dados.

A Carta de Direitos Fundamentais da Europa de 2000, por seu turno, em seu artigo 8.º dispõe que “todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito” (1), os quais “devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei” (2)¹⁸⁶.

Analisamos, então, os princípios aplicáveis aos tratamentos de dados pessoais e, em consequência, aqueles que se aplicam e possuem maior relevância no contexto das decisões automatizadas e definições de perfis.

2.1.1 Princípios relativos à proteção de dados pessoais

O primeiro princípio é o da licitude¹⁸⁷, previsto no artigo 5.º, (1), a), segundo o qual o tratamento deverá subsumir em concreto a uma ou mais causas de licitude tratadas no artigo 6.º do RGPD. Pressupõe o cumprimento do próprio Regulamento e legislação correlata¹⁸⁸.

¹⁸⁵ DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**. 2.ª ed. São Paulo: Revista dos Tribunais, 2019, p. 197-198. No mesmo sentido, CORDEIRO, António Barreto Menezes – **Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020, p. 33.

¹⁸⁶ UNIÃO EUROPEIA. Parlamento Europeu. Conselho. Comissão – Carta de Direitos Fundamentais União Europeia. **Jornal Oficial da União Europeia**. C 326/391. (26 out. 2012), p. 391-407.

¹⁸⁷ Art. 1.º (a) (*id.* – Regulamento n.º 679, 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). **Jornal Oficial da União Europeia** [Em linha]. L 119, n.º 2 (04 maio 2016). [Consult. 10 nov. 2019]. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:32016R0679>).

¹⁸⁸ VAINZOF, Rony – **Comentários ao GDPR – Regulamento de Dados da União Europeia**. 2.ª ed. São Paulo: Thomson Reuters Brasil, 2019, p. 47.

contatos com o titular de dados até a eliminação, mantendo-se até mesmo após o fim da relação, e englobando tanto o conteúdo das informações passadas ao titular até os procedimentos de transmissão. Esse princípio não se esgota no direito à informação aos titulares e tem inegável ligação com o princípio da lealdade e da licitude, considerando que o legislador entendeu por bem alinhá-los sucessivamente no dispositivo mencionado¹⁹⁴.

Em conformidade com o considerando 39¹⁹⁵ e o artigo 12.º, o princípio da transparência exige que todas as informações a respeito do tratamento de dados sejam claras, concisas, de fácil acesso e compreensão, com a indicação do responsável pelo tratamento e a finalidade à qual ele se destina. As obrigações de transparência também se encontram previstas no artigo 13.º, dentre as quais se encontra a obrigação de informar sobre a existência de decisões automatizadas, incluindo a definição de perfis, com informações úteis à lógica subjacente, bem como as potenciais consequências previstas do tratamento para o titular.

Além disso, o responsável pelo tratamento deverá ter em conta o público-alvo do tratamento e o nível de compreensão para fazer as adaptações necessárias à comunicação¹⁹⁶.

A transparência do tratamento é requisito fundamental do RGPD. O processo de definição de perfis é muitas vezes imperceptível aos olhos do titular. A definição de perfil pode se dar com dados obtidos na internet, lá expostos pelo próprio titular em redes sociais,

¹⁹⁴ CORDEIRO, António Barreto Menezes – **Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020, p. 154-155.

¹⁹⁵ “Qualquer processamento de dados pessoais deve ser legal e justo. Deve ser transparente para pessoas singulares cujos dados pessoais que lhes dizem respeito são coletados, usados, consultados ou processados de outra forma e em que medida os dados pessoais são ou serão processados. O princípio da transparência exige que qualquer informação e comunicação relativa ao tratamento desses dados pessoais seja facilmente acessível e fácil de entender, e que seja usada uma linguagem clara e simples. Esse princípio diz respeito, em particular, à informação aos titulares dos dados sobre a identidade do responsável pelo tratamento e a finalidades do processamento e informações adicionais para garantir um processamento justo e transparente a respeito das pessoas singulares em causa e o seu direito de obter confirmação e informação sobre dados pessoais que lhes digam respeito que estão sendo tratados. As pessoas singulares devem ser cientificadas dos riscos, regras, garantias e direitos em relação ao processamento de dados pessoais e como exercer seus direitos em relação a tal processamento. Em particular, os propósitos específicos para os quais os dados pessoais são tratados devem ser explícitos e legítimos e determinados no momento da recolha dos dados pessoais. Os dados pessoais devem ser adequados, relevantes e limitados ao que é necessário para os fins para os quais são processados. Isto requer, em particular, assegurar que o período durante o qual os dados pessoais são armazenados é limitado a um mínimo necessário. Dados pessoais somente devem ser tratados se a finalidade do processamento não puder ser razoavelmente cumprida por outros meios. A fim de garantir que os dados pessoais não sejam mantidos por mais tempo do que o necessário, os prazos devem ser estabelecidos pelo controlador para eliminação ou para uma revisão periódica. Cada passo razoável deve ser tomado para garantir que os dados pessoais imprecisos sejam retificados ou excluídos. Os dados pessoais devem ser processados de maneira a garantir a segurança e a confidencialidade apropriadas dos dados pessoais, inclusive para impedir o acesso ou uso não autorizado de dados pessoais e a equipamentos utilizados para o processamento”. Tradução livre para o português do comentário ao artigo 5 (Article 5), sobre o considerando 39 (recital 39) (KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher – **The EU General Data Protection Regulation (GDPR): A commentary**. Oxford: Oxford University Press, 2020, p. 309-310).

¹⁹⁶ VAINZOF, Rony – **Comentários ao GDPR – Regulamento de Dados da União Europeia**. 2.ª ed. São Paulo: Thomson Reuters Brasil, 2019, p. 51-52.

por exemplo, ou inseridos por terceiros sem que os titulares se deem conta de que poderiam ter usos desvinculados das finalidades as quais inicialmente levaram à exposição. Além disso, as pessoas possuem níveis de compreensão diversos, conforme seu nível social ou de escolaridade, ou conforme tenham sido familiarizadas em maior ou menor grau com a evolução da tecnologia, sendo certo, ainda, que existem técnicas complexas envolvidas nas decisões automatizadas e definições de perfis¹⁹⁷.

As orientações do Grupo de Trabalho do artigo 29.º para Proteção de Dados sobre as Decisões Automatizadas e Definições de Perfis traz exemplos da infringência ao princípio da transparência e da lealdade, desde o corretor de dados que vende perfis de consumidores a sociedades financeiras sem consentimento ou conhecimento dos titulares, até seguradoras que oferecem tarifas e serviços de seguros com base no comportamento da pessoa ao volante^{198,199}

Já o princípio da finalidade está previsto no artigo 5.º, b) e consiste na exigência de que os dados só serão “recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 (limitação das finalidades)”²⁰⁰.

O Grupo de Trabalho do Artigo 29, na opinião 03/2013, sobre a limitação de finalidade (*purpose limitation*), definiu os conceitos que compreendem o princípio da finalidade: (i) específica: antes ou no momento da coleta de dados, os objetivos devem ser precisos e totalmente identificados para determinar se o processamento está dentro da finalidade apresentada, bem como para permitir que a licitude do tratamento seja aferida; (ii) explícita: revelada de forma clara, explícita, explicada, para garantir que todos os envolvidos tenham o mesmo nível de entendimento da finalidade do tratamento, independente da diversidade cultural ou linguística; (iii) legítima: vai além da licitude do tratamento,

¹⁹⁷ Considerando 72: “A definição de perfis está sujeita às regras do presente regulamento que regem o tratamento de dados pessoais, como o fundamento jurídico do tratamento ou os princípios da proteção de dados. O Comité Europeu para a Proteção de Dados criado pelo presente regulamento («Comité») deverá poder emitir orientações nesse âmbito”.

¹⁹⁸ UNIÃO EUROPEIA. Comissão – **Orientações sobre as decisões automatizadas e definições de perfis para efeitos do Regulamento 2016/679**. Grupo de Trabalho do 29.º para Proteção de Dados. Com a última redação revista e adotada em 6 de fevereiro de 2018 [Em linha]. Bruxelas, 27 abr. 2016. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>.

¹⁹⁹ Ver também: EUROPEAN UNION. Commission – **Guidelines on transparency under Regulation 2016/679**. Article 29 Data Protection Working Group [Em linha]. Bruxelas, 27 Apr. 2016. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/622227/en>.

²⁰⁰ UNIÃO EUROPEIA – Regulamento (EU) 2016/679 (General Data Protection Regulation - GDPR). **Jornal Oficial da União Europeia**. L119. (04 maio 2016), p. 1-88.

podendo se estender a outras áreas do direito, devendo ser interpretada no contexto do processamento^{201,202,203}.

O mesmo Grupo de Trabalho do Artigo 29.º, nas Orientações sobre as decisões individuais automatizadas e a definição de perfis, comentando sobre o princípio da finalidade, cuida especialmente sobre as ocasiões em que a definição de perfis poderá abranger o uso de dados recolhidos para fins inicialmente distintos, por isso observa que eventual incompatibilidade com as finalidades iniciais para os quais foram recolhidos os dados dependerá de um conjunto de fatores, notadamente as informações inicialmente fornecidas pelo responsável pelo tratamento ao titular dos dados recolhidos. Tais fatores estão refletidos no artigo 6.º, n.º 4 do RGPD: “a relação entre a finalidade para a qual os dados foram recolhidos e a finalidade do tratamento posterior; o contexto em que os dados foram recolhidos e as expectativas razoáveis dos titulares dos dados quanto à sua posterior utilização; a natureza dos dados; o impacto do tratamento posterior sobre os titulares; as garantias aplicadas pelo responsável pelo tratamento para assegurar a lealdade do tratamento e evitar qualquer impacto indevido sobre os titulares dos dados”^{204,205}.

Por fim e em relação à limitação da finalidade, Rony Vainzof cita discussão inaugurada por Lokke Moerel e Corien Prins no sentido de que modernamente a avaliação do legítimo interesse estaria mais adequada do que “uma análise única e segregada da limitação

²⁰¹ VAINZOF, Rony – **Comentários ao GDPR – Regulamento de Dados da União Europeia**. 2.ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 53.

²⁰² No mesmo sentido: CORDEIRO, António Barreto Menezes – **Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020, p. 156.

²⁰³ “Finally, the purposes must be legitimate, which means that they may not entail a disproportionate interference with the rights, freedoms and interests at stake, in the name of the interests of the data controller: What is considered a legitimate purpose depends on the circumstances as the objective is to ensure that a balancing of all rights, freedoms and interests at stake is made in each instance; the right to the protection of personal data on the one hand, and the protection of other rights on the other hand, as, for example, between the interests of the data subject and the interests of the controller or of society. In all cases, data processing serving an unlawful purpose (*i.e.* contrary to the law) cannot be considered to be based on a legitimate purpose” (KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher – **The EU General Data Protection Regulation (GDPR): A commentary**. Oxford: Oxford University Press, 2020, p. 315).

²⁰³ VAINZOF, Rony, *op. cit.*, p. 51-52.

²⁰⁴ UNIÃO EUROPEIA. Comissão – **Orientações sobre as decisões automatizadas e definições de perfis para efeitos do Regulamento 2016/679**. Grupo de Trabalho do 29.º para Proteção de Dados. Com a última redação revista e adotada em 6 de fevereiro de 2018 [Em linha]. Bruxelas, 27 abr. 2016, p. 12. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>.

²⁰⁵ O professor Menezes Cordeiro também ressalta a preocupação as finalidades do tratamento de dados, a formação de perfis e as limitações impostas pelo RGPD, afirmando que “a impossibilidade de rever finalidades assume especial relevância no âmbito da denominada Big Data” (CORDEIRO, António Barreto Menezes – **Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020, p. 155).

da finalidade”, a qual continuaria sendo importante, “mas deve estar vinculada ao legítimo interesse, e não mais ao objetivo original da coleta de dados”^{206,207}.

O princípio da minimização²⁰⁸ está previsto no artigo 5.º, n. 1, c), do RGPD e está intimamente ligado ao princípio da limitação de finalidades. Por esse princípio, os dados devem ser adequados, pertinentes e limitados ao que é estritamente necessário aos cumprimentos das finalidades para as quais foram recolhidos, bem como poderão ser retidos apenas pelo tempo necessário para atingir um propósito específico.

No RGPD, o princípio da minimização ganha contornos mais exigentes do que havia na Directiva n.º 95/46/CE, considerando que a expressão “não excessivos” foi substituída pela expressão “limitados ao que é necessário”²⁰⁹.

²⁰⁶ VAINZOF, Rony – **Comentários ao GDPR – Regulamento de Dados da União Europeia**. 2.ª ed. São Paulo: Thomson Reuters Brasil, 2019, p. 56.

²⁰⁷ “Ademais, era do Big Data, IoT e Inteligência Artificial, na qual a sociedade é orientada por dados, a análise dos referidos requisitos legais do purpose limitation em consonância com a evolução tecnológica é imprescindível, pois, por exemplo, dispositivos que coletam dados de saúde de cidadãos podem antever epidemias, servindo os dados de grande valor para agências governamentais agirem preventivamente na proteção da sociedade. Sobre o assunto, Lokke Moerel e Corien Prins provocam uma discussão interessante: a avaliação do legítimo interesse, na atual era, seria mais adequada do que uma análise única e segregada da limitação da finalidade, que continua sendo relevante, mas deve estar vinculada ao legítimo interesse, e não mais ao objetivo original dados. Parece que tal provocação faz sentido, pois, anteriormente, a coleta de dados pessoais servia como requisito para a utilização de um serviço, como na abertura de uma conta em um banco, mediante o fornecimento de dados cadastrais. Os dados eram principalmente um subproduto da finalidade para a qual eles foram coletados. Porém, agora, referidos dados fazem praticamente parte dos próprios serviços, como nos casos de cidades inteligentes, automação domiciliar ou automóveis autônomos. É improvável deixar de pensar que ‘finalidades determinadas e explícitas’ deverão ser analisadas de forma mais abrangente, mas não como um cheque em branco, é claro. De certa forma, perderão espaço para a análise da ‘finalidade legítima’ e o interesse legítimo do titular. Em sua Opinion 8/2014, sobre IoT, o Art. 29 WP passou a aplicar primeiramente a avaliação de base legal do controller para tratamento de dados, no caso o legítimo interesse, para então verificar o princípio da limitação da finalidade, que praticamente se equivaleria ao primeiro. Por sua vez, em sua Opinion 06/2014, ainda com base na Diretiva 95/46/EC sobre legítimo interesse, o Art. 29 WP dispõe que há uma ligação clara entre a avaliação da necessidade e da conformidade do legítimo interesse com o princípio da limitação da finalidade, sempre considerando a natureza e a origem do interesse legítimo, por um lado, e o impacto do tratamento dos dados ao titular, por outro. Assim, parece-nos que, atualmente, os elementos do princípio da limitação da finalidade estariam cobertos quando realizado o teste do legítimo interesse” (*ibid.*, *loc. cit.*).

²⁰⁸ O Grupo de Trabalho do Art. 29.º consigna que “as oportunidades de negócio geradas pela definição de perfis, os custos mais reduzidos de conservação e a capacidade para tratar grandes quantidades de informação podem incentivar as organizações a recolherem mais dados pessoais do que o efetivamente necessário, para o caso de se revelarem úteis no futuro. Os responsáveis pelo tratamento devem assegurar que respeitam o princípio da minimização dos dados, assim como os requisitos no âmbito dos princípios da limitação das finalidades e da limitação da conservação. Os responsáveis pelo tratamento devem ser capazes de explicar e justificar com clareza a necessidade de recolher e manter dados pessoais, ou considerar o recurso a dados agregados, anonimizados ou (quando tal assegure uma proteção suficiente) pseudonimizados para a definição de perfis” (UNIÃO EUROPEIA. Comissão – **Orientações sobre as decisões automatizadas e definições de perfis para efeitos do Regulamento 2016/679**. Grupo de Trabalho do 29.º para Proteção de Dados. Com a última redação revista e adotada em 6 de fevereiro de 2018 [Em linha]. Bruxelas, 27 abr. 2016, p. 12. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>).

²⁰⁹ CORDEIRO, António Barreto Menezes – **Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020, p. 158.

Para efeitos do princípio da minimização deve ser feito, então, um teste de razoabilidade e adequação para atingimento das finalidades específicas do tratamento, pelo qual se a natureza e quantidade de dados pessoais forem proporcionais às finalidades do tratamento, ele será lícito²¹⁰.

Outro princípio de interesse para nosso tema é o princípio da exatidão, estabelecido no artigo 5.º, n.º 1, d), o qual abrange a proibição da recolha ou armazenamento dados incorretos; o dever de atualização dos dados detidos, sempre que necessário; o dever de apagamento ou retificação dos dados incorretos à luz das finalidades do tratamento. Aqui a tutela se circunscreve a dados objetivos (e não os subjetivos)²¹¹.

Menezes Cordeiro enfatiza que a inexatidão de dados pode gerar um impacto enorme na vida dos indivíduos, mas que, no entanto, nem todos os dados devem estar, o tempo todo, atualizados, considerando que alguns deles só geram interesse na medida em que se mantêm desatualizados em respeito a realidades passadas, a exemplo dos dados médicos descritos em prontuários e que refletem um estado de saúde antigo, mas que fazem parte do histórico do paciente. Por outro lado, assevera, a incorreção pode ser irrelevante para as finalidades perseguidas, de modo que não afetariam o tratamento ou os resultados que decorram de sua análise²¹².

Entre nós, entendemos que, de fato, se os dados incorretos não afetam o resultado perseguido pelo tratamento, não haveria impacto na esfera de direitos e liberdades do titular. Contudo, imprescindível notar a necessidade de que todos os demais princípios sejam observados no tratamento e, nessa hipótese específica, os princípios da transparência e lealdade adquirem grande relevância, uma vez que, para que o titular possa saber da existência de dados inexatos a seu respeito sendo tratados e avaliar se podem ter interferido ou não no resultado, é necessário o acatamento da transparência e lealdade por parte dos responsáveis. Sem isso, retira-se do titular até mesmo seu lícito direito de se insurgir contra os resultados obtidos, cabendo a ele avaliar se houve ou não o impacto, em vista, ainda, da autodeterminação informativa.

O princípio da limitação da conservação encontra-se previsto no artigo 5.º, n.º 1, e), e pressupõe que o armazenamento dos dados pelos responsáveis pelo tratamento está temporalmente limitado ao período necessário ao atingimento de suas finalidades. Assim, os

²¹⁰ VAINZOF, Rony – **Comentários ao GDPR – Regulamento de Dados da União Europeia**. 2.ª ed. São Paulo: Thomson Reuters Brasil, 2019, p. 58.

²¹¹ CORDEIRO, António Barreto Menezes – **Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020, p. 159.

²¹² *Ibid.*, p. 160.

responsáveis pelo tratamento deverão fixar prazos e revê-los de tempos em tempos para garantir que os dados sejam armazenados apenas pelo tempo necessário. Já a segunda parte do preceito traz exceção ao princípio em questão, onde os dados poderão ser conservados por períodos mais alargados para fins de arquivamento de interesse público, para fins de investigação científica ou histórica, ou para fins estatísticos, consoante disposição do artigo 89.º, n.º 1^{213,214}.

As decisões automatizadas e de perfis, por sua natureza, tendem a tratar um volume considerável de dados para estabelecer correlações e estabelecer perfis mais complexos e exatos. No entanto, apesar de o armazenamento prolongado apresentar vantagens para definição desses perfis, principalmente tendo em consideração o aprendizado de máquina (para que o algoritmo possa aprender), os responsáveis pelo tratamento deverão assegurar a observância do princípio de dados mínimos quando da recolha e que os armazenarão apenas pelo período necessário ao atingimento das finalidades do tratamento, bem como que os dados permanecerão atualizados durante o período de conservação como forma de reduzir o risco de inexactidões. Além disso, a política de conservação deverá considerar os direitos e liberdades das pessoas, em conformidade com os requisitos do referido dispositivo²¹⁵.

Por derradeiro, temos os princípios da integridade e confidencialidade, bem como da responsabilidade. Em que pese as Orientações sobre as decisões automatizadas e definições de perfis para efeitos do RGPD do Grupo de Trabalho do artigo 29.º não tratem da aplicabilidade desses princípios às decisões automatizadas e definições de perfis, mesmo na revisão de 2018, entendemos que também são relevantes. Nota-se, ainda, que não foram tratados na Directiva n.º 95/46/CE, tendo sua inclusão no RGPD sido sugerida pelo Parlamento²¹⁶.

Por integridade e confidencialidade se entende a imposição da obrigação dos responsáveis pelo tratamento de garantirem a segurança (contra perda, destruição, etc.) e a confidencialidade dos dados, adotando as medidas técnicas e organizacionais adequadas e necessárias a garantir o seu cumprimento. Considerando que o tratamento automatizado e as definições de perfis se utilizam, normalmente, de uma quantidade de dados consideravelmente maior que outras formas de tratamento, a obediência a esse princípio é de

²¹³ KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher – **The EU General Data Protection Regulation (GDPR): A commentary**. Oxford: Oxford University Press, 2020, p. 318.

²¹⁴ CORDEIRO, António Barreto Menezes – **Direito da Protecção de Dados: à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020, p. 160.

²¹⁵ UNIÃO EUROPEIA. Comissão – **Orientações sobre as decisões automatizadas e definições de perfis para efeitos do Regulamento 2016/679**. Grupo de Trabalho do 29.º para Protecção de Dados. Com a última redação revista e adotada em 6 de fevereiro de 2018 [Em linha]. Bruxelas, 27 abr. 2016, p. 13. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>.

²¹⁶ CORDEIRO, António Barreto Menezes, *op. cit.*, *loc. cit.*

evidente relevância, tendo em conta o impacto para os titulares de dados por eventual incidente de segurança.

O princípio da responsabilidade é o último princípio previsto no elenco do artigo 5.º e prevê dois deveres distintos: (i) de o responsável pelo tratamento atuar sempre em estrito cumprimento dos princípios previstos no dispositivo, bem como (ii) de poder demonstrar/comprovar²¹⁷, notadamente às autoridades de controle e tribunais, o cumprimento dos mesmos princípios, dever este que não poderá ser delegado a um subcontratante ou encarregado (art. 5.º, n.º 2). Esse último dever representa mais uma obrigação imposta aos responsáveis pelo tratamento no RGPD, considerando que não havia essa previsão sob a égide da Directiva n.º 95/46/CE²¹⁸.

Nesse sentido, a exigência de obrigação relacionada à comprovação da conformidade estará trabalhando não só em prol da garantia de existência e aplicação das medidas necessárias à conformidade, na medida que só se pode documentar e comprovar o que existe, mas por ser mais uma forma de garantir a transparência nas operações de tratamento, o que sempre representará um elemento que possibilita o controle por parte das autoridades e do Judiciário e, por fim, um meio a proporcionar ao indivíduo eventualmente lesado, a buscar evitar a lesão a seus direitos e garantias de liberdade, além de eventual reparação.

No próximo tópico apresentamos as bases legais em que poderá se dar o tratamento de dados, as quais deverão ser interpretadas e acatadas em conjunto com os princípios aqui analisados, sendo certo que o tratamento que contrarie os princípios ou que não esteja albergado em uma das bases legais será ilícito.

2.1.2 Da licitude dos fundamentos para as operações de tratamento

O artigo 6.º, n.º 1, traz o elenco taxativo e os únicos fundamentos para o tratamento lícito de dados pessoais, de modo a densificar o princípio da licitude, sendo certo que “o tratamento só é lícito se e na medida em que se verifique pelo menos uma”²¹⁹ das situações constantes do elenco de a) a f).

²¹⁷ Considerando 45: “A responsabilidade do responsável pelo tratamento deverá ser estabelecida em relação ao tratamento de dados pessoais realizado por si ou por sua conta. Em especial, o responsável pelo tratamento deverá ser obrigado a executar as medidas que forem adequadas e eficazes e ser capaz de demonstrar a conformidade das atividades de tratamento com o presente regulamento, incluindo a eficácia das medidas. Essas medidas deverão ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e as liberdades das pessoas singulares”.

²¹⁸ CORDEIRO, António Barreto Menezes – **Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020, p. 161-162.

²¹⁹ UNIÃO EUROPEIA – Regulamento (EU) 2016/679 (General Data Protection Regulation - GDPR). **Jornal Oficial da União Europeia**. L119. (04 maio 2016), p. 1-88.

O primeiro dos seis fundamentos legais para o tratamento elencados na norma é o consentimento. Por princípio, o titular de dados deveria consentir com o tratamento, como uma das principais garantia de proteção aos interesses dos titulares. Trata-se de garantia consagrada também na Carta Europeia (artigo 8.º, n.º 2) e principal causa de legitimidade e licitude do tratamento²²⁰.

O regime do consentimento, de forma geral e não sem críticas doutrinárias²²¹, se encontra no artigo 7.º, acrescido de disposições de caráter especial previstas ao longo do RGPD, quais sejam, as relacionadas no capítulo dos direitos dos titulares, no regime do consentimento dado por crianças (artigo 8.º); no tratamento de dados pessoais sensíveis (artigo 9.º, n.º 2); nas decisões individuais automatizadas (artigo 22.º); e na transferência de dados para países terceiros ou organizações internacionais²²². O consentimento se constitui em manifestação de vontade, livre, específica, infirmada e explícita (artigo 4.º, n.º 11).

O consentimento explícito é umas das exceções à proibição às decisões automatizadas prevista o artigo 22.º, n.º 1, do RGPD, importando notar que a definição de perfis pode ser pouco transparente e se sustenta, no mais das vezes, em dados obtidos ou inferidos de outros dados, os quais, por sua vez, não são fornecidos diretamente pelo titular. Além disso, os responsáveis que buscarem basear o tratamento no consentimento deverão ser capazes de demonstrar que os titulares dos dados estão cientes e compreendem exatamente o tipo, o contexto e possíveis resultados do tratamento (informações suficientes sobre a utilização e consequências) que envolve seu consentimento, garantindo que este importa em uma escolha informada, bem como tem ciência de que o consentimento nem sempre constitui um fundamento adequado para o tratamento²²³.

Rony Vainzof esclarece que o tratamento automatizado, incluindo a definição de perfis, serve para avaliar certos aspectos da pessoa do titular, como analisar ou prever seu desempenho no trabalho, a sua situação econômica e capacidade de pagamento, sua saúde, preferências e interesses pessoais, confiabilidade, localização e deslocamento, por exemplo,

²²⁰ Nesse sentido, CORDEIRO, António Barreto Menezes – **Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020, p. 161-162.

²²¹ Nesse sentido, *ibid.*, p. 168.

²²² Sobre o consentimento consultar: EUROPEAN UNION. Data Protection Board – **Guidelines 05/2020 on consent under Regulation 2016/679**. Article 29 Data Protection Working Group [Em linha]. Brussels, 04 May 2020. [Consult. 15 jul. 2022]. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Quanto às críticas ao consentimento: CORDEIRO, António Barreto Menezes, *op. cit.*, p. 168-171.

²²³ UNIÃO EUROPEIA. Comissão – **Orientações sobre as decisões automatizadas e definições de perfis para efeitos do Regulamento 2016/679**. Grupo de Trabalho do 29.º para Proteção de Dados. Com a última redação revista e adotada em 6 de fevereiro de 2018 [Em linha]. Bruxelas, 27 abr. 2016, p. 13-14. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>.

Algumas vezes poderá haver uma obrigação jurídica de proceder à definição de perfis, a exemplo da prevenção a fraudes ou branqueamento de capitais²²⁸.

A quarta base legal é o tratamento necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular, estabelecida no artigo 6.º, n.º 1, d). Esse fundamento abrange situações em que o tratamento se faz necessário para proteção de um interesse essencial à vida do titular de dados ou de outra pessoa. Um possível exemplo é a definição de perfis necessários ao desenvolvimento de pesquisas e agilidade na análise de resultados de pesquisas que têm por escopo a cura de doenças ou a evitação da propagação delas, como no caso da pandemia da Covid-19. Se o tratamento envolver o tratamento de dados pessoais sensíveis, o responsável terá que assegurar o cumprimento dos requisitos estabelecidos no artigo 9.º, n.º 2, c)²²⁹.

A base legal para tratamento de dados pessoais prevista no artigo 6.º, n.º 1, e) não apresenta maiores dificuldades; refere-se ao tratamento necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento. Em determinadas circunstâncias esta base poderá servir para amparar a utilização das decisões automatizadas e definições de perfis, conquanto as suas finalidades e competências tenham fundamento legal inequívoco²³⁰.

Por fim, o RGPD confere, no artigo 6.º, n.º 1, f), licitude ao tratamento de dados pessoais que for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança. Ou seja, o tratamento baseado no interesse legítimo deverá observar a vedação no caso de prevalecerem os interesses ou direitos e liberdades fundamentais do titular de dados.

As decisões automatizadas e a definição de perfis será, então, permitida se for necessária para efeitos dos interesses legítimos²³¹ prosseguidos pelo responsável pelo tratamento ou por terceiros. Contudo, essa hipótese não é automaticamente aplicável em função da existência de um interesse legítimo. O responsável pelo tratamento deve realizar

²²⁸ UNIÃO EUROPEIA. Comissão – **Orientações sobre as decisões automatizadas e definições de perfis para efeitos do Regulamento 2016/679**. Grupo de Trabalho do 29.º para Proteção de Dados. Com a última redação revista e adotada em 6 de fevereiro de 2018 [Em linha]. Bruxelas, 27 abr. 2016, p. 15. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>.

²²⁹ *Ibid.*, *loc. cit.*

²³⁰ *Ibid.*, *loc. cit.*

²³¹ O interesse legítimo do responsável pelo tratamento não pode ser base de tratamento lícito quando o tratamento se enquadrar na hipótese do artigo 22.º, n.º 1, do RGPD.

um exercício de ponderação com base no qual será possível verificar se aos seus interesses se sobrepõem os interesses ou os direitos e as liberdades fundamentais do titular dos dados.

Há situações em que o legítimo interesse do empregador poderá ser invocado, mas apenas se o processamento é estritamente necessário para um propósito legítimo e o processamento está em conformidade com os princípios da proporcionalidade e da subsidiariedade. Em caso de uso de ferramenta de monitoramento, por exemplo, um teste de proporcionalidade deve ser realizado antes da implantação da ferramenta, para avaliar se todos os dados são necessários, se esse processamento supera os direitos gerais de privacidade que os funcionários também têm no local de trabalho e que medidas devem ser tomadas para garantir que as infrações ao direito de reserva da vida privada e o direito ao sigilo das comunicações são limitados ao mínimo necessário²³².

O Grupo de Trabalho do Artigo 29.º considera os seguintes requisitos para a caracterização do legítimo interesse: (i) que seja lícito; (ii) que seja concreto e claro o teste de equilíbrio entre os interesses em jogo e os direitos fundamentais do titular; (iii) que se refira a um interesse real e atual, não podendo ser especulativo²³³.

Sempre que houver decisões automatizadas e definição de perfis é indispensável que haja uma avaliação cuidadosa. Especialmente se o titular de dados pode prever, razoavelmente, no momento e no contexto em que os dados são coletados, que estes poderão vir a ser tratados com essa finalidade. Os interesses dos titulares poderão sobrepor-se aos interesses do responsável pelo tratamento, quando os dados pessoais forem tratados em circunstâncias em que os titulares não esperam tratamento adicional^{234,235}.

O dado pessoal é hoje o principal insumo da economia global e de políticas públicas modernas. Os indivíduos, consciente ou inconscientemente, estão fornecendo inúmeros dados pessoais para as mais diversas atividades e finalidades. Essa realidade não mudará, e isso nem seria desejável diante dos inúmeros benefícios já alcançados para a humanidade e que ainda virão nos mais variados setores. Contudo, diante dos riscos de significativos impactos nos

²³² EUROPEAN UNION. Commission – **Opinion 2/2017 on data processing at work**. Article 29 Working Party [Em linha]. Brussels, 08 June 2017. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/610169/en>.

²³³ *Id.* – **Opinion 06//2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. Article 29 Data Protection Working Party [Em linha]. Brussels, 09 April 2014. [Consult. 15 jul. 2022]. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

²³⁴ Considerando 47: “A probabilidade e a gravidade dos riscos para os direitos e as liberdades do titular dos dados deverão ser determinadas por referência à natureza, ao âmbito, ao contexto e às finalidades do tratamento. Os riscos deverão ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam um risco ou um risco elevado”.

²³⁵ VAINZOF, Rony – **Comentários ao GDPR – Regulamento de Dados da União Europeia**. 2.ª ed. São Paulo: Thomson Reuters Brasil, 2019, p. 74-75.

direitos e garantias de liberdade dos indivíduos, o RGPD vem como um mecanismo de freios e contrapesos no intuito de que a utilização desses dados pessoais se dê de forma leal, justa, lícita, legítima, digna, transparente e proporcional, sempre garantindo que toda a tecnologia e inovação continuem a servir, cada vez mais brilhantemente, ao ser humano.

2.2 Aproximação conceptual do RGPD: definição de perfis e decisões automatizadas

Segundo a noção do sítio eletrónico oficial da Comissão da União Europeia encontramos a informação segundo a qual “a definição de perfis e as decisões automatizadas são prática comum em vários setores, como os setores bancário e financeiro, fiscal e da saúde. Pode ser mais eficiente, mas menos transparente e pode limitar as suas opções. Embora, como regra geral, as pessoas não devam ser sujeitas a uma decisão baseada exclusivamente em tratamento automatizado, este tipo de decisão pode ser permitido, a título excepcional, se a utilização de algoritmos for permitida por lei e forem consagradas as salvaguardas adequadas”²³⁶.

Os dados de um cidadão podem estar sendo objeto de definição de perfil sem que se dê conta e sem que alcance os interesses que estão em jogo e suas possíveis consequências. Como mencionado, a definição de perfis pode perpetuar estereótipos existentes e a segregação social, pode prender certos seres humanos a uma categoria determinada e limitá-los às suas preferências sugeridas, cerceando sua liberdade de escolha desde a aquisição de determinado produto ou serviço até a preferência musical e na escolha do próximo candidato à Presidência da República²³⁷. Por outro lado, poderá gerar a negativa de acesso a determinados bens e serviços, por uma discriminação injusta efetuada pela máquina.

Assim, necessária se faz a definição do que são tais figuras e a forma como são tratadas no RGPD para compreensão dos mecanismos e salvaguardas existentes para proteção do indivíduo e garantia de suas liberdades e dignidade, dentre os quais se encontram: requisitos de transparência e lealdade; obrigações acrescidas em matéria de responsabilidade; fundamentos jurídicos e específicos para o tratamento; direitos de oposição à definição de

²³⁶ UNIÃO EUROPEIA. Comissão – **Posso ser sujeito a decisões individuais automatizadas, incluindo a definição de perfis?** [Em linha]. Bruxelas, 2022. [Consult. 15 jul. 2022]. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_pt.

²³⁷ Para exemplo do uso do Big Data, definição de perfis e manipulação, inclusive, com efeitos em eleições, confira: KAISER, Brittany – **Targeted: The Cambridge Analytica Whistleblower’s Inside Story of How Big Data, Trump, Brexit and Facebook Broke Democracy and How It Can Happen Again**. New York: HarperCollins, 2019.

perfis e, notadamente, à definição de perfis para fins comerciais; e a necessidade de se proceder a uma avaliação de impacto e determinadas circunstâncias.

2.2.1 Definição de perfis

A definição do que consiste a definição de perfis se encontra prevista no artigo 4.º, n.º 4, do RGPD, segundo o qual a definição de perfis é “qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações”.

Da definição acima destacada percebe-se a existência de três elementos, quais sejam: deve haver uma forma de tratamento automatizado, que pode ser totalmente/exclusivamente automatizado ou não; realizado com dados pessoais; e com objetivo de avaliar os aspectos pessoais do indivíduo ou grupo de indivíduos, sendo irrelevante a eficácia do procedimento²³⁸.

A definição de perfis, ao que indica a definição constante do RGPD, implica em uma série de deduções estatísticas a respeito de aspectos pessoais, que pode implicar em previsões sobre as pessoas recorrendo a dados provenientes de várias fontes. A expressão *avaliar* indica que a definição de perfis envolve algum tipo de apreciação ou juízo sobre a pessoa.

De acordo com o disposto nas Orientações sobre as decisões individuais automatizadas e a definição de perfis, do Grupo de Trabalho do Artigo 29.º, “uma simples classificação de pessoas com base em características conhecidas, como a idade, o sexo e a altura, não acarreta necessariamente uma definição de perfis. Tal dependerá da finalidade da classificação”²³⁹. O exemplo trazido nas orientações diz respeito à hipótese em que uma empresa pretende classificar os seus clientes em função da idade ou do gênero para fins

²³⁸ Nesse sentido: “o primeiro elemento abrange tratamentos efetuados total ou parcialmente por meios automatizados: de fora ficam apenas os tratamentos efetuados exclusivamente por meios manuais. Em princípio, o processo de avaliação é prosseguido por recurso a processos algorítmicos ou similares. Com a sujeição dos dados pessoais a estes procedimentos pretende-se analisar ou prever aspetos relacionados com o desempenho profissional dos respetivos titulares, assim como a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações. A organização ou estruturação dos dados não basta para que essa operação seja, só por isso, subsumível ao conceito de definição de perfis, é necessário um *plus*, ou seja: a intenção de avaliar ou prever certos aspetos dos titulares de dados. A eficácia do procedimento é juridicamente irrelevante” (CORDEIRO, António Barreto Menezes – **Decisões Automatizadas à Luz do RGPD e da LGPD. Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa**. Indaiatuba: Foco, 2021. p. 263-270, p. 268).

²³⁹ UNIÃO EUROPEIA. Comissão – **Orientações sobre as decisões automatizadas e definições de perfis para efeitos do Regulamento 2016/679**. Grupo de Trabalho do 29.º para Proteção de Dados. Com a última redação revista e adotada em 6 de fevereiro de 2018 [Em linha]. Bruxelas, 27 abr. 2016, p. 7. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>.

estatísticos e com a intensão de obter uma visão do conjunto de seus clientes, sem realizar quaisquer previsões ou formar juízos a respeito das pessoas envolvidas no tratamento. Nessa hipótese, a finalidade não é fazer uma apreciação das características individuais, pelo que não se está diante de definição de perfis²⁴⁰.

O conceito de definição de perfis do RGPD é inspirado na Recomendação CM/Rec (2010) n.º 13 do Conselho da Europa, com a diferença de que exclui os tratamentos que não incluam inferências, bem como explica que a definição de perfis pode conter três fases, quais sejam: (i) recolha de dados; (ii) análise automatizada para identificação de correlações; (iii) aplicação das correlações a uma pessoa no intuito de identificar suas características comportamentais para servir à análise ou previsão de, por exemplo, sua capacidade para executar determinada tarefa; dos seus interesses; ou, ainda, do seu comportamento presumível^{241,242}.

2.2.2 Decisões automatizadas

António Barreto Menezes Cordeiro define decisão como “um ato, numa aceção não jurídica, que incida sobre um caso concreto e produza efeitos jurídicos relativamente a um ou mais titulares de dados específicos, quer seja a aceitação ou a recusa de um pedido, a sua caracterização, catalogação, atribuição de uma classificação, definição de perfilou qualquer outra medida análoga produtora de um efetivo resultado”²⁴³.

Para efeitos do RGPD, as decisões devem dizer respeito a um ou mais titulares de dados, pelo que não será atingido pela normativa do Regulamento as decisões abstratas e genéricas, ou que digam respeito a estratégias empresariais sem afetação da esfera jurídica dos titulares de dados. As decisões poderão emanar de pessoas singulares ou coletivas, do setor público ou privado.

Segundo as Orientações sobre decisões automatizadas e definições de perfis do Grupo de Trabalho do Artigo 29.º, decisões automatizadas podem sobrepor-se parcialmente à definição de perfis ou resultar dela, bem como que as decisões exclusivamente automatizadas

²⁴⁰ UNIÃO EUROPEIA. Comissão – **Orientações sobre as decisões automatizadas e definições de perfis para efeitos do Regulamento 2016/679**. Grupo de Trabalho do 29.º para Proteção de Dados. Com a última redação revista e adotada em 6 de fevereiro de 2018 [Em linha]. Bruxelas, 27 abr. 2016, p. 7. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>.

²⁴¹ *Id.* Conselho – **Recomendação CM/Rec (2010) 13 e exposição de motivos** [Em linha]. Bruxelas, 23 nov. 2010. [Consult. 28 jul. 2022]. Disponível em: <https://rm.coe.int/16807096c3>.

²⁴² UNIÃO EUROPEIA. Comissão, *op. cit.*, p. 8.

²⁴³ CORDEIRO, António Barreto Menezes – Decisões Automatizadas à Luz do RGPD e da LGPD. **Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa**. Indaiatuba: Foco, 2021. p. 263-270, p. 266.

são aquelas tomadas exclusivamente por meios tecnológicos e sem a intervenção humana, podendo basear-se em: dados fornecidos diretamente pelo titular; dados observados, a exemplo dos dados de localização; ou de dados obtidos ou inferidos, como os dados de classificação de crédito²⁴⁴.

As decisões automatizadas podem ocorrer com ou sem a definição de perfis, e, por sua vez, pode haver definição de perfis sem uma decisão automatizada. Desse modo, decisão automatizada e definição de perfis podem existir separadamente. Contudo, poderão coexistir a depender da forma com que os dados são utilizados na tomada de decisão²⁴⁵.

Assim, de acordo com o RGPD, pode haver definição de perfis sem que haja uma decisão; decisões tomadas com base em definição de perfil, sem que ela, decisão, seja exclusivamente automatizada, ou seja, que envolva total ou parcialmente a participação humana na tomada de decisão; e decisões exclusivamente automatizadas²⁴⁶, com definição de perfis, que podem produzir efeitos jurídicos ou afetar significativamente de forma similar a esfera pessoal do titular de dados (art. 22.º, n.º 1)²⁴⁷.

Por fim, cabe esclarecer que os responsáveis pelo tratamento poderão se utilizar de decisões automatizadas e definições de perfis desde que atendidos os princípios insculpidos no RGPD e o tratamento tenha fundamento em uma das bases legais elencadas no artigo 6.º.

2.3 Da especificidade da tutela relativa a categorias especiais de dados previstos no n.º 4.º do artigo 22.º do RGPD

O n.º 4 do artigo 22.º do RGPD enuncia que as decisões exclusivamente automatizadas as quais o titular de dados não poderá se negar a submeter-se (artigo 22.º, n.º 2), não poderão

²⁴⁴ UNIÃO EUROPEIA. Comissão – **Orientações sobre as decisões automatizadas e definições de perfis para efeitos do Regulamento 2016/679**. Grupo de Trabalho do 29.º para Proteção de Dados. Com a última redação revista e adotada em 6 de fevereiro de 2018 [Em linha]. Bruxelas, 27 abr. 2016, p. 8. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>.

²⁴⁵ O GT 29 cita dois exemplos: (i) a aplicação de coimas por excesso de velocidade com base exclusivamente em provas obtidas através de radares de velocidade, as quais são automatizadas, mas não incluem definição de perfis; (ii) se na mesma situação fosse associada a definição do perfil comportamental do motorista e sua avaliação para efeitos de reincidência do excesso de velocidade e tais fatores interferissem na aplicação da coima.

²⁴⁶ Decisões exclusiva ou totalmente automatizadas são aquelas que são produzidas sem qualquer intervenção humana (*vide* considerando 71). Trata-se de critério material, donde se entende que a previsão do artigo 22.º do RGPD restará verificada mesmo que haja intervenção humana de maneira meramente burocrática, para fins confirmadores da decisão proferida, despida de crítica. Nesse sentido, *vide* CORDEIRO, António Barreto Menezes – **Decisões Automatizadas à Luz do RGPD e da LGPD. Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa**. Indaiatuba: Foco, 2021. p. 263-270, p. 267.

²⁴⁷ Para as distinções *vide* OLIVEIRA, Madalena Perestrelo de – Definição de perfis e decisões individuais automatizadas no Regulamento Geral sobre a Proteção de Dados. *In* CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (ed.) – **Fin Tech II: Novos Estudos sobre Tecnologia Financeira**. Coimbra: Almedina, 2019. p. 61-88, p. 74.

se basear em categorias especiais de dados (artigo 9.º, n.º 1), a não ser que haja o consentimento explícito do titular, nos termos da letra a), do n.º 1, do artigo 9.º; e se o tratamento for necessário por motivos de interesse público importante, com base nas normas da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção de dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses dos titulares (letra g), do n.º 1, do artigo 9.º), ocasião em que deverão ser aplicadas as mesmas “medidas e adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular”. A preocupação do legislador não é sem fundamento.

De fato, desde as Orientações sobre as decisões automatizadas e definições de perfis para efeitos do RGPD, o GP 29 já alertava para o fato de que “a definição de perfis é suscetível de perpetuar os estereótipos existentes e a segregação social”, bem como que seria capaz de “igualmente amarrar as pessoas a uma categoria específica e limitá-las às respetivas preferências sugeridas, pondo assim em causa a sua liberdade para escolher, por exemplo, determinados produtos ou serviços, tais como livros, música ou fluxos de notícias”, podendo “dar origem a uma negação de serviços e bens e a uma discriminação injustificada”²⁴⁸.

Os trabalhos preparatórios do RGPD fornecem poucas explicações sobre os motivos e fundamentos políticos para o artigo 22.º. No entanto, é possível presumir que um objetivo central do artigo 22.º foi abarcar as preocupações que deram origem ao seu antecedente, qual seja, o artigo 15.º da Directiva 95/46/CE. O catalizador da disposição do artigo 15.º foi o potencial impacto negativo das definições automatizadas de perfis sobre a capacidade das pessoas de controlar a tomada de decisões que os afetassem significativamente. Na proposta inicial para o referido artigo (15.º) da Directiva, a Comissão destacou a preocupação de que “a utilização de extensos arquivos com perfis dos indivíduos por poderosas instituições públicas e privadas priva o indivíduo da capacidade de influenciar processos de tomada de decisão nessas instituições, caso as decisões sejam tomadas com base apenas em sua “sombra de dados”²⁴⁹. Além disso, a mesma Comissão teria expressado receio de que os tratamentos por meio de decisões totalmente automatizadas induzissem os indivíduos a pressupor a validade

²⁴⁸ UNIÃO EUROPEIA. Comissão – **Orientações sobre as decisões automatizadas e definições de perfis para efeitos do Regulamento 2016/679**. Grupo de Trabalho do 29.º para Proteção de Dados. Com a última redação revista e adotada em 6 de fevereiro de 2018 [Em linha]. Bruxelas, 27 abr. 2016, p. 6. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>.

²⁴⁹ KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher – **The EU General Data Protection Regulation (GDPR): A commentary**. Oxford: Oxford University Press, 2020, p. 526. Com livre tradução para o português da citação.

dessas decisões e, com isso, se abstivessem de assumir a responsabilidade de avaliar de forma independente as questões/consequências envolvidas²⁵⁰.

Nota-se nos comentários da Comissão a preocupação de resguardar a dignidade do indivíduo face ao determinismo da máquina e, em particular, ao permitir que os titulares de dados possam exercer em sua plenitude um protagonismo e se autodeterminar²⁵¹. A mesma preocupação também está estampada no Considerando 4, quando dita que “o tratamento dos dados pessoais deverá ser concebido para servir as pessoas”²⁵².

No mais, o GT 29 assevera que a definição de perfis pode acabar por criar categorias especiais de dados a partir de dados que, por si sós, não seriam especiais, mas que podem se tornar quando combinados com outros dados, como se poderia inferir o estado de saúde ou a existência de alguma enfermidade a partir dos hábitos de compras realizadas por um indivíduo em uma farmácia e/ou de seus hábitos alimentares através das compras de supermercado, por exemplo. Do mesmo modo, poder-se-ia chegar à crença religiosa do indivíduo ou grupo de indivíduos pela frequência com que se deslocam para determinado local onde há um culto religioso em especial. Investigadores conseguiriam prever por meio das “curtidas” (“likes”) no Facebook a orientação sexual e a origem étnica com mais de 85% de assertividade²⁵³.

Nesses casos, em que a definição de perfis acaba por deduzir preferências e dados sensíveis, o GT 29 sugere que o responsável pelo tratamento deverá assegurar que: (i) o tratamento não é incompatível com a finalidade inicial; (ii) há fundamento legal para o tratamento de categoria especial de dados; (iii) garante a informação necessária ao titular de dados; bem como (iv) aplica medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados.

Em outro tópico abordamos a questão das medidas para a salvaguarda dos direitos e liberdades dos titulares. Antes, contudo, analisamos o direito a ser informado e seu conteúdo.

²⁵⁰ “The result produced by the machine, using more and more sophisticated software, and even expert systems, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities” (KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher – **The EU General Data Protection Regulation (GDPR): A commentary**. Oxford: Oxford University Press, 2020, p. 526).

²⁵¹ *Ibid.*, *loc. cit.*

²⁵² UNIÃO EUROPEIA – Regulamento (EU) 2016/679 (General Data Protection Regulation - GDPR). **Jornal Oficial da União Europeia**. L119. (04 maio 2016), p. 1-88.

²⁵³ *Ibid.* Comissão – **Orientações sobre as decisões automatizadas e definições de perfis para efeitos do Regulamento 2016/679**. Grupo de Trabalho do 29.º para Proteção de Dados. Com a última redação revista e adotada em 6 de fevereiro de 2018 [Em linha]. Bruxelas, 27 abr. 2016, p. 16. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>.

2.3 Direitos dos titulares dos dados

2.3.1 Direito a ser informado – alínea f) do n.º 2 do art.º 13.º; alínea g) do n.º 2 do art.º 14.º e alínea h) do n.º 1 do art.º 15.º do RGPD

O direito a ser informado previsto nos artigos 13.º e 14.º do RGPD se refere à obrigação dos responsáveis pelo tratamento de fornecerem informações quanto à existência de decisões automatizadas, incluindo a definição de perfis na hipótese do artigo 22.º, n.º 1 e n.º 4, tanto quando da recolha do dado diretamente do próprio titular (art. 13.º) como quando de terceiros (art. 14.º) e, “pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados”²⁵⁴.

Já o artigo 15.º, que trata do direito de acesso, também carrega em seu preceito o dever de prestação de informações por parte do responsável pelo tratamento e, na alínea h) do n.º 1, assim como nos antecedentes aqui tratados, traz mais uma vez o direito do titular a ser informado, conjuntamente com o exercício de seu direito de acesso, da “existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.ºs 1 e 4, e, “pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados”.

Segundo o GT 29, os responsáveis pelo tratamento devem estar atentos “particularmente nas suas obrigações de transparência”, pois os deveres de informação presentes no artigo 13.º, n.º 2, alínea f), e no artigo 14.º, n.º 2, alínea g), exigem que sejam prestadas informações “específicas e de fácil acesso sobre as decisões automatizadas, com base exclusivamente no tratamento automatizado, incluindo a definição de perfis que produzam efeitos jurídicos ou similarmente significativos”, esclarecendo que “a prestação dessas informações ajudará igualmente os responsáveis pelo tratamento a assegurar que cumprem algumas das garantias necessárias a que se referem o artigo 22.º, n.º 3, e o considerando 71”²⁵⁵. Além disso, mesmo que as decisões automatizadas e definição de perfis não esteja em conformidade com o preceito constante do artigo 22.º, n.º 1, a qualquer tempo

²⁵⁴ “Não obstante os artigos 13.º e 14.º estarem sistematicamente separados, levando em conta as circunstâncias de os dados serem recolhidos diretamente, ou não, junto ao titular, certo é que comungam da mesma *ratio* e dos mesmos fundamentos dogmáticos” (CORDEIRO, António Barreto Menezes (coord.) – **Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019**. Lisboa: Almedina: 2021, p. 168).

²⁵⁵ UNIÃO EUROPEIA. Comissão – **Orientações sobre as decisões automatizadas e definições de perfis para efeitos do Regulamento 2016/679**. Grupo de Trabalho do 29.º para Proteção de Dados. Com a última redação revista e adotada em 6 de fevereiro de 2018 [Em linha]. Bruxelas, 27 abr. 2016, p. 27. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>.

deverão ser facultadas as informações mencionadas para tornar o tratamento equitativo²⁵⁶ e dar cumprimento aos demais requisitos do direito à informação disposto nos artigos 13.º e 14.º²⁵⁷.

As tais “informações úteis sobre a lógica subjacente” não seriam uma explicação complexa sobre os algoritmos utilizados ou mesmo sua divulgação por completo (o que poderia importar em revelação de segredo industrial), mas informações simples sobre a forma como se dá o tratamento de seus critérios, sendo que tais informações ainda devem ser suficientemente completas para que o titular possa compreender os motivos da decisão²⁵⁸.

As expressões *importância* e *consequências previstas* sugerem que devem ser fornecidas informações quanto aos tratamentos já previstos ou futuros e sobre a forma como as decisões totalmente automatizadas poderão afetar os titulares, sinalizando ainda, por meio de exemplos, os possíveis resultados e, se necessário, diante do atual estado da digitalização dos meios de comunicação e contratação, utilizando ferramentas (tais como técnicas visuais) para colaborar com a clareza da informação²⁵⁹.

Os artigos 13.º e 14.º encontram paralelo nos artigos 10.º e 11.º da Directiva 95/46/CE revogada. As atuais disposições demonstram maior preocupação com o princípio da transparência, que pode ser atribuída à evolução tecnológica e precisamente à utilização de decisões automatizadas e definições de perfis pela densificação de um rol mais amplo de deveres de informação. No caso do artigo 14.º também se apresentam algumas regras distintas daquelas que havia na Directiva em relação ao momento da comunicação das informações (n.ºs 3 e 4), bem como o estabelecimento de exceções às regras do direito à informação estabelecidas nos n.ºs 1 a 4. Por óbvio, nesse último caso, assim como das exceções do n.º 5, o ônus da prova do enquadramento legal é do responsável pelo tratamento²⁶⁰.

O direito do titular de dados pessoais a ser informado guarda íntima relação com o princípio da transparência e é, nos preceitos acima referidos, a forma pela qual o legislador do

²⁵⁶ Considerando 60: “responsável pelo tratamento deverá fornecer ao titular as informações adicionais necessárias para assegurar um tratamento equitativo e transparente tendo em conta as circunstâncias e o contexto específicos em que os dados pessoais forem tratados. O titular dos dados deverá também ser informado da definição de perfis e das consequências que daí advêm”.

²⁵⁷ UNIÃO EUROPEIA. Comissão – **Orientações sobre as decisões automatizadas e definições de perfis para efeitos do Regulamento 2016/679**. Grupo de Trabalho do 29.º para Proteção de Dados. Com a última redação revista e adotada em 6 de fevereiro de 2018 [Em linha]. Bruxelas, 27 abr. 2016, p. 28. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>.

²⁵⁸ *Ibid.*, loc. cit.

²⁵⁹ *Ibid.*, p. 29.

²⁶⁰ CORDEIRO, António Barreto Menezes (coord.) – **Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019**. Lisboa: Almedina: 2021, p. 157-159, 166-168, 170.

RGPD lhe deu concretude, demonstrando a grande preocupação em torno das decisões automatizadas e seus potenciais riscos discriminatórios.

Mariana Marques Rielli se refere a um ideal histórico de transparência segundo o qual “ser capaz de ver algo cria oportunidades para ‘controlar’ e ‘mudar’ (daí, *accountability*) tal coisa”. Citando Ananny e Crawford²⁶¹ esclarece que um histórico do ideal de transparência a partir do Iluminismo e sua instrumentalização construída como vigilância, os autores concluiriam que a transparência “não é simplesmente um estado de clareza sobre as coisas, mas sim um sistema que promete algum nível de controle sobre aquilo que é observado”²⁶².

Transpondo esse ideal de vigilância, o qual também foi empreendido pelo legislador do RGPD²⁶³ ao longo de seu texto, ora dando direitos aos titulares de dados, ora estabelecendo deveres aos responsáveis pelo tratamento, parece-nos bastante claro o objetivo de controle que poderá ser exercido pelo titular (autodeterminação informativa), além das pelas autoridades e pelo Judiciário.

A informação ao titular de dados sobre os detalhes do tratamento é uma das condições para o tratamento leal (em atendimento ao princípio da lealdade) e certamente uma condição *sine qua non* para transparência²⁶⁴. Prover os indivíduos com os elementos de informação não só os coloca em posição de exercer efetivamente seus direitos como titulares de dados, mas também contribui para garantir a qualidade dos dados. Já em 1980, o direito de informação sobre a operação de tratamento era considerado o direito “chefe” entre os direitos dos titulares de dados²⁶⁵.

Com a emergência da era das decisões por algoritmos, IA e *machine-learning*, a transparência ganhou ainda mais importância.

Gabriela Zanfir-Fortuna afirma que uma “black box²⁶⁶” abastecida com dados pessoais, mesmo que esses dados sejam apenas parte dos dados de entrada (*inputs*) existentes

²⁶¹ Para estes autores: ANANNY, Mike; CRAWFORD, Kate – Seeing without knowing: limitations of the transparency ideal and its application to algorithmic accountability. **New Media & Society** [Em linha]. (2016), p. 1-17, p. 17. [Consult. 15 jul. 2022]. Disponível em: http://mike.ananny.org/papers/anannyCrawford_seeingWithoutKnowing_2016.pdf.

²⁶² RIELLI, Mariana Marques – Críticas ao ideal de transparência como solução para a opacidade de sistemas algorítmicos. In BARBOSA, Mafalda Miranda (coord.) – **Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa**. Indaiatuba: Foco, 2021. p. 437-446, p. 443.

²⁶³ No considerando 68, o legislador do RGPD também está apontando que o princípio da transparência é “especialmente relevante em situações em que a proliferação de operadores e a complexidade tecnológica das práticas tornam difícil que o titular dos dados saiba e compreenda se, por quem e para que fins os seus dados pessoais estão a ser recolhidos, como no caso da publicidade por via eletrônica”.

²⁶⁴ KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher – **The EU General Data Protection Regulation (GDPR): A commentary**. Oxford: Oxford University Press, 2020, p. 415.

²⁶⁵ *Ibid.*, p. 416.

²⁶⁶ A elaboração teórica do termo coube a PASQUALE, Frank. **The Black Box society: the secret algorithms that control money and information**. Cambridge: Harvard University Press, 2015.

no contexto de uma atividade específica de uma organização e que a saída (*outputs*) da “caixa preta” pode afetar significativamente um indivíduo, é muito importante. Compreensão de como uma “caixa preta” específica interage com os dados de um indivíduo e como esse tratamento pode afetar os direitos e interesses dele, dependendo das variáveis, são igualmente importantes²⁶⁷.

Com a entrada em vigor do RGPD, surgiu um debate acadêmico quanto à existência de um direito do titular de dados de receber uma explicação *ex post* relacionada às decisões algorítmicas e outras formas de decisões automatizadas. Entendemos que, independentemente de como é chamado, se direito à informação ou explicação, esse direito está garantido por um conjunto de disposições do RGPD para assegurar a transparência em relação às operações específicas de tratamento (faz-se aqui remissões específicas ao Artigo 5.º, n.º 1; artigo 12.º; artigo 14.º e 15.º do RGPD)²⁶⁸.

Leticia Canut, que igualmente trata do tema, afirma “que a normativa (do RGPD) exige o direito de explicação dos modelos de aprendizado de máquina”²⁶⁹ da mesma forma, qual seja, recorrendo a diversos dispositivos e considerados do RGPD, os quais, em conjunto e sistematicamente analisados, justificam a afirmação de que haveria sim um direito à explicação no RGPD. Temos, ainda, além da própria autora, Andrew Burt²⁷⁰²⁷¹; Bryce

²⁶⁷ PASQUALE, Frank. **The Black Box society: the secret algorithms that control money and information**. Cambridge: Harvard University Press, 2015.

²⁶⁸ No mesmo sentido: “Irrespective of what it is called, such a right is guaranteed in substance by a web of provisions in the GDPR for ensuring transparency regarding specific processing operations. It is significant to also take into account that providing meaningful transparency about how automated systems work with one’s personal data is at the core of the first data protection laws in Europe. The first French data protection law from 1978 already granted persons ‘the right to know and to challenge the information and the reasoning used by automated processing whose results concern them’. Thus, from the early days of data protection law, automated processes (or ‘the machines’) were met with an expectation that they be transparent and comprehensible in the way they work, well before the internet connected them. Meeting these expectations is all the more critical today. Article 13 GDPR, together with the other provisions that ensure transparency under the Regulation, aim to ensure that these expectations are met” (KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher – **The EU General Data Protection Regulation (GDPR): A commentary**. Oxford: Oxford University Press, 2020, p. 416).

²⁶⁹ CANUT, Leticia – Decisões Automatizadas e o Direito à Explicação no Regulamento Geral de Proteção de Dados da União Europeia. **Revista de Direitos e Garantias Fundamentais** [Em linha]. Vol. 22, n.º 1 (jan./abr. 2021), p. 101-130. [Consult. 16 jul. 2022]. Disponível em: <https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1573>.

²⁷⁰ “All of which is to say that if you’re a privacy professional, you’re going to find it difficult to implement these requirements in practice once the GDPR comes into effect. To that end, below are a few pointers designed to help privacy professionals enable the deployment of machine learning systems while complying with the GDPR: [...] With these answers in hand, you should be able to construct a basic explanation of how the model is working, which can help you to put together a general explanation that satisfies the “logic” and “significance” requirements set forth in Articles 13–15, and place them in the context of the “opt-out” requirements in Articles 21–22”.

²⁷¹ BURT, Andrew – **Is there a 'right to explanation' for machine learning in the GDPR?** [Em linha]. Portsmouth, NH, 01 June 2017. [Consult. 16 jul. 2022]. Disponível em: <https://iapp.org/news/a/is-there-a-right-to-explanation-for-machine-learning-in-the-gdpr/>.

Goodman e Seth Flaxman²⁷²; Andrew Selbst e Julia D. Powles^{273,274}, Ronald Vogl, Ashkon Farhangi e Bryan Casey²⁷⁵. Esses autores, em que pese reconheçam a existência de um direito à explicação, podem eventualmente divergir quanto ao escopo e os limites dessa explicação²⁷⁶, o que é bastante plausível face as características particulares dos diferentes tipos sistemas.

Entre os que defendem inexistir um direito à explicação estão Sandra Wachter, Brent Mittelstadt e Luciano Floridi²⁷⁷; EVE (Eve the Analyst's Adventures in the Data Wonderland)²⁷⁸.

²⁷² GOODMAN, Bryce; FLAXMAN, Seth – European Union Regulations on Algorithmic Decision-Making and a “Right to Explanation”. **AI Magazine** [Em linha]. Vol. 38, n.º 3 (2017), p. 50-57. [Consult. 29 jul. 2020]. Disponível em: <https://doi.org/10.1609/aimag.v38i3.2741>

²⁷³ Para eles o direito à explicação deve ser interpretado funcionalmente, com flexibilidade e deve permitir que o titular exerça seus direitos em conformidade com o RGPD e normas de direitos humanos (SELBST, Andrew D.; POWLES, Julia – Meaningful Information and the Right to Explanation. **International Data Privacy Law** [Em linha]. Vol. 7, n.º 4 (2017), p. 233-242. [Consult. 10 dez. 2019]. Disponível em: <https://academic.oup.com/idpl/article/7/4/233/4762325>).

²⁷⁴ Sustentam ainda que a autoridade do Reino Unido (ICO) também entende que há um direito à explicação nas decisões exclusivamente automatizadas. Em nossa investigação apenas encontramos no sítio da referida autoridade o seguinte ao tratar dos Direitos relacionados a decisões automatizadas e definição de perfis (Rights related to automated decision making including profiling): “What else do we need to consider? [...] You must: [...] provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual; use appropriate mathematical or statistical procedures; ensure that individuals can: obtain human intervention; express their point of view; and obtain an explanation of the decision and challenge it [...]”. Sem uma explicação, como seria possível “desafiar”, questionar a decisão? (ICO. Information Commissioner's Office – **Rights related to automated decision making including profiling** [Em linha]. Wilmslow, Cheshire, 2019. [Consult. 10 dez. 2019]. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/>).

A mesma autoridade (ICO) em seu guia sobre decisões automatizada e definição de perfis, responde à pergunta: “How can we explain complicated processes in a way that people will understand?” e explica que “providing ‘meaningful information about the logic’ and ‘the significance and envisaged consequences’ of a process doesn't mean you have to confuse people with over-complex explanations of algorithms. You should focus on describing: the type of information you collect or use in creating the profile or making the automated decision; why this information is relevant and what the likely impact is going to be/how it's likely to affect them.

²⁷⁵ VOGL, Roland; FARHANGI, Ashkon; CASEY, Bryan. **Rethinking Explainable Machines: The Next Chapter in the GDPR's 'Right to Explanation' Debate**. Oxford, 15 May 2018 [Em linha]. [Consult. 4 dez. 2019]. Disponível em: <https://www.law.ox.ac.uk/business-law-blog/blog/2018/05/rethinking-explainable-machines-next-chapter-gdprs-right-explanation>.

²⁷⁶ “Ao contrário do que tem sido comumente afirmado tanto pela mídia quanto pelo meio acadêmico, o direito à explicação previsto no Regulamento estaria limitado a uma explicação relativa à funcionalidade do sistema, isto é, à lógica geral de seu funcionamento e suas consequências previstas, fornecendo, assim, uma explicação *ex ante* à tomada de decisão. O direito à explicação de decisões específicas, por outro lado, que englobaria as razões e circunstâncias individuais de determinada decisão automatizada, possibilitando também uma explicação *ex post*, não faria parte do escopo de aplicação do Regulamento” (DTIBR. Direito, Tecnologia e Inovação – **GDPR e decisões automatizadas: Limites a um "Direito à explicação"** [Em linha]. Belo Horizonte, MG, 21 nov. 2018. [Consult. 4 dez. 2019]. Disponível em: <https://www.dtibr.com/post/2018/11/21/gdpr-e-decis%C3%B5es-automatizadas-limites-a-um-direito-%C3%A0-explic%C3%A7%C3%A3o>).

²⁷⁷ Defendem que existe apenas um direito limitado a ser informado (WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano – Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law** [Em linha]. Vol. 7, n.º 2 (1 May

Por outro lado, alguns autores, compreendendo o que envolveria o direito à explicação posteriormente à tomada de decisão, que englobaria os motivos e as circunstâncias particulares de que determinada decisão totalmente automatizada não seria, na maioria das vezes, tecnicamente possível, esclarecem que um direito à explicação nos termos defendidos não seria a resposta que aqueles que defendem a transparência e a responsabilidade estariam procurando. Em verdade, a transparência buscada seria uma falácia, pelo que propõem outras possíveis soluções na busca de melhor forma de se garantir que esses algoritmos sejam mais confiáveis, explicáveis e centrados no ser humano.

Lilian Edwards e Michael Veale, nesse passo, defendem que o direito à explicação provavelmente não é o remédio que procuramos. Esclarecem que a ideia de um direito à explicação como vem sendo amplamente defendido vem nutrindo a “falácia da transparência” e argumentam que outros trechos do RGPD, como o direito ao apagamento; o direito à portabilidade, bem como o *privacy by design*, relatórios de impacto, certificações e selos de privacidade podem ser as “sementes” que podem ser usadas para fazer com que os algoritmos sejam mais confiáveis, explicáveis e centrados no ser humano²⁷⁹.

Com efeito, além dos citados, outros autores esclarecem que o clamor por transparência parte da premissa de que o saber, necessariamente, traz compreensão e governança, o que é equivocado²⁸⁰. Ananny e Crawford²⁸¹, aos quais nos referimos anteriormente, propõem uma mudança do foco da transparência, olhando para dentro de um sistema, já que sua compreensão e responsabilização dependem do entendimento de como ele funciona como sistema. Por sua vez, Simon Chesterman chega a propor que, diante da opacidade natural de determinados sistemas, novas formas de explicabilidade poderiam ser

2017), p. 76-99 [Em linha]. [Consult. 4 dez. 2019]. Disponível em: <https://academic.oup.com/idpl/article/7/2/76/3860948>.

²⁷⁸ EVE – **Right to Explanation: a Right that Never Was (in GDPR)**. Málaga, Andaluzia, 1 March 2018 [Em linha] [Consult. 4 dez. 2019]. Disponível em: <https://datawanderings.com/2018/03/01/right-to-explanation/>.

²⁷⁹ EDWARDS, Lilian; VEALE, Michael – Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For. **Duke Law & Technology Review** [Em linha]. Vol. 16, n.º 18 (23 maio 2017), p. 18-84. [Consult. 4 dez. 2019]. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855#.

²⁸⁰ Dentre eles: RIELLI, Mariana Marques – Críticas ao ideal de transparência como solução para a opacidade de sistemas algorítmicos. In BARBOSA, Mafalda Miranda (coord.) – **Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa**. Indaiatuba: Foco, 2021. p. 437-446, p. 445; e MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. – Entre as Leis da Robótica e a ética: Regulação para o Adequado Desenvolvimento da Inteligência Artificial. In BARBOSA, Mafalda Miranda (coord.) – **Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa**. Indaiatuba: Foco, 2021. p. 65-78.

²⁸¹ ANANNY, Mike; CRAWFORD, Kate – Seeing without knowing: limitations of the transparency ideal and its application to algorithmic accountability. **New Media & Society** [Em linha]. (2016), p. 1-17, p. 17. [Consult. 15 jul. 2022]. Disponível em: http://mike.ananny.org/papers/anannyCrawford_seeingWithoutKnowing_2016.pdf.

estudadas ou mesmo dever-se-ia aceitar que determinadas decisões não deveriam ser tomadas por meio de algoritmos²⁸².

O *machine learning* é uma tecnologia que constrói a si própria. São algoritmos que constroem outros algoritmos²⁸³ e, de modo geral, não é fácil mesmo para o técnico no assunto (que dirá para o cidadão leigo) descrever os passos dados por um algoritmo até alcançar um dado resultado, mesmo em termos genéricos. Conclui-se, portanto, que os algoritmos “acrescentam um elemento novo à cadeia de informação – a sua opacidade –, que costuma estar associado à dificuldade de decodificar o seu resultado”²⁸⁴.

Para Caitil Mulholland e Isabella Frajhof, que discorrem sobre como funcionam os robôs e os sistemas de IA, diante da ausência de regulação jurídica específica para lidar com as suas diferentes características; a observação de princípios éticos poderia colaborar com a maximização dos benefícios da IA ao passo que os riscos de sua aplicação diminuiriam. Concluem que, “enquanto não houver uma regulação dos sistemas de Inteligência Artificial – ainda que por meio dos códigos deontológicos –, a indagação a respeito do adequado, seguro e confiável desenvolvimento e aplicação da IA permanecerá”, cabendo então “à sociedade como um todo a árdua tarefa de exigir a implementação de um sistema de regulação apropriado que possibilite não somente o pleno desenvolvimento das tecnologias e sistemas de Inteligência Artificial, mas que beneficiarão a todos e promoverão a tutela da pessoa humana”²⁸⁵.

Nesse sentido são as inúmeras iniciativas no intuito do acolhimento de orientações éticas para a IA, como a do Parlamento Europeu com o Regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas de 20 de outubro de 2020²⁸⁶, texto que, entre outras coisas, enfatiza que a IA deve aplicar a ética “por definição” e desde a “concepção”. Voltaremos ao assunto no Capítulo 3.

²⁸² “The means of addressing some or all of these concerns is routinely said to be through transparency. Yet while proprietary opacity can be dealt with by court order and complex opacity through recourse to experts, naturally opaque systems may require novel forms of ‘explanation’ or an acceptance that some machine-made decisions cannot be explained — or, in the alternative, that some decisions should not be made by machine at all” (CHESTERMAN, Simon – **Through a Glass: Artificial Intelligence and the Problem of Opacity** [Em linha]. (14 Apr. 2020), p. 1-26, p. 8. (NUS Law Working Paper, 011) [Consult. 15 jul. 2022]. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3575534)

²⁸³ DOMINGOS, Pedro – **Algoritmo Mestre**. São Paulo: Novatec, 2017, p. 16.

²⁸⁴ DONEDA, Danilo; ALMEIDA, Virgílio Augusto Fernandes – O que é a governança de algoritmos? **Tecnopolíticas da Vigilância: perspectivas da margem**. São Paulo: Boitempo, 2018, p. 142-143.

²⁸⁵ MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. – Entre as Leis da Robótica e a ética: Regulação para o Adequado Desenvolvimento da Inteligência Artificial. In BARBOSA, Mafalda Miranda (coord.) – **Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa**. Indaiatuba: Foco, 2021. p. 65-78.

²⁸⁶ UNIÃO EUROPEIA. Parlamento – **Regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas**. Estrasburgo, 20 out. 2020 [Em linha]. [Consult. 15 jul. 2022]. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_PT.html.

2.4 Das disposições específicas do artigo 22.º do RGPD relativas às decisões automatizadas

2.4.1 Da decisão tomada exclusivamente com base no tratamento automatizado

O artigo 22.º tem campo de aplicação bem delimitado, uma vez que visa delimitar os termos em que se darão: (i) as decisões, (ii) por meio de tratamento exclusivamente automatizado e (iii) que afetem os interesses dos titulares de dados ou produzam afetos na sua esfera jurídica. Como regra geral, esse dispositivo garante o direito de os titulares de dados não estarem submetidos a decisões, incluindo a definição de perfis, por tratamento unicamente automatizado. Cabe, então, a análise dos seus três elementos de identificação.

Como visto, a decisão pode ser conceituada como “um ato, numa aceção não jurídica, que incida sobre um caso concreto e produza efeitos jurídicos relativamente a um ou mais titulares de dados específicos, quer seja a aceitação ou a recusa de um pedido, a sua caracterização, catalogação, atribuição de uma classificação, definição de perfil ou qualquer outra medida análoga produtora de um efetivo resultado”²⁸⁷.

Para efeitos do RGPD, as decisões devem dizer respeito a um ou mais titulares de dados, pelo que não será atingido pela normativa do Regulamento as decisões abstratas e genéricas, ou que digam respeito a estratégias e segredos empresariais sem afetação da esfera jurídica dos titulares de dados. As decisões poderão emanar de pessoas singulares ou coletivas, do setor público ou privado.

A definição de perfil está conceituada no artigo 4.º, n.º 4 do RGPD como sendo o tratamento automatizado de dados pessoais com o propósito de avaliar ou prever certos aspectos dos titulares. Por essa definição, não basta a mera organização dos dados para que o tratamento seja considerado uma definição de perfil. De haver, necessariamente, a intenção de avaliar e prever determinadas características dos titulares de dados.

Por decisão exclusivamente automatizada, entende-se a decisão que é produzida sem qualquer interferência humana. O critério é material e não formal, de modo que a previsão do artigo 22.º se verificará sempre que a intervenção humana se der de forma meramente burocrática, para fins de confirmação da decisão automatizada, intervenção esta despida de

²⁸⁷ CORDEIRO, António Barreto Menezes – Decisões Automatizadas à Luz do RGPD e da LGPD. **Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa**. Indaiatuba: Foco, 2021. p. 263-270, p. 266-267.

crítica. Nos casos em que o agente opte por não proceder à reavaliação em concreto, muito embora até possa fazê-lo, são subsumíveis ao preceito²⁸⁸.

Segundo o GT 29, o termo *direito* constante do preceito não significa que o artigo 22.º, n.º 1, possa ser aplicado somente quando invocado pelo titular. Ao contrário, ele prevê uma proibição geral de tomada de decisões com base exclusivamente em tratamento automatizado e que produza efeitos em sua esfera jurídica.

2.4.2 Efeitos na esfera jurídica do titular dos dados

O preceito também não se aplica a todas as decisões automatizadas, mas apenas àquelas que produzam efeitos na esfera jurídica do titular ou que os afete significativamente de forma similar. Muito embora RGPD não defina os conceitos de “esfera jurídica”, “significativamente de forma similar” o preceito abrange apenas efeitos com impactos graves na esfera jurídica do titular de dados²⁸⁹.

Por decisão que produz efeitos jurídicos entende-se aquelas que afetem direitos legais do indivíduo, como sua liberdade de escolha, por exemplo, ou quando a decisão automatizada produza efeitos em direitos que possua no âmbito de um contrato²⁹⁰.

Por decisão que afete significativamente de forma similar, muito embora Menezes Cordeiro entenda que não vê “que decisões possam afetar significativamente de forma similar os titulares de dados, mas que não produzam efeitos na sua esfera jurídica ou que vedam a sua produção”²⁹¹, o GT 29 entende, ao contrário, que um mesmo processo e tomada de decisão poderia não ter efeitos “nos direitos legais das pessoas” e poderia ser abrangido pelo preceito se “produzir efeitos equivalentes ou similarmente significativos no seu impacto”²⁹². Em sua orientação, o Grupo ainda elenca uma série de exemplos de decisões unicamente

²⁸⁸ CORDEIRO, António Barreto Menezes – Decisões Automatizadas à Luz do RGPD e da LGPD. **Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa**. Indaiatuba: Foco, 2021. p. 263-270, p. 266-267.

²⁸⁹ UNIÃO EUROPEIA. Comissão – **Orientações sobre as decisões automatizadas e definições de perfis para efeitos do Regulamento 2016/679**. Grupo de Trabalho do 29.º para Proteção de Dados. Com a última redação revista e adotada em 6 de fevereiro de 2018 [Em linha]. Bruxelas, 27 abr. 2016, p. 23-24. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>.

²⁹⁰ *Ibid.*, *loc. cit.*

²⁹¹ CORDEIRO, António Barreto Menezes, *op. cit.*, p. 267.

²⁹² “Mesmo quando um processo de tomada de decisão não tenha efeitos nos direitos legais das pessoas, pode, ainda assim, ser abrangido no âmbito de aplicação do artigo 22.º, se produzir efeitos equivalentes ou similarmente significativos no seu impacto. Por outras palavras, mesmo nos casos em que não há alterações nos seus direitos ou obrigações legais, o titular dos dados pode, contudo, sofrer um impacto suficiente para solicitar as proteções garantidas pela disposição em análise. O RGPD introduz o termo «de forma similar» (que não existia no artigo 15.º da Diretiva 95/46/CE) junto da expressão «afete significativamente». Por conseguinte, o limiar de *importância* deve ser similar ao da decisão que produz efeitos jurídicos” (UNIÃO EUROPEIA. Comissão, *op. cit.*, *loc. cit.*).

automatizadas cujos efeitos são considerados relevantes o suficiente para subsunção ao preceito²⁹³.

2.4.3 Exceções à proibição

O artigo 22.º, n.º 1, estabelece uma proibição geral²⁹⁴²⁹⁵ de tratamento por meio de decisões unicamente automatizadas, com efeitos jurídicos ou similarmente significativos, que afetem os titulares de dados. As exceções à proibição estão elencadas no n.º 2.º, quais sejam, (a) quando necessária para a execução ou a celebração de um contrato; (b) quando autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou (c) quando fundada no consentimento explícito do titular dos dados.

Importante lembrar que sempre que a tomada de decisão disser respeito às categorias especiais de dados (artigo 9.º, n.º 1), o responsável deverá assegurar o cumprimento dos requisitos previsto no artigo 22.º, n.º 4, bem como, nos casos das letras a) e c) do n.º 2, o responsável pelo tratamento também deverá garantir o cumprimento dos requisitos do artigo 22.º, n.º 3.

2.4.3.1 Execução de um contrato

Eventualmente as decisões automatizadas poderão ser utilizadas para celebração e/ou execução de contratos.

Essa primeira exceção é corolário lógico do direito à autodeterminação informativa, uma vez que o recurso a uma decisão exclusivamente automatizada seria consequência de uma tomada de decisão livre e consciente do titular de dados em contratar com o responsável pelo tratamento.²⁹⁶

²⁹³ “[...] decisões que afetem a situação financeira de uma pessoa, designadamente a sua elegibilidade para obtenção de crédito; decisões que afetem o acesso de uma pessoa aos serviços de saúde; decisões que impeçam o acesso de uma pessoa a uma oportunidade de emprego ou a coloquem em séria desvantagem; decisões que afetem o acesso de uma pessoa à educação, como, por exemplo, o ingresso em estabelecimentos de ensino superior”.

²⁹⁴ Haveria um dissenso em relação ao artigo 22.º, n.º 1 ser um direito a ser exercido pelo Titular ou uma proibição geral ao tratamento. *Vide*: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher – **The EU General Data Protection Regulation (GDPR): A commentary**. Oxford: Oxford University Press, 2020, p. 530-531.

²⁹⁵ Entendendo há uma proibição genérica ao tratamento exclusivamente automatizado (CORDEIRO, António Barreto Menezes (coord.) – **Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019**. Lisboa: Almedina: 2021, p. 222-223).

²⁹⁶ *Id.* – Decisões Automatizadas à Luz do RGPD e da LGPD. **Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa**. Indaiatuba: Foco, 2021. p. 263-270, p. 268.

Nesses casos, o responsável pelo tratamento deverá ser capaz de demonstrar que o tratamento em questão é necessário e que não haveria método menos intrusivo da privacidade dos titulares. Em havendo outro método que seja menos lesivo aos direitos de privacidade dos titulares, o tratamento não seria necessário, descabendo a subsunção da hipótese à exceção constante da letra a), do n.º 2, do artigo 22.º, do RGPD²⁹⁷.

Sempre que a execução do contrato ou conclusão/disponibilização da oferta pressupuser uma decisão automatizada, ela será considerada necessária²⁹⁸.

Por fim, em conformidade com o n.º 3 do artigo 22.º, “responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão”²⁹⁹.

2.4.3.2 Autorizada pelo Direito da União ou do Estado-Membro

De acordo com a letra b) do n.º 2 do artigo 22.º, as decisões totalmente automatizadas, incluindo a definição de perfis, poderão ser autorizadas se o direito da União ou de Estado-Membro a que o titular estiver sujeito autorizar sua utilização, pelo que, nessa hipótese, o responsável pelo tratamento também deverá, igualmente, demonstrar que adotou as medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses dos titulares de dados.

O GT 29, em suas Orientações sobre decisões automatizadas e definições de perfis, esclarece que o considerando 71 poderia incluir as decisões automatizadas para prevenção de fraudes e evasão fiscal ou para garantir a segurança e fiabilidade do responsável pelo tratamento, no caso, a própria União ou Estado-Membro³⁰⁰.

²⁹⁷ UNIÃO EUROPEIA. Comissão – **Orientações sobre as decisões automatizadas e definições de perfis para efeitos do Regulamento 2016/679**. Grupo de Trabalho do 29.º para Proteção de Dados. Com a última redação revista e adotada em 6 de fevereiro de 2018 [Em linha]. Bruxelas, 27 abr. 2016, p. 25-26. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>.

²⁹⁸ CORDEIRO, António Barreto Menezes – Decisões Automatizadas à Luz do RGPD e da LGPD. **Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa**. Indaiatuba: Foco, 2021. p. 263-270, p. 268.

²⁹⁹ UNIÃO EUROPEIA – Regulamento (EU) 2016/679 (General Data Protection Regulation - GDPR). **Jornal Oficial da União Europeia**. L119. (04 maio 2016), p. 1-88.

³⁰⁰ UNIÃO EUROPEIA. Comissão, *op. cit.*, p. 26.

2.4.3.3 Consentimento explícito

A terceira exceção é o consentimento do titular que deve ser explícito³⁰¹, e não “expresso”, como consta do artigo 7.º, o qual se entende, de acordo com o artigo 4.º, n.º 11, “uma manifestação de vontade, livre, específica, informada e inequívoca, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento”.

Também no caso do consentimento explícito, o responsável pelo tratamento, a teor do n.º 3 do artigo 22.º, deverá comprovar que adotou as “medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão”.

2.4.4 Garantias adequadas

O estabelecimento de garantias adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados pelo responsável pelo tratamento é exigido em todas as exceções previstas no n.º 2 do artigo 22.º do RGPD. Essas medidas referidas devem incluir, no mínimo, um meio pelo qual o titular possa obter a intervenção humana, manifestar seu ponto de vista e contestar a decisão³⁰².

O titular dos dados sempre terá o direito de exigir a revisão humana de uma decisão totalmente automatizada, exceto quando a decisão estiver em conformidade com a lei (n.º 2, letra b)). A intervenção humana nesses casos poderá ocorrer, no entanto, se for adotada como uma das “garantias adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados”. Além disso, “qualquer revisão tem de ser levada a cabo por alguém com a devida autoridade e competência para alterar a decisão. O revisor deve realizar uma avaliação exaustiva de todos os dados pertinentes, incluindo quaisquer informações adicionais transmitidas pelo titular dos dados”³⁰³.

³⁰¹ Para os requisitos do consentimento explícito: UNIÃO EUROPEIA. Comitê para Proteção de Dados – **Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679**. Bruxelas, 4 maio 2020 [Em linha]. [Consult. 15 jul. 2020]. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf.

³⁰² *Id.* Comissão – **Orientações sobre as decisões automatizadas e definições de perfis para efeitos do Regulamento 2016/679**. Grupo de Trabalho do 29.º para Proteção de Dados. Com a última redação revista e adotada em 6 de fevereiro de 2018 [Em linha]. Bruxelas, 27 abr. 2016, p. 26. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>.

³⁰³ KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher – **The EU General Data Protection Regulation (GDPR): A commentary**. Oxford: Oxford University Press, 2020, p. 538.

O elenco de direitos mencionados no artigo 22.º, n.º 3, não é exaustivo. Contudo, ainda se discute quais outros interesses estariam aí incluídos. Em especial, como anteriormente mencionado, a doutrina diverge sobre se o artigo 22.º contempla um direito dos titulares dos dados à explicação *ex post* das decisões automatizadas que os afetam. Esse debate se estende a várias outras disposições do RGPD (artigos 13.º, n.º 2, f) e 14.º, n.º 2, g) e 15.º, n.º 1, h). Para muitos, o considerando 71 traria a menção expressa a este direito “em qualquer dos casos”³⁰⁴, mas isso não o torna por si só um direito, já que desprovido de exigibilidade.

Nota-se, mais uma vez, a necessidade de transparência, uma vez que, somente se garantida, poderá o titular exercer seu direito de contestação da decisão e de manifestar seu ponto de vista. Se não houver um conjunto de informações suficientemente claras para o exercício desses direitos, eles estarão obstaculizados e, assim, violado estará o preceito.

No mais, parece-nos que caberá ao responsável colocar à disposição do titular de dados uma ou mais formas de exercício dos seus direitos. Sem isso, as disposições do RGPD estarão violadas.

³⁰⁴ Considerando 71: “Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão. [...] A fim de assegurar um tratamento equitativo e transparente no que diz respeito ao titular dos dados, tendo em conta a especificidade das circunstâncias e do contexto em que os dados pessoais são tratados, o responsável pelo tratamento deverá utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos”.

3 INTELIGÊNCIA ARTIFICIAL E DIREITO: DEMARCAÇÃO DE FRONTEIRAS NA TRANSPOSIÇÃO DE CARACTERÍSTICAS DA INTELIGÊNCIA HUMANA PARA PROCESSOS AUTOMATIZADOS

3.1 Inteligência artificial – Sistemas de inteligência artificial: distinção de figuras afins: *machine learning* e *deep learning*

Existem duas acepções da palavra *Inteligência Artificial (IA)*. A primeira é a IA geral (*general artificial intelligence*), cujo conceito está contaminado pelo senso comum e pela ficção científica, sendo aquela que gostaríamos que existisse e que é fruto de nossa imaginação, mas que ainda não alcançamos; e a segunda, a IA em sentido estrito (*narrow artificial intelligence*), que são os programas de computação (*softwares*) em atuação no mundo virtual, que visam produzir previsões com base em grandes volumes de dados, como por exemplo, assistentes de voz, programas de organização e análise de imagens, motores de busca, ou que possam ser integrados a dispositivos físicos, tais como os carros autônomos, aplicações de internet das coisas e veículos aéreos não tripulados³⁰⁵.

A Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comitê Econômico e Social Europeu e ao Comitê das Regiões: Inteligência Artificial para Europa, esclarece que “o conceito de inteligência artificial (IA) aplica-se a sistemas que apresentam um comportamento inteligente, analisando o seu ambiente e tomando medidas — com um determinado nível de autonomia — para atingir objetivos específicos”³⁰⁶. O texto fala com entusiasmo sobre a IA capaz de transformar o mundo assim como ocorreu com a máquina a vapor e a eletricidade e alerta para a necessidade do cuidado no tratamento da IA em um quadro europeu sólido, com atuação coordenada para que a UE possa “liderar o caminho no desenvolvimento e utilização da IA para o bem comum, tendo por base os seus valores e pontos fortes”, entre os quais destaca o RGPD, que entraria em vigor um mês depois.

Entre os objetivos para a IA na UE, a comunicação destaca: (i) o reforço da capacidade tecnológica e industrial da União Europeia e a aceitação da IA em todos os setores

³⁰⁵ BROUSSARD, Meredith – **Artificial Unintelligence: How computers Misunderstand the World**. Cambridge, MA: The MIT Press, 2018. A autora, que é desenvolvedora de software e jornalista, critica o entusiasmo geral pelas novas tecnologias e lembra que nem sempre se cobra delas a eficiência que deveriam ter. Além disso, ela alerta para o fato de que existem limites fundamentais para o que poderíamos (e deveríamos) fazer com a tecnologia.

³⁰⁶ UNIÃO EUROPEIA. Comissão – **Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comitê Econômico e Social Europeu e ao Comitê das regiões** [Em linha]. Bruxelas, 25 abr. 2018 [Consult. 09 Apr. 2020]. Disponível em: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/PT/COM-2018-237-F1-PT-MAIN-PART-1.PDF>.

da economia, tanto no setor privado quanto público; (ii) preparar as mudanças socioeconômicas decorrentes; (iii) garantir um quadro ético e jurídico apropriado, baseado nos valores da União Europeia e com a Carta de Direitos Fundamentais da União Europeia.

Por sua vez, o *Livro Branco sobre Inteligência Artificial* resume o conceito de IA a “um conjunto de tecnologias que combinam dados, algoritmos e capacidade computacional”³⁰⁷, e a Hewlett Packard Enterprise “se refere amplamente a qualquer comportamento semelhante ao do humano apresentado por uma máquina ou sistema. Na forma mais básica da IA, os computadores são programados para ‘imitar’ o comportamento humano usando dados extensivos de exemplos anteriores de comportamento similar. Eles podem variar desde reconhecer diferenças entre um gato e um pássaro até realizar atividades complexas em uma fábrica”³⁰⁸.

Caitlin Mulholland e Isabella Frajhof alertam que, apesar de uma forte associação à inteligência humana, os processos cognitivos de artefatos humanos e não humanos são bastante diferentes do ponto de vista da apreensão do conhecimento. Numa concepção genérica, a IA se sustentaria na ideia de que essas máquinas são criadas para alcançar determinados objetivos, que, por sua vez, são atendidos por meio de algumas características desses sistemas inteligentes, tais como percepção, aprendizado e autonomia. Esses mecanismos possuem sensores que captam informações sobre o ambiente no qual se encontram e vão somando dados àqueles já inseridos inicialmente neles. Assim, o conhecimento vai se desenvolvendo e sendo acrescido de novos dados, que vão construindo autonomia tal qual previam seus criadores. Para avaliação da taxa de sucesso de seu comportamento, são estabelecidas métricas. Assim, esses sistemas interagem com o ambiente, adquirem conhecimento e agem de acordo com a finalidade para a qual foram construídos³⁰⁹.

Para evitar mal-entendidos quanto à definição de IA, o Grupo de Peritos de Alto Nível pretendeu esclarecer alguns aspectos em torno do conceito, o que resultou na Comunicação da Comissão da EU de abril de 2019. O documento propõem uma definição atualizada do IA, que coincide com a definição citada acima, a qual pode ser assim traduzida: “os sistemas de

³⁰⁷ UNIÃO EUROPEIA. Comissão – **Livro Branco sobre Inteligência Artificial: Uma abordagem europeia virada para a excelência e confiança** [Em linha]. Bruxelas, 19 fev. 2020. [Consult. 10 jul. 2022]. Disponível em: <https://op.europa.eu/pt/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1>.

³⁰⁸ Extraído do glossário eletrônico corporativo da HPE que contém as principais definições sobre IA, para a compreensão de não técnicos (HPE. Hewlett Packard Enterprise – **Inteligência artificial** [Em linha]. Houston, TE, 2022. [Consult. 8 ago. 2022]. Disponível em: <https://www.hpe.com/br/pt/what-is/artificial-intelligence.html>).

³⁰⁹ MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. – Entre as Leis da Robótica e a ética: Regulação para o Adequado Desenvolvimento da Inteligência Artificial. In BARBOSA, Mafalda Miranda (coord.) – **Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa**. Indaiatuba: Foco, 2021. p. 65-78, p. 68.

inteligência artificial (IA) são sistemas de software (e possivelmente também de hardware) projetados por humanos que, uma vez dado um objetivo complexo, atuam na dimensão física ou digital percebendo seu ambiente através de dados aquisição, interpretando os dados estruturados ou não estruturados coletados, raciocinando sobre o conhecimento ou processando as informações, derivadas desses dados e decidir a(s) melhor(es) ação(ões) a serem tomadas para atingir o objetivo determinado. Sistemas de IA podem usar regras simbólicas ou aprender um modelo numérico, e também podem adaptar seu comportamento analisando como o ambiente é afetado por suas ações anteriores”³¹⁰.

Além disso, o documento esclarece que a IA pode ter várias abordagens técnicas e que podem ser separadas em dois grupos, os quais se referem à capacidade (i) de raciocínio, donde se inclui o raciocínio de máquina, que envolve planejamento, programação, representação e raciocínio do conhecimento, busca e otimização; e (ii) de aprendizagem, donde se inclui o aprendizado de máquina (*machine learning*), das quais o aprendizado e o aprendizado por reforço são exemplos específicos. A robótica, que inclui controle, percepção, sensores e atuadores, bem como a integração de todas as outras técnicas em sistemas ciber-físicos, seria outra disciplina, também muito relevante³¹¹.

No grupo de técnicas de aprendizado se incluem, além do aprendizado de máquina (*machine learning*), redes neurais, aprendizado profundo (*deep learning*), árvores de decisão e muitas outras técnicas de aprendizagem. Essas técnicas permitem que um sistema de IA aprenda a resolver problemas que não podem ser especificados com precisão ou cujo método de solução não pode ser descrito por regras de raciocínio simbólico. Exemplos de tais problemas são aqueles que têm a ver com capacidades de percepção, como compreensão de fala e linguagem, bem como visão computacional ou previsão de comportamento. Tais problemas podem parecer fáceis para o ser humano, mas são bastante complexos para sistemas de IA, uma vez que não podem contar com o auxílio dos sentidos (ou pelo menos, ainda não) próprios dos seres humanos, sendo particularmente difícil quando o sistema precisa interpretar dados não estruturados. É nesse contexto que as técnicas de aprendizagem se fazem úteis e ganham valor. As técnicas de aprendizado de máquina produzem um modelo

³¹⁰ EUROPEAN UNION. Commission – **A definition of Artificial Intelligence: main capabilities and scientific disciplines** [Em linha]. Brussels, 8 Apr. 2019, p. 6. [Consult. 10 jul. 2022]. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>.

³¹¹ *Ibid.*, p. 3.

(ou seja, uma fórmula matemática – algoritmo) usado para calcular a decisão a partir dos dados³¹².

A máquina é programada para reconhecer padrões que não seriam perceptíveis a olhos humanos a partir de um conjunto de dados (*inputs*), e, com o treinamento, a máquina é apresentada a um outro conjunto de dados que não foram analisados anteriormente por ela, para que sejam identificados padrões e, com base neles, gerar modelos que são usados para predição a respeito dos dados tratados (*outputs*). O aprendizado vai evoluindo, se aperfeiçoando por meio de *feedbacks* e técnicas estatísticas, fazendo com que seu algoritmo vá se adaptando e se aperfeiçoando^{313,314}.

Por sua vez, os sistemas de *machine learning* podem ser divididos em dois grupos: supervisionados e não supervisionados³¹⁵. O primeiro grupo, do *machine learning* supervisionado, é aquele no qual “os critérios de correlações iniciais são parametrizados (ou ensinados) por seres humanos. Em ambientes dinâmicos, são necessárias várias interações iniciais de treinamento e calibragem do sistema por um humano com domínio na área específica até que o sistema consiga resultados satisfatórios. O *machine learning* não supervisionado dispensa esse treinamento e calibragem inicial por humanos, o que é alcançado por meio do desenvolvimento de novas tecnologias, como as redes neuronais, o *deep learning*³¹⁶, que são capazes de criar padrões de correlações próprios, alheios ao

³¹² EUROPEAN UNION. Commission – **A definition of Artificial Intelligence: main capabilities and scientific disciplines** [Em linha]. Brussels, 8 Apr. 2019, p. 3. [Consult. 10 jul. 2022]. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>.

³¹³ MULHOLLAND, Caitlin – Responsabilidade civil e processos decisórios autônomos em sistemas de Inteligência Artificial (IA): autonomia, imputabilidade e responsabilidade. In MULHOLLAND, Caitlin; FRAZÃO, Ana (coord.) – **Inteligência Artificial e Direito: ética, regulação e responsabilidade**. São Paulo: Thompson Reuters Brasil, 2019. p. 327-348, p. 329.

³¹⁴ O glossário eletrônico corporativo da HPE define que “machine learning é o processo pelo qual os computadores desenvolvem o reconhecimento de padrões ou a capacidade de aprender continuamente ou fazer previsões com base em dados, e podem fazer ajustes sem serem especificamente programados para isso. Uma forma de inteligência artificial, o machine learning automatiza com eficiência o processo de construção de modelos analíticos e permite que as máquinas se adaptem a novos cenários de forma independente. As quatro etapas de construção de um modelo de machine learning são: 1. Selecionar e preparar um conjunto de dados de treinamento necessário para resolver o problema. Esses dados podem ser rotulados ou não rotulados; 2. Escolher um algoritmo a ser executado nos dados de treinamento. Se os dados forem rotulados, o algoritmo pode ser baseado em regressão, árvores de decisão ou instâncias. Se os dados não forem rotulados, o algoritmo pode ser um algoritmo de cluster, um algoritmo de associação ou uma rede neural; 3. Treinar o algoritmo para criar o modelo. 4. Use e melhore o modelo” (HPE. Hewlett Packard Enterprise – **Inteligência artificial** [Em linha]. Houston, TE, 2022. [Consult. 8 ago. 2022]. Disponível em: <https://www.hpe.com/br/pt/what-is/artificial-intelligence.html>).

³¹⁵ “Existem três métodos de machine learning: o aprendizado “supervisionado” trabalha com dados rotulados e requer menos treinamento. O aprendizado “não supervisionado” é usado para classificar dados não rotulados identificando padrões e relações. O aprendizado “semisupervisionado” usa um pequeno conjunto de dados rotulados para guiar a classificação de um conjunto de dados não rotulados maior” (*ibid.*).

³¹⁶ “There are several kinds of neural networks and machine learning approaches, of which currently one of the most successful one is deep learning. This approach refers to the fact that the neural network has several

raciocínio humano”^{317,318}. Isso é possível porque possuem múltiplas unidades (linhas ou níveis) de redes não lineares de processamento dados que se retroalimentam de modo a mimetizar o comportamento humano, sendo esses sistemas capazes de analisar um ambiente dinâmico e extrair correlações e padrões por si sós³¹⁹.

Nesse cenário, é possível perceber que são muitas formas e tipos de aplicação de IA, assim como muitas são as formas de criá-las e treiná-las e também inúmeras as possibilidades de aplicações. Também é preciso que se diga que nem toda IA é um robô e que nem todo robô tem um corpo físico, como na ficção ou imagem idealizada pela maioria das pessoas. Nosso dia a dia possui inúmeros exemplos de aplicações de IA. Assistentes virtuais³²⁰, sistemas de atendimento ao cliente³²¹, *e-mail*³²², redes sociais³²³, serviços de *streaming*³²⁴, *games*³²⁵,

layers between the input and the output that allow to learn the overall input-output relation in successive steps. This makes the overall approach more accurate and with less need of human guidance. Neural networks are just one machine learning tool, but there are many others, with different properties: random forests & boosted trees, clustering methods, matrix factorization, etc.” (EUROPEAN UNION. Commission – **A definition of Artificial Intelligence: main capabilities and scientific disciplines** [Em linha]. Brussels, 8 Apr. 2019, p. 4. [Consult. 10 jul. 2022]. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>).

³¹⁷ GUTIERREZ, Andriei – É possível confiar em um sistema de Inteligência Artificial? Práticas em torno da melhoria de sua confiança, segurança, evidências de accountability. In MULHOLLAND, Caitlin; FRAZÃO, Ana (coord.) – **Inteligência Artificial e Direito: ética, regulação e responsabilidade**. São Paulo: Thompson Reuters Brasil, 2019. p. 83-97, p. 86.

³¹⁸ O glossário eletrônico corporativo da HPE define que “o deep learning é um subconjunto do machine learning que demonstrou ter desempenho significativamente superior ao de alguns métodos tradicionais de machine learning. O deep learning utiliza uma combinação de redes neurais artificiais de várias camadas e treinamentos com uso intenso de dados e de computação, inspirados na mais recente compreensão do comportamento do cérebro humano. Essa abordagem tornou-se tão eficaz que até começou a ultrapassar as habilidades humanas em várias áreas, como reconhecimento de imagem e voz e processamento de linguagem natural. Os modelos de deep learning processam grandes quantidades de dados e são geralmente não supervisionados ou semisupervisionados” (HPE. Hewlett Packard Enterprise – **Inteligência artificial** [Em linha]. Houston, TE, 2022. [Consult. 8 ago. 2022]. Disponível em: <https://www.hpe.com/br/pt/what-is/artificial-intelligence.html>).

³¹⁹ *Ibid.*

³²⁰ Siri (Apple), Cortana (Windows), Google Assistente (Google) e Alexa (Amazon).

³²¹ “Os chatbots são um ótimo exemplo de robô sem corpo físico. Eles simulam um ser humano na conversação por chat e são uma excelente ferramenta de atendimento, pois possibilitam que todo e qualquer usuário seja atendido de imediato, resolvendo ou direcionando para o setor responsável. Isso agiliza o processo e otimiza o tempo dos colaboradores” (D’ARC, Tânia – O que é inteligência artificial: 16 exemplos no seu dia a dia. **Smart Hint** [Em linha]. Curitiba, PR, 25 mar. 2022. [Consult. 8 ago. 2022]. Disponível em: <https://www.smarthint.co/o-que-e-inteligencia-artificial-exemplos/>).

³²² As caixas de e-mail utilizam IA para identificar mensagens de spam e evitam que sua caixa de entrada fique lotada e que eventualmente você receba mensagens maliciosas (*phishing*) ou vírus.

³²³ As redes sociais são inundadas por mecanismos perfilação (definição de perfis ou *profiling*) o que se dá por sistemas de IA, que monitoram seu comportamento de navegação em tempo real, curtidas (“likes”) sendo possível até a compreensão do estado emocional dos usuários a partir de postagem, com destaque para conteúdos de imagens. Algumas das mais famosas redes sociais também usam sistemas de IA para detecção de *fake news* e postagens racistas ou impróprias, por exemplo.

³²⁴ Exemplos mais comuns são o Netflix, Amazon Prime e Spotify. Eles utilizam sistemas de IA para definição do perfil do usuário e sugestão de séries, filmes e músicas.

³²⁵ Alguns recursos nos games são possíveis pela utilização de IA, como a realidade virtual, tornando-os mais reais.

bancos³²⁶, motores de busca³²⁷, comércio eletrônico³²⁸, segurança digital³²⁹, recursos humanos³³⁰, aplicativos de GPS³³¹, transporte³³², indústria³³³, medicina³³⁴ e agricultura³³⁵.

Em todas essas aplicações da IA vemos que o que potencializou sua expansão e desenvolvimento foi a imensa disponibilidade de dados e as novas formas de automação impulsionadas pelo desenvolvimento tecnológico e capacidade de seu processamento³³⁶.

Nesse passo, “os algoritmos tomam (ou contribuem para a tomada de) decisões cujos efeitos, positivos ou negativos, recaem sobre indivíduos que não detêm o conhecimento ou as

³²⁶ Costumam usar IA para otimizar processos. Também utilizam assistentes virtuais e *chatbox* para atendimento remoto a clientes. Outro exemplo são as *fintechs* que vêm explorando a utilização de sistemas de IA em seus robôs consultores (*robots advisors*).

³²⁷ “O Google é um dos maiores exemplos de uso da inteligência artificial no dia a dia. A empresa global já usa essa tecnologia há um bom tempo e em quase todos os produtos e serviços que oferece. Está presente no funcionamento de e-mails — como é o caso citado no exemplo 3 —; em aplicativos, como o Google Lens, que faz buscas por reconhecimento de imagem; Google Maps; e até softwares criados pela empresa e voltados para outros setores, como o da medicina. Mas merecem destaque o Google Ads e o buscador, que é o mais utilizado no mundo todo e que, através do aprendizado da inteligência, tem evoluído e trazido resultados de pesquisa cada vez mais assertivos. Essa tecnologia permite que os resultados de busca apareçam cada vez com mais velocidade e que a ferramenta reconheça sinônimos, assuntos relacionados, semelhança entre sons das letras, entre outras coisas. E quanto mais as pessoas o utilizam, mais ele aprende sobre a intenção de busca e sobre o comportamento, gerando uma melhor experiência para os usuários. Já no caso do Google Ads, a inteligência artificial está focada principalmente nas análises de navegação, utilizando essas informações para recomendação de anúncios personalizados e, por isso, mais assertivos” (D’ARC, Tânia – O que é inteligência artificial: 16 exemplos no seu dia a dia. **Smart Hint** [Em linha]. Curitiba, PR, 25 mar. 2022. [Consult. 8 ago. 2022]. Disponível em: <https://www.smarthint.co/o-que-e-inteligencia-artificial-exemplos/>).

³²⁸ Sistemas de IA são utilizados para melhorar a experiência de compra, desde a seleção de sugestões de compra, menores preços ou produtos mais vendidos numa seção específica.

³²⁹ IA é utilizada em softwares e segurança, impedindo invasões e detectando riscos aos dados de usuários como em alguns aplicativos de pagamentos online.

³³⁰ No setor de recursos humanos já se faz seleção de currículos, coleta de dados e definição de perfis. Também são frequentemente utilizados sistemas de IA para controle de frequência e uso de dados biométricos.

³³¹ Sistemas e IA são utilizados em aplicativos de deslocamento e acompanhamento do trânsito em tempo real. Eles identificam bloqueios policiais, acidentes e interdições no caminho do trajeto selecionado pelo usuário, sugerindo alternativas.

³³² Em relação ao transporte o exemplo mais relevante são os veículos autônomos, tripulados ou não, que se deslocam, identificam obstáculos e respeitam a sinalização. Além disso, também está presente no rastreamento do transporte público e na logística de entregas.

³³³ A IA está presente na automação de tarefas repetitivas e na conferência de produtos, por exemplo.

³³⁴ A IA está presente em tratamentos médicos, análises clínicas, e o próprio Google desenvolveu um software para detecção de câncer de mama e pulmão (*ibid.*).

³³⁵ Na agricultura a utilização de IA vão desde a análise e seleção de sementes, tratores e lançadores de defensivos agrícolas, até no monitoramento do clima, saúde das plantações e qualidade do solo.

³³⁶ Nesse sentido: “Em síntese, a disponibilidade de mais recursos computacionais e também de mais informação, resultantes tanto do desenvolvimento tecnológico como do paradigma surgimento de sistemas de inteligência artificial que não fossem total ou prioritariamente baseados em um modelo de regras pré-fixadas, mas que fossem alimentados com grandes quantidades de dados, para que pudessem neles fundamentar suas decisões e formar seus padrões decisoriais” (DONEDA, Danilo Cesar Maganhoto *et al.* – Considerações iniciais sobre Inteligência Artificial, ética e autonomia pessoal. **Pensar - Revista de ciências jurídicas** [Em linha]. Vol. 23, n.º 4 (2018), p. 1-17. [Consult. 8 ago. 2022]. Disponível em: <https://periodicos.unifor.br/rpen/article/view/8257>).

ferramentas para compreendê-las”³³⁷. Tal opacidade resulta do funcionamento desses tipos de sistemas. Dados são usados como entrada (*inputs*) e produzem um resultado (*outputs*) que pode ser uma classificação (se um crédito pode ou não ser concedido, ou se um *e-mail* deve ser enviado para a caixa de *spam*). O recebedor dessa resposta (resultado), que pode ter sido o titular dos dados usados como “*inputs*”, dificilmente vai ter uma noção concreta de que aquele “*output*” foi gerado a partir da entrada inserida no sistema³³⁸.

Por essa razão, conforme os sistemas de IA vão se desenvolvendo e se tornando cada vez mais parte do cotidiano, também cresce o interesse em se conhecer como eles podem ser avaliados e auditados em relação ao seu impacto social e ao atendimento às normas legais e regulatórias.

Essa realidade também atingiu os mercados financeiros. A informação é peça-chave diante não só da necessidade de transparência para conter eventuais situações de crise, de dotar o investidor de conhecimento necessário ao investimento para tomada de decisões/opções conscientes, bem como o risco a ela associado para o sistema financeiro. A automação e utilização de sistemas de IA vem sendo largamente aproveitado pelas intuições financeiras para reduzir custos e operacionalização, dando ensejo ao surgimento dos *robots advisors*³³⁹. Mas o que são os *robots advisors* e como funcionam?

3.2 *Robots advisors*: raciocínio/processamento de informação e tomada de decisões

Mafalda Miranda Barbosa explica que os “*robots advisors* são plataformas que, funcionando por meio de algoritmos, providenciam aconselhamento financeiro. Em regra, recolhem online informação acerca dos clientes, da sua situação financeira, do seu perfil, dos seus objetivos de investimento, e utilizam esses dados para prestar conselhos ou investir

³³⁷ RIELLI, Mariana Marques – Críticas ao ideal de transparência como solução para a opacidade de sistemas algorítmicos. In BARBOSA, Mafalda Miranda (coord.) – **Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa**. Indaiatuba: Foco, 2021. p. 437-446, p. 438.

³³⁸ *Ibid.*, *loc. cit.*

³³⁹ BARBOSA, Mafalda Miranda – *Robots advisors* e responsabilidade civil. **Revista de Direito Comercial** [Em linha]. (18 jan. 2020). p. 1-68. [Consult. 8 ago. 2022]. Disponível em: <https://www.revistadedireitocomercial.com/robot-advisers>.

automaticamente os fundos daqueles”^{340,341}. Trata-se de mais um robô, sem a figura física do robô. Um robô consultor³⁴².

Os consultores robóticos, que já são como uma febre entre as Fintechs³⁴³, podem oferecer, por exemplo, configuração de conta, planejamento robusto de metas, serviços de contas e gerenciamento de portfólio. Além disso, oferecem recursos de segurança, atendimento atencioso ao cliente, educação abrangente e taxas baixas.

Em 2010, foi lançado o primeiro robô consultor, da Betterment, criado em Nova York por Jon Stein e Eli Broverman. Eles lançaram sua plataforma *online* na conferência TechCrunch Disrupt e captaram seus primeiros 400 clientes em 24 horas. A Betterment foi fundada em 2008 e, somente após testes com protótipos iniciais e registro na SEC (Securities and Exchange Commission)³⁴⁴, foi lançada a plataforma. Em 24 de junho de 2016, a Betterment interrompeu as negociações na bolsa de valores por 2 horas e meia, depois que o resultado inesperado do referendo no Reino Unido (Brexit) causou caos nos mercados financeiros. Por isso, a empresa foi criticada pela comunicação insuficiente com seus clientes, o que se refletiu nas redes sociais e nas declarações dos parceiros dessa plataforma. Em 31 de janeiro de 2017, a Betterment alterou sua estrutura de preços, o que basicamente significou um aumento de preço para clientes com depósitos superiores a US\$ 100.000 de 0,15% para 0,25%. Mais uma vez ela foi bastante criticada³⁴⁵.

³⁴⁰ BARBOSA, Mafalda Miranda – Robots advisors e responsabilidade civil. **Revista de Direito Comercial** [Em linha]. (18 jan. 2020). p. 1-68. [Consult. 8 ago. 2022]. Disponível em: <https://www.revistadedireitocomercial.com/robot-advisers>.

³⁴¹ “Robo-advisors are digital platforms that provide automated, algorithmic investment services with minimal human supervision. They often automate and optimize passive indexing strategies based on modern portfolio theory” (FRANKENFIELD, Jake – Robo-Advisor. **Investopedia** [Em linha]. New York, 22 set. 2022. [Consult. 8 ago. 2022]. Disponível em: <https://www.investopedia.com/terms/r/roboadvisor-roboadvisor.asp>).

³⁴² “Os robo-advisors são plataformas que usam algoritmos para gerenciar e alocar fundos do investidor. Esses serviços analisam o estado financeiro atual de cada cliente, aversão ao risco e objetivos. A partir daí, recomendam o melhor portfólio de ações ou ativos disponíveis com base nesses dados” (CEDRO TECH – **O que é Robo-Advisor: um relatório completo** [Em linha]. Uberlândia, MG 20 out. 2017. [Consult. 8 ago. 2022]. Disponível em: <https://blog.cedrotech.com/o-que-e-robo-advisor-um-relatorio-completo>).

³⁴³ “A palavra fintech é uma abreviação para financial technology (tecnologia financeira, em português). Ela é usada para se referir a startups ou empresas que desenvolvem produtos financeiros totalmente digitais, nas quais o uso da tecnologia é o principal diferencial em relação às empresas tradicionais do setor” (NUBANK – **O que é fintech e por que esse termo ficou tão popular?** [Em linha]. São Paulo, 03 out. 2017. [Consult. 8 ago. 2022]. Disponível em: <https://blog.nubank.com.br/fintech-o-que-e/>).

³⁴⁴ As autoridades de supervisão do mercado financeiro dos EUA são a Securities and Exchange Commission (SEC) e a Financial Industry Regulatory Authority (FINRA).

³⁴⁵ KITCES, Michael – **Betterment Raises Fees And Pivots To Platform Offering Human Advisors** [Em linha]. Reston, VA, 02 Feb. 2017. [Consult. 8 ago. 2022]. Disponível em: <https://www.kitces.com/blog/betterment-digital-raises-fees-adds-plus-premium-and-advisor-network/>.

Hoje a maioria dos *robots advisors* utiliza estratégias de indexação passiva otimizadas, por meio uma variante moderna de portfólio (MPT)³⁴⁶. Alguns consultores robóticos oferecem portfólios otimizados para investimento socialmente responsável (SRI), investimento Halal ou estratégias táticas que imitam fundos de *hedge*. Além disso, eles podem lidar com tarefas muito mais sofisticadas, como coleta de perdas fiscais, seleção de investimentos e planejamento de aposentadoria³⁴⁷.

Com a expansão dos robôs no mercado e a ameaça de que grandes quantidades de negócios fossem retiradas dos consultores humanos tradicionais, algum deles passaram a contribuir para plataformas de *robots-advisors* ao invés de tentar competir com eles, em uma clara demonstração dos impactos da automação nos direitos de liberdades individuais. Alguns exemplos de plataformas independentes são: a Betterment (EUA), Wealthfront (EUA), Bloom (EUA), SigFig (EUA), Magnetis (Brasil), Waren (Brasil), Véríos (Brasil), Monetis (Brasil) e Robobanking (Índia). Já de empresas de consultoria de investimento com *robots-advisors* temos: Vanguard Personal Advisor Services (EUA), Schwab Intelligent Portfolios (EUA), Fidelity Go (EUA), E-Trade Adaptive Portfolio (EUA) e Rico Alkanza (Brasil)³⁴⁸.

São inúmeras as vantagens associadas à utilização desses sistemas de IA, contudo, como não poderia deixar de ser, também são inúmeros os problemas que se colocam no plano ético, regulatório e jurídico.

Mafalda Miranda Barbosa assevera que “a revolução no campo da robótica trouxe-nos mais: de simples mecanismos capazes de auxiliar os humanos nos sistemas produtivos, passámos a confrontar-nos com robots dotados de inteligência artificial, capazes de uma atuação autónoma. De acordo com os estudiosos na matéria, a sua complexidade e sofisticação são crescentes: é crescente a sua autonomia, bem como a capacidade para aprenderem com base na experiência acumulada e para tomarem decisões independentes. Por outro lado, mostram-se aptos, em algumas situações, a modificar as instruções que lhes foram dadas, levando a cabo atos que não estão de acordo com uma programação pré-definida, mas

³⁴⁶ HAYES, Adam – Enacting a rational actor: Roboadvisors and the algorithmic performance of ideal types. **Economy and Society** [Em linha]. Vol. 49, n.º 4 (2020), p. 562-595. [Consult. 8 ago. 2022]. Disponível em: <https://www.tandfonline.com/doi/abs/10.1080/03085147.2020.1782054>.

³⁴⁷ FRANKENFIELD, Jake – Robo-Advisor. **Investopedia** [Em linha]. New York, 22 set. 2022. [Consult. 8 ago. 2022]. Disponível em: <https://www.investopedia.com/terms/r/roboadvisor-roboadviser.asp>.

³⁴⁸ CEDRO TECH – **O que é Robo-Advisor: um relatório completo** [Em linha]. Uberlândia, MG 20 out. 2017. [Consult. 8 ago. 2022]. Disponível em: <https://blog.cedrotech.com/o-que-e-robo-advisor-um-relatorio-completo>.

que são potenciados pela interação com o meio. Autores há que salientam, igualmente, que os entes dotados de inteligência artificial são capazes de sentir empatia³⁴⁹.

A IA está remodelando as economias em todo o mundo. A promessa é de mais produtividade, eficiência e redução de custos, bem como de contribuição para uma vida melhor, com melhores previsões e para decisões mais bem informadas e assertivas. Essas tecnologias, contudo, ainda estão em seus estágios iniciais e ainda há muito e muitas promessas a serem desenvolvidas para o enfrentamento de desafios globais e promoção de inovação e crescimento. À medida que os impactos da IA permeiam as sociedades, seu poder de transformação deve ser colocado a serviço do ser humano e do planeta.

Ao mesmo tempo, a IA também está alimentando preocupações éticas, considerando especialmente que a Lei (*i.e.*, RGPD) não é suficiente à garantia de tutela de valores e direitos fundamentais no que diz respeito ao desenvolvimento, aplicação e utilização de sistema de IA. Existem perguntas sobre a confiabilidade dos sistemas de IA, incluindo os perigos de codificar e reforçar preconceitos existentes, como aqueles relacionados a gênero e raça, ou de infringir os direitos humanos e valores como privacidade. Crescem as preocupações sobre os sistemas de IA exacerbando a desigualdade, as mudanças climáticas, a concentração de mercado e a exclusão digital. Nenhum país ou ator internacional tem todas as respostas para esses desafios. Portanto, precisamos de cooperação internacional e respostas multissetoriais para orientar o desenvolvimento e o uso da IA para o bem mais amplo³⁵⁰.

Assim, a problemática em torno dos sistemas de IA pode ser resumida da seguinte forma: (i) algoritmos tomam decisões relevantes sobre a vida das pessoas todos os dias; (b) esses algoritmos podem produzir decisões com vieses que fazem parte de decisões humanas anteriores, ou seja, podem carregar em si, e a experiência mostrou que carregam³⁵¹, vieses discriminatórios; (c) muito embora sejam hoje de imensa importância para facilitação de processos e redução de custos, a maior parte das vezes não será possível vislumbrar a lógica por de trás dos resultados produzidos por esses sistemas.

³⁴⁹ BARBOSA, Mafalda Miranda – Robots advisors e responsabilidade civil. **Revista de Direito Comercial** [Em linha]. (18 jan. 2020). p. 1-68, p. 43. [Consult. 8 ago. 2022]. Disponível em: <https://www.revistadedireitocomercial.com/robot-advisers>.

³⁵⁰ OECD. Organisation for Economic Co-operation and Development – **Artificial Intelligence in Society** [Em linha]. Paris: OECD Publishing, 11 June 2019. [Consult. 8 ago. 2022]. Disponível em: <https://doi.org/10.1787/eedfee77-en>.

³⁵¹ BIDDLE, Sam – Especialistas alertam sobre perigos, discriminação e violação de privacidade por tecnologia de reconhecimento facial: Um instituto da Universidade de Nova York compara alguns produtos de reconhecimento facial com pseudociência do século 19. **The Intercept Brasil** [Em linha]. Rio de Janeiro, 05 jan. 2019. [Consult. 8 set. 2022]. Disponível em: <https://theintercept.com/2019/01/04/especialistas-alertam-contra-reconhecimento-facial/>.

Veja-se que, antes mesmo que pensarmos em *accountability*, talvez devêssemos nos preocupar com algo mais básico e simples, como a revelação de informações ocultas ao público, os que, ao menos em tese, seriam os beneficiários (ou atingidos?) pelos resultados da máquina, tal como ocorreu com a professora norte-americana avaliada e demitida pelo sistema de IA chamado IMPACT, citado por Kathy O’Neil³⁵², a respeito da qual nos referimos no segundo capítulo.

É nesse contexto que ganharam força as resoluções, os códigos de conduta e as orientações de caráter *soft*³⁵³ sobre ética para regulação da IA, principalmente na Europa, no intuito de maximizar seus benefícios e diminuir os riscos envolvidos.

3.3 Enquadramento jurídico-ético para sistemas de inteligência artificial

Em 25 de abril de 2018³⁵⁴ e 07 de dezembro de 2018³⁵⁵, a Comissão Europeia apresentou comunicação em que estabeleceu sua visão para desenvolvimento da IA na Europa, assentada em três pilares, que deverão ser observados durante todo o ciclo de vida do sistema: a) deve ser “Legal”, no sentido de cumprir com a legislação e regulamentação legais aplicáveis; b) deve ser “Ética”, garantindo a observância de princípios e valores éticos; e c) deve ser “Sólida” tanto do ponto de vista técnico, de sua robustez, quanto do ponto de vista social, uma vez que, mesmo sendo bem intencionados, sistemas de IA podem causar danos

³⁵² O’NEIL, Cathy – **Algoritmos de Destruição em Massa: como o big data aumenta a desigualdade e ameaça à democracia**. São Paulo: Rua do Sabão, 2020, p. 6-7.

³⁵³ “Comumente o termo *soft law* é conhecido no âmbito do direito internacional para se referir à flexibilidade pela qual os Estados negociam e se organizam através de resoluções, códigos de conduta ou recomendações não equiparadas ao direito formal hierarquizado e sancionador. Sem tradução precisa para o português, seu significado se aproxima a “direito flexível”, um contraponto às normas duras do *hard law*. Utilizado com reservas, *soft law* ainda é um marco jurídico negado por alguns autores como Prosper Weil ao afirmar sobre o conteúdo vago e a forma indefinida do *soft law*, considerando-o uma falácia por não existirem outras compreensões além do direito/não direito. [...] Essa característica não vinculativa facilita “o desenvolvimento de ideias compartilhadas de negócios globais, com grande possibilidade de flexibilidade quando das incertezas dos negócios pactuados”, fazendo com que esse processo de interação entre os entes gere possibilidade de mudanças na percepção dos interesses de cada um sobre um determinado assunto. Ademais, segundo Shelton apud Gregório, os instrumentos de *soft law* têm os procedimentos de adoção, alteração e revisão mais rápidos, tornando-se mais adequados às questões que necessitam de revisões reiteradas. Enquanto para alguns *soft law* ainda apresenta aspectos imprecisos, para outros, oferece aspectos multifacetados: *soft law* como instrumento regulatório e não norma jurídica; como etapa prévia à criação da norma jurídica tradicional; como fonte de direito; como opinião pública internacional; como norma de natureza interdisciplinar, pois versa sobre questões jurídico-políticas, econômicas ou morais” (LOPES, Juliana; MAZURKIEWICZ, Lígia; BARBOSA, Ruth – **Soft Law Como Novo Paradigma Jurídico. Empório do Direito** [Em linha]. São Paulo, 30 ago. 2019. [Consult. 8 ago. 2022]. Disponível em: <https://emporiiododireito.com.br/leitura/soft-law-como-novo-paradigma-juridico>).

³⁵⁴ UNIÃO EUROPEIA. Comissão – **Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das regiões** [Em linha]. Bruxelas, 25 abr. 2018 [Consult. 09 Apr. 2020]. Disponível em: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/PT/COM-2018-237-F1-PT-MAIN-PART-1.PDF>.

³⁵⁵ *Ibid.*

não intencionais, sendo a conjugação dos três pilares, cuja harmonização deverá ser procurada pela sociedade, uma meta para o atingimento de uma IA de confiança.

O quadro ético foi traçado pelo GPAN IA³⁵⁶ e o quadro legal está ainda sendo discutido, tendo sido apresentada, em 21 de abril de 2021, uma proposta de Regulamento para a IA³⁵⁷ no contexto Europeu.

As Orientações apresentadas pelo GPAN IA possuem três níveis de abstração, iniciando pelo mais abstrato, com abordagem baseada nos direitos fundamentais, passando pelo nível intermediário onde são apresentados sete requisitos para os sistemas de IA, até ao nível mais concreto, baseado em uma lista não exaustiva de avaliação da IA de confiança, destinada a operacionalizar os requisitos anunciados

3.3.1 Os direitos fundamentais como direitos de caráter moral e jurídico com exigência de tutela reforçada

Os direitos fundamentais resultam do forte movimento de constitucionalização a partir do século XVIII, sobretudo com o Bill of Rights, de 1776, e em seguida com a Declaração Universal dos Direitos do Homem e do Cidadão³⁵⁸. Muito têm contribuído para o progresso moral da sociedade, sendo inerentes aos seres humanos e pré-existentes ao ordenamento jurídico, decorrendo da própria natureza humana.

Os direitos fundamentais definidos na Carta de Direitos Fundamentais da União Europeia são vinculativos para todos os países membros da EU. Já no plano internacional, a Convenção Europeia dos Direitos Humanos é vinculativa para os Estados Membros da EU, além de domínio não abrangido pelo direito da União. Nesse sentido, ponderam os peritos proponentes das Orientações que “há que sublinhar que direitos fundamentais também são conferidos a indivíduos e (até certo ponto) a grupos por força de seu estatuto moral como seres humanos, independente do seu valor jurídico. [...] Entendidos como universais, alicerçados no estatuto moral inerente aos seres humanos, estão também subjacentes à segunda componente de uma IA de confiança (a IA ética), respeitante das normas éticas que,

³⁵⁶ UNIÃO EUROPEIA. Comissão – **Orientações éticas para uma IA de confiança** [Em linha]. Bruxelas, 08 abr. 2019. [Consult. 09 jul. 2020]. Disponível em: <https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-pt/format-pdf>.

³⁵⁷ *Id.* – **Proposta de Regulamento do Parlamento Europeu e do Conselho que Estabelece Regras Harmonizadas em Matéria de Inteligência Artificial (Regulamento Inteligência Artificial) e Altera Determinados Atos Legislativos da União** [Em linha]. Bruxelas, 21 abr. 2021. [Consult. 09 jul. 2020]. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206>.

³⁵⁸ MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet – **Curso de Direito Constitucional**. 4.^a ed. São Paulo: Saraiva, 2009.

embora não sejam necessariamente vinculativas em termos jurídicos, são cruciais para assegurar a fiabilidade”³⁵⁹.

Robert Alexy afirma que os direitos do homem são diretos morais³⁶⁰. Segundo ele, “direitos morais podem, simultaneamente, ser direitos jurídico-positivos; sua validade, porém, não pressupõe uma positividade. Para a validade ou existência de um direito moral basta que a norma, que está na sua base, valha moralmente. Uma norma vale moralmente quando ela, perante cada um que aceita uma fundamentação racional, pode ser justificada. Direitos do homem existem, com isso, exatamente então quando eles, no sentido apresentado, podem ser justificados perante cada um. À *universalidade da estrutura* dos direitos do homem, que consiste nisto, que eles são, fundamentalmente, direitos de todos contra todos, cabe, com isso, uma *universalidade de validade* que é definida por sua fundamentabilidade perante cada um que aceita uma fundamentação racional”^{361,362}.

Dessa forma, os direitos fundamentais previstos nos referidos instrumentos normativos estão aptos a colaborar com a reflexão ética acerca do modo de desenvolvimento, implantação e utilização da IA de confiança a impactar nos direitos fundamentais e valores subjacentes.

3.3.2 Princípios éticos aplicados à inteligência artificial

Muitas organizações do setor público e privado se inspiram nos direitos humanos/direitos fundamentais para produzir normas éticas para a IA, a exemplo da IBM^{363,364} e da Microsoft³⁶⁵.

³⁵⁹ UNIÃO EUROPEIA. Comissão – **Orientações éticas para uma IA de confiança** [Em linha]. Bruxelas, 08 abr. 2019, p. 12. [Consult. 09 jul. 2020]. Disponível em: <https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-pt/format-PDF>.

³⁶⁰ ALEXY, Robert – Direitos fundamentais no Estado constitucional democrático: para a relação entre direitos do homem. **Revista de Direito Administrativo**. Vol. 217 (1999), p. 55-66, p. 60.

³⁶¹ *Ibid.*, grifos do autor.

³⁶² “O direito do homem ao direito positivo não é um direito do homem ao direito positivo de qualquer conteúdo, senão a um direito positivo que respeita, protege e fomenta os direitos do homem. porque é exatamente o asseguramento dos direitos do homem que fundamenta o direito do homem ao direito positivo. A observação aos direitos do homem é uma condição necessária para a legitimidade do direito positivo. Nisto, que o direito positivo deve respeitar, proteger e fomentar os direitos do homem para ser legítimo, portanto, ser suficiente à sua pretensão à exatidão, manifesta-se a prioridade dos direitos do homem. Direitos do homem estão, com isso, em uma relação necessária com o direito positivo, que está caracterizada pela prioridade dos direitos do homem. Essa prioridade necessária é a terceira marca definidora dos direitos do homem” (*ibid.*, p. 61).

³⁶³ IBM. International Business Machines – **A abordagem multidisciplinar e multidimensional da IBM para a Ética de IA** [Em linha]. Armonk, NY 2020. [Consult. 09 jul. 2020]. Disponível em: <https://www.ibm.com/br-pt/artificial-intelligence/ethics>.

³⁶⁴ *Id.* – **Princípios e práticas para a construção de uma inteligência artificial mais confiável** [Em linha]. Armonk, NY, 16 dez. 2021. [Consult. 09 jul. 2020]. Disponível em: <https://www.ibm.com/blogs/ibm-comunica/principios-e-praticas-para-a-construcao-de-uma-ia-mais-confiavel/>.

Vários documentos que foram por nós consultados possuem guias ou recomendações para adoção de princípios éticos para a regulação da IA. Entre eles, o “*Artificial Intelligence in Society*”³⁶⁶, da OCDE, especialmente o quarto capítulo e os 23 princípios de Asilomar³⁶⁷, resultantes da *Asilomar Conference on Beneficial AI*, realizada em dezembro de 2017 e organizada pelo *Future of Life Institute*³⁶⁸, que reuniu acadêmicos, indústria, organizações não governamentais, bem como a Declaração de Montreal pelo Desenvolvimento Responsável da IA, de 2018³⁶⁹.

O GPAN IA reconhece a maioria dos princípios já apresentados por vários grupos, estabelecendo que tais princípios éticos deverão colaborar com a interpretação dos direitos fundamentais à medida em que o ambiente social e técnico evolui ao longo do tempo e orientar a criação, desenvolvimento e utilização dos sistemas de IA adaptando-se conforme a evolução da sociedade. Muitos deles, já são parte dos requisitos jurídicos previstos na norma jurídica (IA Legal), mas, na medida em que reflitam princípios éticos, farão parte também da IA Ética, segunda componente da IA de confiança.

3.3.2.1 Respeito pela autonomia humana

O direito à liberdade e autonomia dos seres humanos é direito fundamental previsto na Carta de Direitos Fundamentais da EU. Assim, os indivíduos que interagirem com sistemas de IA devem ter garantida a manutenção desses direitos, mantendo sua autodeterminação plena e efetiva.

Por esse princípio, “os sistemas de IA não devem subordinar, coagir, enganar, manipular, condicionar, arregimentar injustificadamente os seres humanos”; deverão ser

³⁶⁵ CRAMPTON, Natasha – Microsoft’s framework for building AI systems responsibly. **Microsoft** [Em linha]. Redmond, WA, 21 June 2022. [Consult. 8 ago. 2022]. Disponível em: <https://blogs.microsoft.com/on-the-issues/2022/06/21/microsofts-framework-for-building-ai-systems-responsibly/>.

³⁶⁶ “Chapter 4, “Public policy considerations”, reviews salient policy issues that accompany the diffusion of AI. The chapter supports the OECD AI Principles adopted in May 2019, first in terms of values: **inclusive growth, sustainable development and well-being; human-centred values and fairness; transparency and explainability; robustness, Security And Safety; And Accountability**. Secondly, It Outlines National Policies To Promote Trustworthy AI Systems: Investing In Responsible AI Research And Development; Fostering A Digital Ecosystem For AI; Shaping An Enabling Policy Environment For AI; Preparing People For Job Transformation And Building Skills; And Measuring Progress” (OECD. Organisation for Economic Co-operation and Development – **Artificial Intelligence in Society** [Em linha]. Paris: OECD Publishing, 11 June 2019. [Consult. 8 ago. 2022]. Disponível em: <https://doi.org/10.1787/eedfee77-en>).

³⁶⁷ FUTURE OF LIFE INSTITUTE – **Asilomar AI Principles** [Em linha]. Boston, MA, 2017. [Consult. 8 ago. 2022]. Disponível em: <https://futureoflife.org/2017/08/11/ai-principles/>.

³⁶⁸ Disponível em: <https://futureoflife.org/>.

³⁶⁹ UNIVERSITÉ DE MONTRÉAL – **Declaração de Montreal pelo Desenvolvimento Responsável da Inteligência Artificial** [Em linha]. Montréal, 2018. [Consult. 8 ago. 2022]. Disponível em: https://www.sbmac.org.br/wp-content/uploads/2021/02/Portugue%CC%82s-UdeM Decl-IA-Resp LA-Declaration_vf.pdf.

instrumentos para desenvolvimento, complementação e capacitação das competências cognitivas, sociais e culturais dos seres humanos. As formas de criação e idealização de sistemas de IA devem ser centradas no ser humano e devem lhes deixar uma oportunidade significativa de escolha³⁷⁰.

3.3.2.2 Prevenção de danos e responsabilidade

Por esse princípio, os sistemas de IA não poderão causar danos ou agravá-los, nem afetar negativamente os seres humanos. Deverão ser protegidas a dignidade, a integridade física e mental, pelo que os ambientes em que operam devem ser protegidos e seguros. Além disso, deverão ser sólidos e protegidos no sentido de se evitar que sejam utilizados para fins maléficos. Assim, as pessoas mais vulneráveis deverão ter maior atenção e ser incluídas no desenvolvimento e implantação de sistemas de IA.

Os sistemas de IA também deverão se precaver no sentido de não gerar assimetrias de poder ou de informação nas relações entre trabalhadores e empregadores, consumidores e empresas, governos e cidadãos, além da prevenção de danos ao meio ambiente e seres vivos³⁷¹.

Além disso, os responsáveis pela criação de sistemas de IA, sejam *designers* ou construtores, pessoas singulares ou coletivas, públicas ou privadas, são partes interessadas e responsáveis pelas implicações morais da utilização ou má utilização dos sistemas de IA³⁷².

3.3.2.3 Equidade

A equidade para efeitos das Orientações tem uma dimensão substantiva e processual. Implica um compromisso com a garantia de distribuição igualitária e justa de benefícios e de custos, bem como a inexistência vieses discriminatórios, injustos e de estigmatização do indivíduo ou de um grupo de indivíduos. Deverá proporcionar também igualdade de oportunidade de acesso aos sistemas de educação, aos bens e serviços e à tecnologia.

Além disso, a utilização de sistemas de IA não poderá levar a que os indivíduos sejam enganados ou prejudicados em sua liberdade de escolha.

³⁷⁰ UNIÃO EUROPEIA. Comissão – **Orientações éticas para uma IA de confiança** [Em linha]. Bruxelas, 08 abr. 2019, p. 15. [Consult. 09 jul. 2020]. Disponível em: <https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-pt/format-PDF>.

³⁷¹ *Ibid.*, *loc. cit.*

³⁷² FUTURE OF LIFE INSTITUTE – **Asilomar AI Principles** [Em linha]. Boston, MA, 2017. [Consult. 8 ago. 2022]. Disponível em: <https://futureoflife.org/2017/08/11/ai-principles/>.

Os profissionais desenvolvedores dos sistemas de IA deverão fazer um juízo de proporcionalidade entre meios e fins, equilibrando os interesses e objetivos em causa. A dimensão processual da equidade implica na possibilidade de contestar e procurar vieses de acesso eficazes contra decisões tomadas pelos sistemas de IA, de modo que os desenvolvedores e responsáveis pela decisão deverão ser identificados e os processos decisórios deverão ser explicáveis.

3.3.2.4 Informação e esclarecimento

O GPAN IA fala no princípio da explicabilidade como sendo crucial para a IA de confiança e para que haja confiança dos utilizadores nos sistemas de IA. Assim, os processos deverão ser transparentes, as capacidades e finalidades dos sistemas comunicadas de forma inteligível e as decisões, tanto quanto possível, explicáveis. Sem tais informações estarão prejudicados os direitos de contestação. Em se tratando de sistemas de IA opacos (do tipo “black box”), poderão ser necessárias outras medidas de explicabilidade (por exemplo, auditabilidade, rastreabilidade), desde que o sistema respeite os direitos fundamentais. O grau de explicabilidade dependerá do contexto e da gravidade das consequências de um resultado errado ou inexato³⁷³.

Por fim, o GPAN IA orienta que, em havendo conflitos entre os princípios, deverão “ser estabelecidos métodos de deliberação responsável para fazer face a esses conflitos”, bem como que “os benefícios globais dos sistemas de IA devem ser substancialmente superiores aos riscos individuais”³⁷⁴. Além disso, a Orientação esclarece que não se espera que desenvolvedores encontrem a solução adequada com base apenas nos princípios éticos, mas que deverão abordar os dilemas éticos e as soluções por meio de uma reflexão racional, baseada em fatos e não em hipóteses ou intuição numa apreciação aleatória. Por fim, enfatizam que direitos fundamentais e princípios a eles relacionados são absolutos e não poderão ser objeto de ponderação.

³⁷³ UNIÃO EUROPEIA. Comissão – **Orientações éticas para uma IA de confiança** [Em linha]. Bruxelas, 08 abr. 2019, p. 16. [Consult. 09 jul. 2020]. Disponível em: <https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-pt/format-PDF>.

³⁷⁴ *Ibid.*, *loc. cit.*

3.3.3 A vinculatividade a inteligência artificial aos direitos fundamentais

3.3.3.1 A dignidade da pessoa humana

O direito à dignidade do ser humano (artigo 1.º - Carta da UE) constitui não só um direito fundamental em si mesmo, mas também a própria base dos direitos fundamentais. Assim, a dignidade do ser humano é valor fundamental que indica que o ser humano nunca poderá ser diminuído, posto em causa, ou reprimido por outras pessoas ou organizações e, menos ainda, por sistemas de IA. Os seres humanos devem ser tratados como sujeitos morais, e não objetos passíveis de serem examinados, classificados, arregimentados, condicionados e manipulados. Portanto, os sistemas de IA devem ser concebidos de forma a respeitar, servir e proteger a integridade física e mental dos indivíduos, satisfazendo suas necessidades essenciais.

3.3.3.2 Liberdade

Os sistemas de IA devem garantir que os indivíduos sejam livres para tomar suas decisões, no sentido de não serem influenciados ou enganados em suas escolhas. Pelos governos e organizações deve ser garantido que as pessoas vulneráveis e em situação de exclusão tenham acesso aos benefícios e oportunidades gerados pela IA. Portanto, os sistemas de IA devem proporcionar aos seres humanos a liberdade de controle sobre suas próprias vidas, incluindo a proteção à livre iniciativa, de desenvolvimento das artes e ciências, da liberdade de expressão, do respeito à vida privada e familiar, bem como à liberdade de reunião e associação³⁷⁵.

3.3.3.3 Igualdade, não discriminação e solidariedade

Todos os seres humanos têm direito ao tratamento igualitário e não discriminatório, assim como o direito de acesso a todos os benefícios proporcionados pelos sistemas de IA. As operações de sistemas de IA não podem gerar resultados ou tratamentos discriminatórios, devendo ser o mais inclusivo possível, notadamente em relação a grupos potencialmente discriminados, como mulheres, empregados, minorias étnicas, pessoas com deficiência, crianças, consumidores e outros grupos em risco de exclusão³⁷⁶.

³⁷⁵ UNIÃO EUROPEIA. Comissão – **Orientações éticas para uma IA de confiança** [Em linha]. Bruxelas, 08 abr. 2019, p. 13. [Consult. 09 jul. 2020]. Disponível em: <https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-pt/format-PDF>.

³⁷⁶ *Ibid.*, loc. cit.

3.3.3.4 Privacidade e governança dos dados pessoais

Importante notar que os direitos de privacidade e da proteção de dados pessoais são direitos fundamentais, de modo que os princípios constantes do RGPD e relacionados aos direitos dos titulares de dados e deveres dos responsáveis pelo tratamento deverão ser encarados à luz do que pode ser ou não pode ser feito, compondo, nesse sentido, orientações a serem seguidas pelas organizações dos setores público e privado durante todo o ciclo de vida da IA, desde sua concepção até sua utilização.

Por fim, sabemos que os desafios que a proteção do direito à privacidade e proteção de dados, bem assim como os direitos de liberdade e direitos fundamentais enfrentam na sociedade contemporânea são ainda enormes. O desenvolvimento tecnológico é fonte de numerosas questões sobre a tutela de direitos e valores fundamentais que o direito ainda terá de enfrentar. Como mostra a história, vantagens econômicas e lucro são obtidos, muitas das vezes, por meio do enfraquecimento dos direitos da personalidade.

Por essa razão, os instrumentos de *soft law* dotados de flexibilidade, celeridade e sendo de mais fácil adoção (que sofrem menos resistência que a *hard law*) possibilitaram que a comunidade internacional começasse a conviver com uma nova forma de lidar as questões relacionadas ao desenvolvimento de sistemas de IA, influenciando a mudança de comportamento e, quem sabe, a criação de normas internas (*hard law*) entre países membros que inspirem e sirvam de diretrizes para a comunidade global, como se deu a exemplo do regulamento de proteção de dados.

Não nos esqueçamos de que cabe aos Estados Democráticos cumprir e fazer cumprir as normas, devendo haver um esforço para que todas as recomendações e legislações (*hard law* ou *soft law*) existentes sejam implementadas na prática pelos governos (inclusive de Portugal e em todos os níveis), pelas populações e pelos Poderes Judiciários para que efetivamente se alcance seus objetivos de proteção dos valores e direitos fundamentais da Europa, ao mesmo tempo que se incentiva e se promove o desenvolvimento dos sistemas de IA.

Mesmo que parte da doutrina não seja, muitas vezes, convergente em relação à atuação dos instrumentos de *soft law*, na prática internacional e ao menos para fins do tema aqui explorado verifica-se a sua indelével contribuição diante da expansão e criação de códigos de ética para desenvolvimento e utilização de sistemas de IA. A *soft law* foi e é elemento unificador das relações internacionais, a facilitar não só as relações comerciais, mas as relações privadas e o respeito aos direitos humanos.

Em um ambiente de veloz desenvolvimento das relações humanas e de crise da legitimidade global, os instrumentos não vinculativos se revelam como fortes colaboradores da integração internacional, do fortalecimento do diálogo e modelagem dos costumes internacionais, que são fontes de direito. Por fim, deve-se reconhecer a eficácia da utilização dos instrumentos de *soft law* para promoção da harmonia a induzirem comportamentos leais e de boa-fé, e na cooperação internacional³⁷⁷.

Feitas tais considerações sobre a IA Ética, merece nossa atenção, mesmo que de forma sintética, a IA Legal, considerando recente proposta de Regulamento da Inteligência Artificial para Europa. No contexto da Proteção de Dados Pessoais, o RGPD teve por principais propósitos a tutela dos direitos e liberdades fundamentais dos cidadãos (notadamente a proteção de dados) e a promoção da circulação de dados pessoais em um espaço regulado³⁷⁸. O que se pretende agora com um Regulamento de IA, no contexto do desenvolvimento dos sistemas de IA, é a consolidação de um quadro jurídico para uma IA de confiança, que resguarde e se desenvolva respeitando os valores e direitos fundamentais da EU, ao mesmo tempo que promove e incentiva o desenvolvimento dos sistemas de IA robustos, centrados no ser humano e que trabalhem em seu próprio benefício.

3.4 A proposta de Regulamento da Inteligência Artificial

A proposta de Regulamento espelha o compromisso político assumido (orientações políticas para 2019-2024)³⁷⁹ pela Presidente da UE, de que a Comissão apresentaria uma proposta legislativa com abordagem que considerasse as implicações humanas e éticas da IA.

O *Livro Branco sobre IA*, a que já nos referimos anteriormente, define opções políticas sobre a forma de alcançar o objetivo de promover a IA e os riscos associados a específicas abordagens de IA. A proposta de Regulamento visa dar conta do segundo objetivo, qual seja, de estruturar um ambiente de confiança para utilização e desenvolvimento da IA a partir de um quadro jurídico bem formatado no sentido de dar concretude a esses objetivos.

De seu texto é possível identificar que a proposta tem como base fundamente “os valores e os direitos fundamentais da UE e pretende dar às pessoas e a outros utilizadores a

³⁷⁷ GREGÓRIO, Fernando da Silva – Consequências sistêmicas da *soft law* para a evolução do direito internacional e o reforço da regulação global. **Revista de Direito Constitucional e Internacional**. Vol. 95 (abr./jul. 2016), p. 299-320, p. 306.

³⁷⁸ CORDEIRO, António Barreto Menezes – **Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020, p. 33.

³⁷⁹ LEYEN, Usula von der – **Orientações Políticas para a Próxima Comissão Europeia 2019-2024**. Uma União mais ambiciosa. O meu programa para a Europa: pela candidata à função de Presidente da Comissão Europeia Usula von der Leyen [Em linha]. Burgdorf, 2019. [Consult. 07 set. 2022]. Disponível em: https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_pt.pdf.

confiança necessária para adotar soluções baseadas em IA, ao mesmo tempo que incentiva as empresas para que as desenvolvam. A inteligência artificial deve ser uma ferramenta a serviço das pessoas e uma força positiva para a sociedade, com o objetivo final de aumentar o bem-estar dos seres humanos. As regras aplicáveis às tecnologias de inteligência artificial disponibilizadas no mercado da União ou que afetam as pessoas da União devem, por isso, centrar-se no ser humano, de modo que as pessoas possam confiar que a tecnologia é utilizada de uma forma segura e em cumprimento da lei, incluindo em matéria de respeito dos direitos fundamentais”³⁸⁰.

A proposta também coloca a importância de dar resposta a desafios como a opacidade, a complexidade, os enviesamentos (que poderiam levar à discriminação), algum grau de imprevisibilidade e comportamentos parcialmente autônomos de determinados sistemas de IA, a fim de garantir compatibilidade desses sistemas com os direitos fundamentais e contribuir para aplicação das normas jurídicas^{381,382}.

Logo na primeira parte, a proposta estabelece os seguintes objetivos específicos: (i) garantir que os sistemas de IA colocados no mercado da União e utilizados sejam seguros e respeitem a legislação em vigor em matéria de direitos fundamentais e valores da União; (ii) garantir a segurança jurídica para facilitar os investimentos e a inovação no domínio da IA; (iii) melhorar a governação e a aplicação efetiva da legislação em vigor em matéria de direitos fundamentais e dos requisitos de segurança aplicáveis aos sistemas de IA; (iv) facilitar o desenvolvimento de um mercado único para as aplicações de IA legítimas, seguras e de confiança e evitar a fragmentação do mercado³⁸³.

Com isso, a EU está a permitir o desenvolvimento e a adição da IA no âmbito da União Europeia e Estados-Membros; a acelerar o uso da IA nesse espaço territorial; a garantir que funcione para as pessoas e seja mais uma força para o bem da sociedade e dos cidadãos; a

³⁸⁰ UNIÃO EUROPEIA. Comissão – **Proposta de Regulamento do Parlamento Europeu e do Conselho que Estabelece Regras Harmonizadas em Matéria de Inteligência Artificial (Regulamento Inteligência Artificial) e Altera Determinados Atos Legislativos da União** [Em linha]. Bruxelas, 21 abr. 2021. [Consult. 09 jul. 2020]. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206>.

³⁸¹ *Ibid.*

³⁸² *Id.* – **A Carta dos Direitos Fundamentais no contexto da inteligência artificial e da transformação digital (Conclusões da Presidência)** [Em linha]. Bruxelas, 21 out. 2020, p. 2. [Consult. 09 jul. 2020]. Disponível em: <https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/pt/pdf>.

³⁸³ UNIÃO EUROPEIA. Comissão – **A Carta dos Direitos Fundamentais no contexto da inteligência artificial e da transformação digital (Conclusões da Presidência)** [Em linha]. Bruxelas, 21 out. 2020, p. 3. [Consult. 09 jul. 2020]. Disponível em: <https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/pt/pdf>.

construir uma liderança estratégica em setores de alto impacto³⁸⁴ e entre as maiores potências em tecnologia.

Em suas regras, a proposta aborda os riscos criados por sistemas de IA; classificam os sistemas consoante seus riscos; define requisitos claros e objetivos para sistemas de IA de alto risco; define obrigações específicas tanto para usuários quanto para desenvolvedores/fornecedores de IA de alto risco; propõe uma avaliação de conformidade do sistema de IA em etapa anterior a sua disponibilização no mercado de produto ou serviços; e propõe uma estrutura de governança. Com esse conjunto de normas se pretende dar aos desenvolvedores, implantadores e usuários de sistemas de IA a segurança necessária, intervindo apenas em situações específicas onde se vislumbrem riscos, bem como, por meio de uma linguagem clara, estabelece quatro níveis de riscos: risco inaceitável, risco alto, risco limitado e risco mínimo. Desse conjunto de classificações, os sistemas de IA qualificados como de risco inaceitável serão vedados.

A proposta também estabelece obrigações específicas de transparência e prestação de contas, as quais, segundo especialistas do MIT Technology Review não seriam viáveis, a exemplo da aplicação das “redes neurais” cujos processos são complexos, o que tornaria impossível a demonstração de como certos resultados e conclusões são produzidos³⁸⁵. Ou seja, nesta parte a problemática da opacidade dos algoritmos continuaria presente.

No que se refere às medidas de apoio à inovação, há incentivo a que as autoridades nacionais criem *sandboxes* regulatórias³⁸⁶ e que prevejam medidas para reduzir encargos regulatórios impostos às pequenas e médias empresas e *start-ups*.

Como não poderia ser diferente, a proposta traz multas pesadas como medida para assegurar a execução eficaz do Regulamento aplicáveis às violações de suas disposições, a exemplo do que já se encontra previsto RGPD. Nesse caso, as multas podem chegar aos trinta

³⁸⁴ VAINZOF, Rony – **Proposta de Regulamento da UE – Inteligência Artificial de "Excelência e Confiável"** [Em linha]. 13 jun. 2021. [Consult. 09 jul. 2022]. Disponível em: <https://www.linkedin.com/pulse/proposta-de-regulamento-da-ue-intelig%C3%A2ncia-e-rony-vainzof/?originalSubdomain=pt>.

³⁸⁵ LOBO, Flavio – Lei europeia poderá ser marco global para regulação da inteligência artificial. **IPEA - Centro de Pesquisa em Ciência, Tecnologia e Sociedade** [Em linha]. Brasília, 02 jun. 2022. [Consult. 09 jul. 2022]. Disponível em: <https://www.ipea.gov.br/cts/pt/central-de-conteudo/noticias/noticias/313-lei-europeia-podera-ser-marco-global-para-regulacao-da-inteligencia-artificial>.

³⁸⁶ Sobre a proposta de se experimentar as *sandboxes* regulatórias para equilibrar a inovação em sistemas de IA com seus riscos potenciais, confira-se: RANCHORDAS, Sofia – **Experimental Regulations for AI: Sandboxes for Morals and Mores**. [Em Linha]. Groningen: University of Groningen, Faculty of Law, May 4, 2021. (Research Paper n.º 7). [Consult. 27 set. 2022]. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839744.

milhões de euros ou a 6% do volume total anual de negócios, relativamente ao exercício financeiro anterior^{387,388}.

Sofia Ranchordas, ao comentar sobre a proposta da EU de regulação da IA, aponta que a regulação funcionará com base em avaliações de risco e proibições *ex ante* e, se aprovada no formato atual, proibirá uma série de aplicações de IA que manipulam e discriminam indivíduos e impõem restrições a muitos sistemas de IA, com impacto negativo sobre direitos fundamentais. No entanto, assevera que esse regime aparentemente restritivo não fecha totalmente a porta para novos desenvolvimentos de IA. Ao contrário, o texto indica que a proposta visa criar um quadro legal que seja amigável à inovação, à prova de futuro e resiliente à disrupção. Nele está consignado que isso será alcançado por meio do incentivo às autoridades competentes para a criação de *sandboxes* regulatórias³⁸⁹. Espera-se, então, que *sandboxes* regulatórias estabeleçam um ambiente controlado para testar inovações tecnológicas por um tempo limitado e com base em um plano de testes acordado com as autoridades competentes. À primeira vista, a proposta de permitir experiências regulamentares no nível dos Estados-Membros pode parecer atraente. Encaixa-se, inclusive, na recente tendência da UE de promover soluções flexíveis e preparadas para o futuro abordagens para a regulação e ajuda a consolidar o princípio da inovação. Alerta, no entanto, que “brincar com caixas de areia, não é brincadeira de criança”³⁹⁰.

Por fim, em seus breves comentários à referida proposta, Mafalda Abreu Peixoto afirma que, em que pese o louvável esforço em se construir a referida regulamentação, o texto não está isento de “riscos e constrangimentos”. Isso porque, como bem coloca, “não é certamente fácil construir uma casa onde convivam alegremente, debaixo do mesmo teto, o

³⁸⁷ PEIXOTO, Mafalda Abreu – **A proposta de Regulamento da IA da Comissão Europeia e os seus constrangimentos globais** [Em linha]. Porto, 24 nov. 2021. [Consult. 09 jul. 2022]. Disponível em: <https://www.itchannel.pt/news/opiniao/a-proposta-de-regulamento-da-ia-da-comissao-europeia-e-os-seus-constrangimentos-globais>.

³⁸⁸ “(84) Os Estados-Membros devem tomar todas as medidas necessárias para assegurar a aplicação das disposições do presente regulamento, inclusive estabelecendo sanções efetivas, proporcionadas e dissuasivas aplicáveis à sua violação. No caso de determinadas violações específicas, os Estados-Membros devem ter em conta as margens e os critérios estabelecidos no presente regulamento. A Autoridade Europeia para a Proteção de Dados deve ter competências para impor coimas às instituições, órgãos e organismos da União que se enquadram no âmbito do presente regulamento” e Artigo 71.º (UNIÃO EUROPEIA. Comissão – **A Carta dos Direitos Fundamentais no contexto da inteligência artificial e da transformação digital (Conclusões da Presidência)** [Em linha]. Bruxelas, 21 out. 2020, p. 3. [Consult. 09 jul. 2020]. Disponível em: <https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/pt/pdf>).

³⁸⁹ PORTUGAL. Presidência do Conselho de Ministros – Decreto-Lei n.º 147/2021, de 30 de julho (Estabelece o regime e define o modelo de governação para a promoção da inovação de base tecnológica através da criação de zonas livres tecnológicas - ZLT). **Diário da República n.º 147/2021** [Em linha], Série I de 2021-07-30, p. 29-37. [Consult. 29 Set. 2022]. Disponível em: <https://dre.pt/dre/detalhe/decreto-lei/67-2021-168697990>

³⁹⁰ RANCHORDAS, Sofia – **Experimental Regulations for AI: Sandboxes for Morals and Mores**. [Em Linha]. Groningen: University of Groningen, Faculty of Law, May 4, 2021, p. 3. (Research Paper n.º 7). [Consult. 27 set. 2022]. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839744.

progresso tecnológico à velocidade da luz e a garantia de proteção dos direitos fundamentais dos cidadãos, em especial os relativos à proteção de dados pessoais”³⁹¹.

Comungamos da opinião de que para a convivência harmônica entre a sociedade (assim entendido o grupo de indivíduos) e o desenvolvimento tecnológico, em crescimento conjunto, as organizações se adaptem ao um novo *mindset*, tal qual se exigiu quando da entrada em vigor do RGPD. Sem a mudança cultural, novos paradigmas não poderão ser implementados. A mudança já é verificável nos compromissos e estratégias da EU em matéria de sustentabilidade (ESG – Environmental, Social and Governance)³⁹², “o de que a sua atividade só será aceite e viável no futuro, na medida em que for transparente, responsabilizável, e enquanto puder contribuir para a resolução de problemas na sociedade, sociais, ambientais ou outros”³⁹³.

Dessa forma, espera-se que haja uma adição crescente de critérios de ESG pelas organizações, ao mesmo passo em que já são exercidas as imposições regulatórias e legais, com visíveis reflexos e contribuições aos usuários, bem como que a adoção dessas medidas se dê mais pelo reconhecimento de que são necessárias para garantir a sustentabilidade dessas organizações do que apenas para fins de marketing.

A previsão de entrada em vigor do regulamento era para o segundo semestre de 2022, mas ainda não há notícias a esse respeito, tendo sido noticiado de que ainda deverá levar mais um ano para que isso aconteça³⁹⁴.

³⁹¹ PEIXOTO, Mafalda Abreu – **A proposta de Regulamento da IA da Comissão Europeia e os seus constrangimentos globais** [Em linha]. Porto, 24 nov. 2021. [Consult. 09 jul. 2022]. Disponível em: <https://www.itchannel.pt/news/opiniao/a-proposta-de-regulamento-da-ia-da-comissao-europeia-e-os-seus-constrangimentos-globais>.

³⁹² BERTÃO, Naiara – Entenda o que é ESG e por que a sigla é importante para as empresas. **Valor Econômico e O Globo** [Em linha]. São Paulo, 21 fev. 2022. [Consult. 09 jul. 2022]. Disponível em: <https://valor.globo.com/empresas/esg/noticia/2022/02/21/entenda-o-que-e-esg-e-por-que-a-sigla-esta-em-alta-nas-empresas.ghtml>.

³⁹³ PEIXOTO, Mafalda Abreu, *op. cit.*

³⁹⁴ LOBO, Flavio – Lei europeia poderá ser marco global para regulação da inteligência artificial. **IPEA - Centro de Pesquisa em Ciência, Tecnologia e Sociedade** [Em linha]. Brasília, 02 jun. 2022. [Consult. 09 jul. 2022]. Disponível em: <https://www.ipea.gov.br/cts/pt/central-de-conteudo/noticias/noticias/313-lei-europeia-podera-ser-marco-global-para-regulacao-da-inteligencia-artificial>.

CONCLUSÃO

Em nosso trabalho começamos apresentando o direito à reserva sobre a intimidade da vida privada e sua evolução, passando pelo direito à privacidade até se chegar ao direito à autodeterminação informativa e à proteção de dados pessoais. Nesse capítulo demonstramos que essa evolução se deu à medida que a sociedade moderna e a tecnológica evoluía, tendo saído de uma visão ligada aos direitos de propriedade para alcançar seu fundamento no indivíduo. Com efeito, foi com a valorização e respeito ao ser humano e o estabelecimento de princípios e direitos fundamentais que as constituições dos Estados Democráticos passaram aos direitos de privacidade como direitos fundamentais apoiados no valor da dignidade do ser humano. Por fim, demonstrou-se que o surgimento de normas relacionadas à proteção de dados pessoais não se justificou apenas para proteger direitos individuais, estes já amparados pelos direitos da personalidade, mas para acautelar interesses distintos, os quais talvez tenham ideologias opostas.

De um lado os interesses de proteção aos interesses das pessoas singulares e grupos de pessoas, de outro lado os interesses de grupos econômicos e das grandes potências de se beneficiarem ao máximo, inclusive economicamente, dos benefícios trazidos pela aplicação de grandes volumes de dados pessoais e em larga escala por sistemas de IA inteligentes (*i.e.*, *machine learning e deep learning*).

A disciplina de proteção de dados é cercada de aparentes paradoxos: ora se protege e se tutela a confidencialidade de dados, ora se busca promover a transparência; ora se visa evitar a colheita e armazenamento, ora se defende as benesses do tratamento automatizado de grandes volumes de dados, ora as decisões automatizadas lesam direitos e liberdades individuais. Existe toda sorte de argumentos econômicos, técnicos e pragmáticos que procuram apontar as supostas incoerências do sistema de proteção de dados. Mas essas tensões não enfraquecem a disciplina. Longe disso. Na verdade, reforçam a necessidade de um equilíbrio a ser realizado entre o Direito e a tecnologia.

O RGPD se esforçou em trazer uma disciplina focada no valor da dignidade humana, estabelecendo direitos aos titulares de dados e deveres para os responsáveis pelo tratamento no intuito de garantir a máxima transparência e inteligibilidade das decisões automatizadas as quais o titular de dados, nas hipóteses previstas, não poderá se recusar a se submeter. O direito à informação ou a explicação está nele previsto exatamente neste intuito, como uma disciplina jurídica centrada no ser humano, não importando o nome que se dê ao direito previsto. O que estaria em questão, então, em função das especificidades dos sistemas de IA

que produzem decisões totalmente automatizadas, seria o conteúdo e limites desse direito. Nesse sentido, entendemos que o sistema de proteção de dados apresentado pelo RGPD cumpre com o objetivo da disciplina centrada no indivíduo, onde encontra sua unidade e razão primeira de ser, mas se revela insuficiente em seus mecanismos de tutela. A segunda conclusão a que chegamos é de que uma tutela suficiente, em razão das questões técnicas envolvidas e do necessário amparo e fomento do desenvolvimento tecnológico será alcançada com a utilização integrada de diversos instrumentos disponíveis de tutela, principalmente no que concerne a instrumentos que possuam maleabilidade e a facilidade de adaptação a novos cenários e à inovação, característica dos instrumentos normativos de caráter “*soft*”, como as normas deontológicas, códigos de autorregulação (códigos de ética e governação), diretrizes principiológicas, etc.

Os sistemas de IA inteligentes, que dispensam a intervenção do ser humano, criando padrões e correlações por eles mesmos e com inúmeras aplicações, algumas mais inofensivas como os serviços de atendimento ao cliente e de *streaming*, outros que podem ser aplicados na medicina para diagnósticos de câncer ou nos transportes como é o caso dos veículos autônomos, por exemplo, mostram o quanto evoluímos em sistemas e o quanto ainda seremos capazes de criar em termos de IA. Exemplos claro disso são os robôs consultores que se tornaram cada dia mais presentes no setor de consultoria privada de investimentos, com seus benefícios amplamente propagandeados, mas que também revelam seus riscos não só no que se refere a transparência dos sistemas e confiança que se pode deles esperar, mas os indeléveis reflexos no mercado de trabalho e na mudança que já impõem a mudança nesse mercado. Mais uma vez a norma positivada não é capaz de dar conta dos problemas que vão surgindo com a rápida evolução dos sistemas de IA nas mais variadas esferas.

Essas tecnologias, contudo, ainda estão em seus estágios iniciais e ainda há muito e muitas promessas a serem desenvolvidas para o enfrentamento de desafios globais de promoção de inovação e crescimento. Nesse cenário ganham força e se fazem presentes as resoluções, os códigos de conduta e as orientações de caráter *soft* sobre ética para regulação da IA, principalmente na Europa, no intuito de potencializar seus benefícios e mitigar os riscos envolvidos.

O enquadramento jurídico-ético da IA no contexto da UE através do louvável trabalho desenvolvido pelo GPAN IA em suas Orientações éticas para uma IA de confiança, são exemplos da influência das normas de índole *soft*. Fundamentadas de forma declarada nos direitos fundamentais previstos na Carta da Europa, tonando-se aptas contribuir, como de fato

contribuíram, para a reflexão ética acerca do modo de desenvolvimento, implantação e utilização da IA de confiança a impactar nos direitos fundamentais e valores subjacentes.

Por fim, a proposta de Regulamento da IA para a UE ainda em discussão, demonstra que as reflexões éticas havidas até então tiveram sua contribuição para a organização e disposição das normas legais que compõem aquela proposta. As lacunas eventualmente surgidas pelo rápido desenvolvimento tecnológico poderão e deverão ser supridas pelos regulamentos de índole *soft*, favorecendo sua adesão, a mudança cultural, bem como significando um limite para a expansão dos sistemas de IA, mesmo que sem previsão uma penalidade específica em caso de desvio do padrão normativo estabelecido.

REFERÊNCIAS

Fontes Documentais

- BRASIL. Presidência da República – **Constituição da República Brasileira de 1988** [Em linha]. Brasília, 1988. [Consult. 10 nov. 2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.
- BRASIL. Presidência da República – Emenda Constitucional nº 115 de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial da União** [Em linha]. N.º 30, Seção 1 (11 fev. 2022), p. 2. [Consult. 24 jul. 2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. ISSN 1677-7042.
- BRASIL. Presidência da República – Lei n.º 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União** [Em linha]. Seção 1 (11 jan. 2002), p. 1. [Consult. 10 abr. 2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm.
- BRASIL. Presidência da República – Lei nº 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. **Diário Oficial da União** [Em linha]. Seção 1 (10 jun. 2011), p. 2. [Consult. 20 jul. 2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112414.htm. ISSN 1677-7042.
- BRASIL. Presidência da República – Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União** [Em linha]. N.º 157, Seção 1 (15 ago. 2019), p. 59-215. [Consult. 20 jul. 2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. ISSN 1677-7042.
- COUNCIL OF EUROPE – **Resolution (73) 22 of the Committee of Ministers to Members States on the protection of the privacy of individuals Vis-a-vis electronic data banks in the private sector** [Em linha]. Luxembourg, 26 Sept. 1973. [Consult. 17 jul. 2002]. Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502830>.

COUNCIL OF EUROPE – **Resolution (73) 23 of the Committee of Ministers to Members States on harmonization measures in the field of legal data processing in the Member States of the Council of Europe** [Em linha]. Luxembourg, 26 Sept. 1973. [Consult. 17 jul. 2015]. Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680502830.

COUNCIL OF EUROPE – **Resolution (74) 29 of the Committee of Ministers to Members States on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector** [Em linha]. Luxembourg, 20 Sept. 1974. [Consult. 17 July 2022]. Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804d1c51.

COUNCIL OF EUROPE. Parliamentary Assembly – **Resolution 428. Declaration on mass communication media and Human Rights** [Em linha]. New York, 23 Jan. 1970. [Consult. 17 jul. 2022]. Disponível em: <https://pace.coe.int/en/files/15842>.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS; EUROPEAN COURT OF HUMAN RIGHTS; COUNCIL OF EUROPE – **Manual da Legislação Europeia sobre Proteção de Dados** [Em linha]. Luxemburgo: Serviço das Publicações da União Europeia, 2014, p. 16. [Consult. 17 jul. 2022]. Disponível em: http://publications.europa.eu/resource/ellar/af9d0b3f-82be-11e5-b8b7-01aa75ed71a1.0017.03/DOC_2. ISBN 978-92-871-9939-3 (Conselho da Europa). ISBN 978-92-9239-498-1 (FRA).

EUROPEAN UNION. Commission – **A definition of Artificial Intelligence: main capabilities and scientific disciplines** [Em linha]. Brussels, 8 Apr. 2019. [Consult. 10 jul. 2022]. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>.

EUROPEAN UNION. Commission – **Guidelines on transparency under Regulation 2016/679**. Article 29 Data Protection Working Group [Em linha]. Bruxelas, 27 Apr. 2016. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/622227/en>.

EUROPEAN UNION. Commission – **Opinion 06//2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. Article 29 Data Protection Working Party [Em linha]. Brussels, 09 April 2014. [Consult. 15 jul. 2022]. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

- EUROPEAN UNION. Commission – **Opinion 2/2017 on data processing at work**. Article 29 Working Party [Em linha]. Brussels, 08 June 2017. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/610169/en>.
- EUROPEAN UNION. Data Protection Board – **Guidelines 05/2020 on consent under Regulation 2016/679**. Article 29 Data Protection Working Group [Em linha]. Brussels, 04 May 2020. [Consult. 15 jul. 2022]. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
- EUROPEAN UNION. Data Protection Board – **Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects**. Brussels, 08 Oct. 2019. European Data Protection Board [Em linha]. Brussels, 08 Oct. 2019. [Consult. 15 jul. 2022]. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.
- OECD. Organisation for Economic Co-operation and Development – **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data** [Em linha]. Paris: OECD, 2013. [Consult. 22 abr. 2020]. Disponível em: <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsdatapersonal.htm>.
- ONU. Organização das Nações Unidas. Assembleia Geral – **Pacto Internacional de Direitos Civis e Políticos** [Em linha]. New York, 16 dez. 1966. [Consult. 17 jul. 2022]. Disponível em: https://www.cne.pt/sites/default/files/dl/2_pacto_direitos_civis_politicos.pdf.
- PORTUGAL – **Constituição da República Portuguesa**. 2.^a ed. Lisboa: INCM, 2016, p. 36. ISBN 978-972-27-2466-1.
- PORTUGAL. Assembleia da República – **Constituição da República Portuguesa de 1976** [Em linha]. Lisboa, 1976. [Consult. 10 nov. 2019]. Disponível em: <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>.
- PORTUGAL. Assembleia da República – Lei n.º 58/2019, de 8 de agosto. Lei da Proteção de Dados Pessoais. Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Diário da República** [Em linha]. N.º 151, Série I (08 ago. 2019), p. 3-40. [Consult. 13 set. 2022]. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra

articulado.php?artigo_id=3118A0002&nid=3118&tabela=leis&pagina=1&ficha=1&so_mio=&nversao=.

PORTUGAL. Ministério da Justiça – Decreto-Lei n.º 47.344/66, de 25 de novembro (Código Civil português). **Diário do Governo** [Em linha]. Série I (25 nov. 1966), p. 1883-2086. [Consult. 10 abr. 2022]. Disponível em: <https://dre.pt/dre/detalhe/decreto-lei/47344-1966-477358>.

PORTUGAL. Ministério Público – **Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal** [Em linha]. Estrasburgo, 28 jan. 1981. [Consult. 17 jul. 2022]. Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/convencao_protecao_pessoas_tratamento_automatizado_dados_caracter_pessoal.pdf.

PORTUGAL. Presidência do Conselho de Ministros – Decreto-Lei n.º 147/2021, de 30 de julho (Estabelece o regime e define o modelo de governação para a promoção da inovação de base tecnológica através da criação de zonas livres tecnológicas - ZLT). **Diário da República n.º 147/2021** [Em linha], Série I de 2021-07-30, p. 29-37. [Consult. 29 Set. 2022]. Disponível em: <https://dre.pt/dre/detalhe/decreto-lei/67-2021-168697990>

PORTUGAL. Procuradoria-Geral Distrital de Lisboa – Lei n.º 67/98, de 26 de outubro (Lei de Protecção da Dados Pessoais). **Diário da República** [Em linha]. N.º 247, Série I-A (26 out. 1998). [Consult. 17 jul. 2022]. Disponível em: <https://dre.pt/dre/legislacao-consolidada/lei/1998-34450175>.

THE UNITED STATES. Department of Justice – **Privacy Act of 1974** [Em linha]. Washington, D.C., 1974. [Consult. 29 maio 2022]. Disponível em: <https://www.justice.gov/opcl/privacy-act-1974>.

TRIBUNAL EUROPEU DOS DIREITOS DO HOMEM. Council of Europe – **Convenção Europeia de Direitos Humanos** [Em linha]. Strasbourg, 2002. [Consult. 17 jul. 2022]. Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/convention_por.pdf.

UNIÃO EUROPEIA – Regulamento (EU) 2016/679 (General Data Protection Regulation - GDPR). **Jornal Oficial da União Europeia**. L119. (04 maio 2016), p. 1-88.

UNIÃO EUROPEIA. Comissão – **Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das regiões** [Em linha]. Bruxelas, 25 abr. 2018 [Consult. 09 Apr. 2020]. Disponível em: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/PT/COM-2018-237-F1-PT-MAIN-PART-1.PDF>.

- UNIÃO EUROPEIA. Comissão – **Livro Branco sobre Inteligência Artificial: Uma abordagem europeia virada para a excelência e confiança** [Em linha]. Bruxelas, 19 fev. 2020. [Consult. 10 jul. 2022]. Disponível em: <https://op.europa.eu/pt/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1>.
- UNIÃO EUROPEIA. Comissão – **Orientações éticas para uma IA de confiança** [Em linha]. Bruxelas, 08 abr. 2019. [Consult. 09 jul. 2020]. Disponível em: <https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-pt/format-PDF>.
- UNIÃO EUROPEIA. Comissão – **Orientações sobre as decisões automatizadas e definições de perfis para efeitos do Regulamento 2016/679**. Grupo de Trabalho do 29.º para Proteção de Dados. Com a última redação revista e adotada em 6 de fevereiro de 2018 [Em linha]. Bruxelas, 27 abr. 2016. [Consult. 15 jul. 2022]. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en>.
- UNIÃO EUROPEIA. Comissão – **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento enunciado no artigo 7.º da Diretiva 95/46/CE** [Em linha]. Bruxelas, 09 abr. 2014. [Consult. 15 jul. 2002]. Disponível em: https://www.uc.pt/protecao-de-dados/suporte/20140409_wp_217_partecer_2_2014_conceito_interesses_legitimos_resp_trat_diretiva_95.
- UNIÃO EUROPEIA. Comissão – **Posso ser sujeito a decisões individuais automatizadas, incluindo a definição de perfis?** [Em linha]. Bruxelas, 2022. [Consult. 15 jul. 2022]. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_pt.
- UNIÃO EUROPEIA. Comissão – **Proposta de Regulamento do Parlamento Europeu e do Conselho que Estabelece Regras Harmonizadas em Matéria de Inteligência Artificial (Regulamento Inteligência Artificial) e Altera Determinados Atos Legislativos da União** [Em linha]. Bruxelas, 21 abr. 2021. [Consult. 09 jul. 2020]. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206>.
- UNIÃO EUROPEIA. Comitê para Proteção de Dados – **Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679**. Bruxelas, 4 maio 2020 [Em linha]. [Consult. 15 jul. 2020]. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf.

- UNIÃO EUROPEIA. Conselho – **A Carta dos Direitos Fundamentais no contexto da inteligência artificial e da transformação digital (Conclusões da Presidência)** [Em linha]. Bruxelas, 21 out. 2020, p. 2. [Consult. 09 jul. 2020]. Disponível em: <https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/pt/pdf>.
- UNIÃO EUROPEIA. Conselho – **Recomendação CM/Rec (2010) 13 e exposição de motivos** [Em linha]. Bruxelas, 23 nov. 2010. [Consult. 28 jul. 2022]. Disponível em: <https://rm.coe.int/16807096c3>.
- UNIÃO EUROPEIA. Parlamento – **Regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas**. Estrasburgo, 20 out. 2020 [Em linha]. [Consult. 15 jul. 2022]. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_PT.html.
- UNIÃO EUROPEIA. Parlamento e Conselho – Regulamento n.º 679, 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). **Jornal Oficial da União Europeia** [Em linha]. L 119, n.º 2 (04 maio 2016). [Consult. 10 nov. 2019]. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:32016R0679>.
- UNIÃO EUROPEIA. Parlamento Europeu. Conselho. Comissão – Carta de Direitos Fundamentais União Europeia. **Jornal Oficial da União Europeia**. C 326/391. (26 out. 2012).
- US SUPREME COURT – Griswold v. Connecticut, 381 U.S. 479 (1965). **Justia**, 2022 [Em linha] [Consult. 10 abr. 2022]. Disponível em: <https://supreme.justia.com/cases/federal/us/381/479/>.

Bibliografia

- ALEXY, Robert – Direitos fundamentais no Estado constitucional democrático: para a relação entre direitos do homem. **Revista de Direito Administrativo**. Vol. 217 (1999), p. 55-66, ISSN 0034-8007.
- ANANNY, Mike; CRAWFORD, Kate – Seeing without knowing: limitations of the transparency ideal and its application to algorithmic accountability. **New Media & Society** [Em linha]. (2016), p. 1-17. [Consult. 15 jul. 2022]. Disponível em: http://mike.ananny.org/papers/anannyCrawford_seeingWithoutKnowing_2016.pdf.
- ASCENSÃO, Jose de Oliveira – A Reserva da Intimidade da Vida Privada e Familiar. **Revista da Faculdade de Direito de Lisboa**. Vol. 43, n.º 1 (2002), p. 9-25. ISSN 0870-3116.
- BABO, Gustavo Schainberg S. – **Discriminação Algorítmica: Origens, Conceitos e Perspectivas Regulatórias** [Em linha]. Belo Horizonte, MG: DTIBR, 15 jun. 2020. [Consult. 30 jul. 2020]. Disponível em: <https://www.dtibr.com/post/discriminacao-algoritmica-origens-conceitos-e-perspectivas-regulatorias-parte-1>.
- BARBOSA, Mafalda Miranda – Robots advisors e responsabilidade civil. **Revista de Direito Comercial** [Em linha]. (18 jan. 2020). p. 1-68. [Consult. 8 ago. 2022]. Disponível em: <https://www.revistadedireitocomercial.com/robot-advisers>. ISSN 2183-9824.
- BASTOS, Celso Ribeiro – **Curso de Direito Constitucional**. 17.^a ed. São Paulo: Saraiva, 1989. Vol. 2. ISBN 8502021737.
- BERTÃO, Naiara – Entenda o que é ESG e por que a sigla é importante para as empresas. **Valor Econômico e O Globo** [Em linha]. São Paulo, 21 fev. 2022. [Consult. 09 jul. 2022]. Disponível em: <https://valor.globo.com/empresas/esg/noticia/2022/02/21/entenda-o-que-e-esg-e-por-que-a-sigla-esta-em-alta-nas-empresas.ghtml>.
- BIDLE, Sam – Especialistas alertam sobre perigos, discriminação e violação de privacidade por tecnologia de reconhecimento facial: Um instituto da Universidade de Nova York compara alguns produtos de reconhecimento facial com pseudociência do século 19. **The Intercept Brasil** [Em linha]. Rio de Janeiro, 05 jan. 2019. [Consult. 8 set. 2022]. Disponível em: <https://theintercept.com/2019/01/04/especialistas-alertam-contra-reconhecimento-facial/>.

- BOBBIO, Norberto – **A Era dos Direitos**. Rio de Janeiro: Elsevier, 2004. ISBN 13-978-85-352-1561-8.
- BROUSSARD, Meredith – **Artificial Unintelligence: How computers Misunderstand the World**. Cambridge, MA: The MIT Press, 2018. ISBN 978-0262346733.
- BURT, Andrew – **Is there a 'right to explanation' for machine learning in the GDPR?** [Em linha]. Portsmouth, NH, 01 June 2017. [Consult. 16 jul. 2022]. Disponível em: <https://iapp.org/news/a/is-there-a-right-to-explanation-for-machine-learning-in-the-gdpr/>.
- CABARAL, Rita Amaral – O direito à intimidade da vida privada. Breve reflexão acerca do art. 80º. Do Código Civil. **Separata dos estudos em memória ao prof. Dr. Paulo Cunha**, Lisboa, 1998.
- CALVÃO, Felipa Urbano – O direito fundamental à proteção de dados pessoais e a privacidade 40 anos depois. **Jornadas nos quarenta anos da constituição da República portuguesa: impacto e evolução**. Porto: Universidade Católica, 2017. p. 85-101. ISBN 978-989-8835-19-2.
- CANOTILHO, José Joaquim Gomes – **“Brançosos” e Interconstitucionalidade: Itinerários dos Discursos Sobre a Historicidade Constitucional**. Coimbra: Almedina, 2008. ISBN 978-9724034850.
- CANOTILHO, José Joaquim Gomes; MOREIRA, Vital – **Constituição da República Portuguesa Anotada**. 4.^a ed., rev. Coimbra: Coimbra, 2014. Vol. 1. ISBN 978-972-32-2286-9.
- CANUT, Leticia – Decisões Automatizadas e o Direito à Explicação no Regulamento Geral de Proteção de Dados da União Europeia. **Revista de Direitos e Garantias Fundamentais** [Em linha]. Vol. 22, n.º 1 (jan./abr. 2021), p. 101-130. [Consult. 16 jul. 2022]. Disponível em: <https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1573>.
- CARDOZO, Virgínia Fehlberg – **O direito à intimidade da vida privada: o problema do enquadramento jurídico constitucional das escutas telefónicas em processo penal** [Em linha]. Coimbra, 2016. Dissertação de Mestrado em Direito apresentado à Universidade de Coimbra, 2016. (polic.^a), p. 61. [Consult. 1 set 2020] Disponível em: <https://estudogeral.sib.uc.pt/bitstream/10316/41203/1/Virg%C3%ADnia%20Fehlberg%20Cardozo.pdf>.
- CARRIERE-SWALLOW, Yan; HAKSAR, Vikram – **The Economics and Implications of Data: An Integrated Perspective** [Em linha]. Washington, D.C.: IMF, 23 Sept. 2019. (Departmental Paper, No. 13) ISBN 978-1513511436. [Consult. 21 abr. 2022].

- Disponível em: <https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596>.
- CEDRO TECH – **O que é Robo-Advisor: um relatório completo** [Em linha]. Uberlândia, MG 20 out. 2017. [Consult. 8 ago. 2022]. Disponível em: <https://blog.cedrotech.com/o-que-e-robo-advisor-um-relatorio-completo>.
- CHESTERMAN, Simon – **Through a Glass: Artificial Intelligence and the Problem of Opacity** [Em linha]. (14 Apr. 2020), p. 1-26. (NUS Law Working Paper, 011) [Consult. 15 jul. 2022]. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3575534.
- CITRON, Danielle Keats; PASQUALE, Frank – The scored society: due process for automated predictions. **Washington Law Review** [Em linha]. Vol. 89 (2014), p. 1-33. [Consult. 12 set. 2022]. Disponível em: <https://core.ac.uk/download/pdf/327104566.pdf>.
- COELHO, Larissa A. – Investigação de "casamentos brancos" e a reserva da intimidade da vida privada: Uma análise do acórdão do Tribunal Central Administrativo Sul, de 17 de dezembro de 2009. **Revista Jus Navigandi**. Ano 16, n. 3012 (30 set. 2011) [Em linha] [Consult. 1 fev. 2022]. Disponível em: <https://jus.com.br/artigos/20110/investigacao-de-casamentos-brancos-e-a-reserva-da-intimidade-da-vida-privada/1>. ISSN 1518-4862.
- CORDEIRO, António Barreto Menezes – Decisões Automatizadas à Luz do RGPD e da LGPD. **Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa**. Indaiatuba: Foco, 2021. p. 263-270. ISBN 978-65-5515-253-1.
- CORDEIRO, António Barreto Menezes – **Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019**. Coimbra: Almedina, 2020. ISBN 978-972-40-8304-9.
- CORDEIRO, António Barreto Menezes (coord.) – **Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019**. Lisboa: Almedina: 2021. ISBN 9789724092614.
- CORREIA, Victor – Sobre o Direito à privacidade. **O Direito**. [Em Linha] Ano 146, n.º 1 (2014), p. 9-32. [Consult. 17 jul. 2022]. Disponível em: https://www.academia.edu/6106718/Sobre_o_direito_%C3%A0_privacidade. ISBN 978-9724051178.
- COSTA ANDRADE, Manuel da – **Liberdade de imprensa e inviolabilidade pessoal: uma perspetiva jurídico-criminal**. Coimbra: Coimbra, 1996. ISBN 9723207508.
- COSTA, Inês da Silva – A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas. **Revista Eletrónica de Direito** [Em linha]. Vol. 24, n.º 1 (fev. 2021), p. 34-82. [Consult. 06 jun. 2022]. Disponível em: https://cije.up.pt/client/files/0000000001/4-ines-costa_1677.pdf. ISSN 1678-8729.

- CRAMPTON, Natasha – Microsoft’s framework for building AI systems responsibly. **Microsoft** [Em linha]. Redmond, WA, 21 June 2022. [Consult. 8 ago. 2022]. Disponível em: <https://blogs.microsoft.com/on-the-issues/2022/06/21/microsofts-framework-for-building-ai-systems-responsibly/>.
- D’ARC, Tânia – O que é inteligência artificial: 16 exemplos no seu dia a dia. **Smart Hint** [Em linha]. Curitiba, PR, 25 mar. 2022. [Consult. 8 ago. 2022]. Disponível em: <https://www.smarthint.co/o-que-e-inteligencia-artificial-exemplos/>.
- DESHAW&CO [Em linha] New York, NY, 2022. [Consult. 7 jun. 2022]. Disponível em: <https://www.deshaw.com/>.
- DOMINGOS, Pedro – **Algoritmo Mestre**. São Paulo: Novatec, 2017. ISBN 978-85-7522-538-7.
- DONEDA, Danilo – **Da privacidade à proteção de dados pessoais**. 2.^a ed. São Paulo: Revista dos Tribunais, 2019. ISBN 978-85-5321-957-5.
- DONEDA, Danilo Cesar Maganhoto; MENDES, Laura Schertel; SOUZA, Carlos Affonso Pereira; ANDRADE, Norberto Nuno Gomes – Considerações iniciais sobre Inteligência Artificial, ética e autonomia pessoal. **Pensar - Revista de Ciências Jurídicas** [Em linha]. Vol. 23, n.º 4 (2018), p. 1-17. [Consult. 8 ago 2022]. Disponível em: <https://periodicos.unifor.br/rpen/article/view/8257>. ISSN-2317-2150.
- DONEDA, Danilo; ALMEIDA, Virgílio Augusto Fernandes – O que é a governança de algoritmos? **Tecnopolíticas da Vigilância: perspectivas da margem**. São Paulo: Boitempo, 2018. ISBN 978-85-7559-662-3.
- DOTTI, René Ariel – **Proteção da vida privada e liberdade de informação** [Em linha]. São Paulo: Revista dos Tribunais, 1980. [Consult. 01 maio 2022]. Disponível em: <http://localhost:8080/xmlui/handle/123456789/1303>.
- DRAY, Guilherme – O direito à reserva da intimidade da vida privada: o artigo 80.º do Código Civil de 1966. **Revista de Direito Civil**. Ano II, n.º 3 (2017). p. 673-699. ISBN 978-03-17-35535-2.
- DTIBR. Direito, Tecnologia e Inovação – **GDPR e decisões automatizadas: Limites a um "Direito à explicação"** [Em linha]. Belo Horizonte, MG, 21 nov. 2018. [Consult. 4 dez. 2019]. Disponível em: <https://www.dtibr.com/post/2018/11/21/gdpr-e-decis%C3%B5es-automatizadas-limites-a-um-direito-%C3%A0-explica%C3%A7%C3%A3o>.
- EDWARDS, Lilian; VEALE, Michael – Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For. **Duke Law & Technology Review** [Em linha]. Vol. 16, n.º 18 (23 maio 2017), p. 18-84. [Consult. 4

- dez. 2019]. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855#.
- EVE – **Right to Explanation: a Right that Never Was (in GDPR)**. Málaga, Andaluzia, 1 March 2018 [Em linha] [Consult. 4 dez. 2019]. Disponível em: <https://datawanderings.com/2018/03/01/right-to-explanation/>.
- FARINHO, Domingos Soares – **Intimidade da Vida Privada e Media no Ciberespaço**. Coimbra: Almedina, 2006. ISBN 972-40-2740-6.
- FERRAZ, Tércio Sampaio – Sigilo de dados: direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito de São Paulo**. Vol. 88 (jan./dez. 1993), p. 439-459.
- FERREIRA, Diogo Figueiredo Perfeito Dias – Trabalhador, reserva da intimidade da vida privada e “redes sociais”: nótulas reflexivas sobre este delicado problema laboral. **Estudos Laborais** [Em Linha]. Ano 80, Vol. III/IV (jul./dez. 2020), p. 585-611. [Consult. 17 jul. 2022] Disponível em: <https://portal.oa.pt/media/132093/diogo-figueiredo-perfeito-dias-ferreira.pdf>. ISSN. 0870-8118.
- FESTAS, David de Oliveira – O direito à reserva da intimidade da vida privada do trabalhador no Código do Trabalho. **Revista da Ordem dos Advogados (ROA)** [Em linha]. Ano 64, Vol. I-II (nov. 2004), p. 1 [Em linha]. [Consult. 02 fev. 2022]. Disponível em: <https://portal.oa.pt/publicacoes/revista-da-ordem-dos-advogados-roa/ano-2004/ano-64-vol-i-ii-nov-2004/artigos-doutriniais/david-de-oliveira-festas-o-direito-a-reserva-da-intimidade-da-vida-privada-do-trabalhador-no-codigo-do-trabalho-star/>.
- FRANKENFIELD, Jake – Robo-Advisor. **Investopedia** [Em linha]. New York, 22 set. 2022. [Consult. 8 ago. 2022]. Disponível em: <https://www.investopedia.com/terms/r/roboadvisor-roboadviser.asp>.
- FUTURE OF LIFE INSTITUTE – **Asilomar AI Principles** [Em linha]. Boston, MA, 2017. [Consult. 8 ago. 2022]. Disponível em: <https://futureoflife.org/2017/08/11/ai-principles/>.
- GONZÁLEZ, José Alberto Rodríguez Lorenzo – **Código Civil Anotado. Parte Geral**. Lisboa: Quid Iuris, 2019. Vol. 1. ISBN 978-972724820-9.
- GOODMAN, Bryce; FLAXMAN, Seth – European Union Regulations on Algorithmic Decision-Making and a “Right to Explanation”. **AI Magazine** [Em linha]. Vol. 38, n.º 3 (2017), p. 50-57. [Consult. 29 jul. 2020]. Disponível em: <https://doi.org/10.1609/aimag.v38i3.2741>. ISSN 0738-4602.

- GREGÓRIO, Fernando da Silva – Consequências sistêmicas da *soft law* para a evolução do direito internacional e o reforço da regulação global. **Revista de Direito Constitucional e Internacional**. Vol. 95 (abr./jul. 2016), p. 299-320, p. 306. ISSN 1518-272X.
- GUTIERREZ, Andriei – É possível confiar em um sistema de Inteligência Artificial? Práticas em torno da melhoria de sua confiança, segurança, evidências de accountability. In MULHOLLAND, Caitlin; FRAZÃO, Ana (coord.) – **Inteligência Artificial e Direito: ética, regulação e responsabilidade**. São Paulo: Thompson Reuters Brasil, 2019. p. 83-97. ISBN 978-85-5321-729-8.
- HAYES, Adam – Enacting a rational actor: Roboadvisors and the algorithmic performance of ideal types. **Economy and Society** [Em linha]. Vol. 49, n.º 4 (2020), p. 562-595. [Consult. 8 ago. 2022]. Disponível em: <https://www.tandfonline.com/doi/abs/10.1080/03085147.2020.1782054>. ISSN 1588-970X.
- HIRSH, Dennis D. – The Glass House Effect: Big Data, The New Oil, and The Power of Analogy. **Maine Law Review** [Em linha]. (12 fev. 2014), p. 1-28 [Em linha]. [Consult. 13 set. 2022]. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393792.
- HPE. Hewlett Packard Enterprise – **Inteligência artificial** [Em linha]. Houston, TE, 2022. [Consult. 8 ago. 2022]. Disponível em: <https://www.hpe.com/br/pt/what-is/artificial-intelligence.html>.
- IBM. International Business Machines – **A abordagem multidisciplinar e multidimensional da IBM para a Ética de IA** [Em linha]. Armonk, NY [Consult. 09 jul. 2020]. Disponível em: <https://www.ibm.com/br-pt/artificial-intelligence/ethics>.
- IBM. International Business Machines – **Princípios e práticas para a construção de uma inteligência artificial mais confiável** [Em linha]. Armonk, NY, 16 dez. 2021. [Consult. 09 jul. 2020]. Disponível em: <https://www.ibm.com/blogs/ibm-comunica/principios-e-praticas-para-a-construcao-de-uma-ia-mais-confiavel/>.
- ICO. Information Commissioner’s Office – **Rights related to automated decision making including profiling** [Em linha]. Wilmslow, Cheshire, 2019. [Consult. 10 dez. 2019]. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/>.
- IGLESIAS CUBRÍA, Manuel – **El Derecho a La Intimidad**. Discurso Inaugural del año académico 1970-1971 [Em linha]. Oviedo: Universidad de Oviedo, 1970). [Consult. 10 abr. 2022]. Disponível em: <https://core.ac.uk/download/pdf/71852292.pdf>.

- KAISER, Brittany – **Targeted: The Cambridge Analytica Whistleblower`s Inside Story of How Big Data, Trump, Brexit and Facebook Broke Democracy and How It Can Happen Again**. New York: HarperCollins, 2019. ISBN 978-0008363901.
- KIRBY, Michael – **30 Years After: the Impact of the OECD Privacy Guidelines** [Em linha]. Paris: OECD, 10 Mar. 2010. [Consult. 01 ago. 2022]. Disponível em: <http://www.oecd.org/internet/ieconomy/30yearsaftertheimpactoftheoecdprivacyguidelines.htm>.
- KITCES, Michael – **Betterment Raises Fees And Pivots To Platform Offering Human Advisors** [Em linha]. Reston, VA, 02 Feb. 2017. [Consult. 8 ago. 2022]. Disponível em: <https://www.kitces.com/blog/betterment-digital-raises-fees-adds-plus-premium-and-advisor-network/>.
- KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher – **The EU General Data Protection Regulation (GDPR): A commentary**. Oxford: Oxford University Press, 2020. ISBN 978-0198846864.
- LEYEN, Usula von der – **Orientações Políticas para a Próxima Comissão Europeia 2019-2024**. Uma União mais ambiciosa. O meu programa para a Europa: pela candidata à função de Presidente da Comissão Europeia Usula von der Leyen [Em linha]. Burgdorf, 2019. [Consult. 07 set. 2022]. Disponível em: https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_pt.pdf.
- LOBO, Flavio – Lei europeia poderá ser marco global para regulação da inteligência artificial. **IPEA - Centro de Pesquisa em Ciência, Tecnologia e Sociedade** [Em linha]. Brasília, 02 jun. 2022. [Consult. 09 jul. 2022]. Disponível em: <https://www.ipea.gov.br/cts/pt/central-de-conteudo/noticias/noticias/313-lei-europeia-podera-ser-marco-global-para-regulacao-da-inteligencia-artificial>.
- LOCKE, John – **Segundo tratado sobre governo civil: ensaio sobre a origem, os limites e os fins verdadeiros do governo**. Petrópolis: Vozes, 1999. ISBN 85-326-1240-7.
- LOPES, Juliana; MAZURKIEWICZ, Lígia; BARBOSA, Ruth – Soft Law Como Novo Paradigma Jurídico. **Empório do Direito** [Em linha]. São Paulo, 30 ago. 2019. [Consult. 8 ago. 2022]. Disponível em: <https://emporiododireito.com.br/leitura/soft-law-como-novo-paradigma-juridico>.
- MARINELLI, Marcelo Romão – **Privacidade e redes sociais virtuais**. Rio de Janeiro: Lumen Juris, 2017. ISBN: 978-8551900536.

- MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet – **Curso de Direito Constitucional**. 4.^a ed. São Paulo: Saraiva, 2009. ISBN 978-85-02-07819-2.
- MENDES, Laura Schertel Ferreira Mendes – Autodeterminação informativa: a história de um conceito. **Pensar – Revista de Ciências Jurídicas [Em linha]**. Vol. 25, n.º 4 (out./dez. 2020), p. 1-18. [Consult. 22 abr. 2022]. Disponível em: <https://periodicos.unifor.br/rpen/article/view/10828>. ISSN-2317-2150.
- MIGLIETTI, Lucia – Profili storico-comparativi del diritto alla privacy. **Diritti Comparati: comparare i diritti fondamentali in Europa [Em linha]**. (04 dic. 2014). [Consult 10 abr. 2022]. Disponível em: <https://www.diritticomparati.it/profili-storico-comparativi-del-diritto-alla-privacy/>.
- MILL, John Stuart – **Sobre a liberdade**. São Paulo: Martins Fontes, 2000. ISBN 978-8595070363.
- MIRANDA, Jorge; MEDEIROS, Rui – **Constituição Portuguesa Anotada**. Lisboa: Universidade Católica, 2017. Vol. 1. ISBN 9789725405413.
- MONIZ, Helena – Notas sobre a proteção de dados pessoais perante a informática. **Revista Portuguesa de Ciência Criminal**. Ano 7, Fasc. 2.º (abr./jun. 1997), p. 231-261. ISSN 0871-8563.
- MOTA PINTO, Paulo – A limitação voluntária do direito à reserva sobre a intimidade da vida privada. **Separata de Estudos em homenagem a Cunha Rodrigues [Em linha]**. Coimbra: Coimbra, 2001. [Consult. 02 fev. 2022] Disponível em: <https://xdocs.com.br/doc/limitacao-do-direito-a-reserva-xn45y7x343oj>.
- MOTA PINTO, Paulo – O direito à reserva da intimidade. **Boletim da Faculdade de Direito: Universidade de Coimbra**. Vol. LXIX (1993), p. 479-586. ISSN 0303-9773.
- MOTA PINTO, Paulo; MONTEIRO, João Pinto – **Código Civil e legislação complementar e jurisprudência**. 2.^a ed. Lisboa: INCM, 2016. ISBN 978-972-27-2428-9.
- MULHOLLAND, Caitlin – Responsabilidade civil e processos decisórios autônomos em sistemas de Inteligência Artificial (IA): autonomia, imputabilidade e responsabilidade. *In* MULHOLLAND, Caitlin; FRAZÃO, Ana (coord.) – **Inteligência Artificial e Direito: ética, regulação e responsabilidade**. São Paulo: Thompson Reuters Brasil, 2019. p. 327-348. ISBN 978-85-5321-729-8.
- MULHOLLAND, Caitlin Sampaio – Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**. Vol. 19, n.º 3 (2018), p. 159-180.

- [Consult. 10 abr. 2022]. Disponível em: <https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603/pdf>. ISSN 2175-6058.
- MULHOLLAND, Caitlin Sampaio – **Mercado, Pessoa Humana e Tecnologias: a Internet das Coisas e a proteção do direito à privacidade** [Em linha]. Rio de Janeiro: PUC-RJ, ago. 2021. [Consult. 07 maio 2022]. Disponível em: <https://www.jur.puc-rio.br/wp-content/uploads/2021/08/CAITLIN-SAMPAIO-Mercado-Pessoa-Humana-e-Tecnologias.pdf>.
- MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. – Entre as Leis da Robótica e a ética: Regulação para o Adequado Desenvolvimento da Inteligência Artificial. In BARBOSA, Mafalda Miranda (coord.) – **Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa**. Indaiatuba: Foco, 2021. p. 65-78. ASIN B08Z8P2XR2.
- NUBANK – **O que é fintech e por que esse termo ficou tão popular?** [Em linha]. São Paulo, 03 out. 2017. [Consult. 8 ago. 2022]. Disponível em: <https://blog.nubank.com.br/fintech-o-que-e/>.
- O'NEIL, Cathy – **Algoritmos de Destruição em Massa: como o big data aumenta a desigualdade e ameaça à democracia**. São Paulo: Rua do Sabão, 2020. ISBN 978-65-86460-02-5.
- OECD. Organisation for Economic Co-operation and Development – **Artificial Intelligence in Society** [Em linha]. Paris: OECD Publishing, 11 June 2019. [Consult. 8 ago. 2022]. Disponível em: <https://doi.org/10.1787/eedfee77-en>.
- OLIVEIRA, Madalena Perestrelo de – Definição de perfis e decisões individuais automatizadas no Regulamento Geral sobre a Proteção de Dados. In CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (ed.) – **Fin Tech II: Novos Estudos sobre Tecnologia Financeira**. Coimbra: Almedina, 2019. p. 61-88. ISBN 978-972-40-7839-7.
- ONU. Organização das Nações Unidas – **Declaração Universal dos Direitos Humanos** [Em linha]. Paris, 10 dez. 1948. [Consult. 09 jun. 2022]. Disponível em: <https://brasil.un.org/sites/default/files/2020-09/por.pdf>.
- OTERO, Paulo – **Manual de Direito Administrativo**. Coimbra: Almedina, 2016. Vol. I. ISBN 978-972-40-5388-2.
- PASQUALE, Frank. **The Black Box society: the secret algorithms that control money and information**. Cambridge: Harvard University Press, 2015. ISBN 978-0674970847.
- PEIXOTO, Fabiano Hartmann – **Inteligência Artificial e Direito: convergência ética e estratégica**. Curitiba: Alteridade, 2020. ISBN 978-65-990587-2-1.

- PEIXOTO, Mafalda Abreu – **A proposta de Regulamento da IA da Comissão Europeia e os seus constrangimentos globais** [Em linha]. Porto, 24 nov. 2021. [Consult. 09 jul. 2022]. Disponível em: <https://www.itchannel.pt/news/opiniao/a-proposta-de-regulamento-da-ia-da-comissao-europeia-e-os-seus-constrangimentos-globais>.
- PINHEIRO, José Alexandre Guimarães de Souza – **Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional** [Em linha]. Lisboa, 2012. Tese de doutorado em Direito (Ciências Jurídico-Políticas) apresentada à Universidade de Lisboa. (polic.^a), p. 350. [Consult. 10 out. 2021]. Disponível em: <https://repositorio.ul.pt/handle/10451/7407?locale=en> ou Lisboa: AAFDL, 2015. ISBN 9786120002605.
- PIPOCA 3D – Brigitte Bardot – **sensual e no tribunal** [Em linha]. 2022. [Consult. 23 jul. 2022]. Disponível em: <https://www.pipoca3d.com.br/2015/02/brigitte-bardot-sensual-e-no-tribunal.html>.
- PRATA, Ana (coord.) – **Código Civil Anotado. Volume I (Artigos 1.º a 1250.º)**. Coimbra: Almedina, 2019. ISBN 9789724079073.
- RANCHORDAS, Sofia – **Experimental Regulations for AI: Sandboxes for Morals and Mores**. [Em Linha]. Groningen: University of Groningen, Faculty of Law, May 4, 2021. (Research Paper n.º 7). [Consult. 27 set. 2022]. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839744.
- RIELLI, Mariana Marques – Críticas ao ideal de transparência como solução para a opacidade de sistemas algorítmicos. In BARBOSA, Mafalda Miranda (coord.) – **Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa**. Indaiatuba: Foco, 2021. p. 437-446. ISBN 978-65-5515-253-1.
- RIGEUS, Rafael – Reconhecimento facial falha e homem inocente passa 10 dias na cadeia. **Olhar Digital** [Em linha]. São Paulo, 30 dez. 2020. [Consult. 12 set. 2022]. Disponível em: <https://olhardigital.com.br/2020/12/30/noticias/reconhecimento-facial-falha-e-homem-inocente-passa-10-dias-na-cadeia/>.
- RODOTÁ, Stefano – **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008. ISBN 978-857147-688-2.
- RODRIGUES, Cunha – Informática e a reserva da vida privada. Comunicação e Defesa do Consumidor. **Atas do Congresso Internacional organizado pelo Instituto Jurídico da Comunicação da Faculdade de Direito da Universidade de Coimbra, de 25 a 27 de novembro de 1993**. Coimbra, 1996. p. 287-292.

- SAMPAIO, José Adércio Leite – **Direito à intimidade e à vida privada**. Belo Horizonte: Del Rey, 1998. ISBN 8573082178.
- SARLET, Ingo Wolfgang – A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I. **Consultor Jurídico** [Em linha]. (11 mar. 2022). [Consult. 24 jul. 2022]. Disponível em: <https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protacao-dados-pessoais-direito-fundamental>. ISSN 1809-2829.
- SELBST, Andrew D.; POWLES, Julia – Meaningful Information and the Right to Explanation. **International Data Privacy Law** [Em linha]. Vol. 7, n.º 4 (2017), p. 233-242. [Consult. 10 dez. 2019]. Disponível em: <https://academic.oup.com/idpl/article/7/4/233/4762325>.
- SHANE, Harris – **Your Samsung SmartTV Is Spying on You, Basically** [Em linha]. New York, 14 Apr. 2017. [Consult. 07 maio 2022]. Disponível em: <https://www.thedailybeast.com/your-samsung-smarttv-is-spying-on-you-basically>.
- SHWAB, Klaus – **A quarta Revolução Industrial**. São Paulo: Edipro, 2016. ISBN 978-85-7283-978-5.
- SILVA, Artur Flamínio da – Inteligência Artificial e Direito Administrativo. **Direito Administrativo e Tecnologia**. Coimbra: Almedina, 2021. ISBN 978-972-40-9271-3.
- SILVA, Nilton Correa – Inteligência Artificial. In MULHOLLAND, Caitlin; FRAZÃO, Ana (coord.) – **Inteligência Artificial e Direito: ética, regulação e responsabilidade**. São Paulo: Thompson Reuters Brasil, 2019. p. 35-52. ISBN 978-85-5321-729-8.
- SOUZA, Marcelo Rebelo de; ALEXANDRINO, José de – **Constituição da República Portuguesa: comentada: introdução teórica e histórica, anotações, doutrina e jurisprudência, Lei do Tribunal Constitucional**. Lisboa: Lex, 2000. ISBN 9729495912.
- STEIBEL, Fabro; VICENTE, Victor Freitas; JESUS, Diego Santos Vieira de – Possibilidade e potenciais da utilização da Inteligência Artificial. In MULHOLLAND, Caitlin; FRAZÃO, Ana (coord.) – **Inteligência Artificial e Direito: ética, regulação e responsabilidade**. São Paulo: Thompson Reuters Brasil, 2019. p. 35-52. ISBN 978-85-5321-729-8.
- THE NEW YORK TIMES – **Wrongfully Accused by an Algorithm** [Em linha]. New York, 03 ago. 2020. [Consult. 12 set. 2022]. Disponível em: <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>.
- UNIVERSIDADE DE COIMBRA. Informação Administrativa e Tratamento de Dados – **Proteção do Tratamento de Dados** [Em linha]. Coimbra: Universidade de Coimbra,

2022. [Consult. 25 ago. 2022]. Disponível em: <https://www.uc.pt/protecao-de-dados/protecao-de-dados-pessoais/principios-do-tratamento-dados/>.
- UNIVERSITÉ DE MONTRÉAL – **Declaração de Montreal pelo Desenvolvimento Responsável da Inteligência Artificial** [Em linha]. Montréal, 2018. [Consult. 8 ago. 2022]. Disponível em: https://www.sbmec.org.br/wp-content/uploads/2021/02/Portugue%CC%82s-UdeM_Decl-IA-Resp_LA-Declaration_vf.pdf.
- VAINZOF, Rony – **Comentários ao GDPR – Regulamento de Dados da União Europeia**. 2.^a ed. São Paulo: Thomson Reuters Brasil, 2019. ISBN 978-8553212309.
- VAINZOF, Rony – **Proposta de Regulamento da UE – Inteligência Artificial de "Excelência e Confiável"** [Em linha]. 13 jun. 2021. [Consult. 09 jul. 2022]. Disponível em: <https://www.linkedin.com/pulse/proposta-de-regulamento-da-ue-intelig%C3%AAncia-e-rony-vainzof/?originalSubdomain=pt>.
- VARELLA, Marcelo Dias – **Direito internacional público**. 7.^a ed. São Paulo: Saraiva, 2017. ASIN B078JWNJ46.
- VOGL, Roland; FARHANGI, Ashkon; CASEY, Bryan. **Rethinking Explainable Machines: The Next Chapter in the GDPR's 'Right to Explanation' Debate**. Oxford, 15 May 2018 [Em linha]. [Consult. 4 dez. 2019]. Disponível em: <https://www.law.ox.ac.uk/business-law-blog/blog/2018/05/rethinking-explainable-machines-next-chapter-gdprs-right-explanation>.
- WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano – Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law** [Em linha]. Vol. 7, n.º 2 (1 May 2017), p. 76-99 [Em linha]. [Consult. 4 dez. 2019]. Disponível em: <https://academic.oup.com/idpl/article/7/2/76/3860948>.