Universidade do Estado do Rio de Janeiro
Centro de Ciências Sociais
Faculdade de Direito

Bernardo José Oliveira Araujo

Proporcionalidade e transparência como parâmetros normativos do tratamento de dados pessoais em aplicações de inteligência artificial

Rio de Janeiro
2025

Bernardo José Oliveira Araujo

Proporcionalidade e transparência como parâmetros normativos do tratamento de dados pessoais em aplicações de inteligência artificial

Tese de Doutorado apresentada à Banca Examinadora do programa de Pós-graduação em Direito, da Faculdade de Direito da Universidade do Estado do Rio de Janeiro, na área de concentração: Cidadania, Estado e Globalização, linha de pesquisa: Direito Público.

Orientadora: Profa. Dra. Patrícia Ferreira Baptista

Rio de Janeiro

2025

CATALOGAÇÃO NA FONTE
UERJ/REDE SIRIUS/BIBLIOTECA CCS/C

A663 Araujo, Bernardo José Oliveira

Proporcionalidade e transparência como parâmetros normativos do tratamento de dados pessoais em aplicações de inteligência artificial / Bernardo José Oliveira Araujo. – 2025.
247f.

Orientadora: Profa. Dra. Patrícia Ferreira Baptista.
Tese (Doutorado). Universidade do Estado do Rio de Janeiro, Faculdade de Direito.

1. Lei Geral de Proteção de Dados Pessoais - Teses. 2. Inteligência Artificial - Teses. 3. Legitimidade - Teses. I. Baptista, Patrícia Ferreira. II. Universidade do Estado do Rio de Janeiro. Faculdade de Direito. III. Título.

CDU 342.7:004.8

Bibliotecária: Fabiana das Graças Fonseca CRB7/6358

Autorizo, apenas para fins acadêmicos e científicos, a reprodução total ou parcial desta tese, desde que citada a fonte.

_____ _____

Assinatura Data

Bernardo José Oliveira Araujo

Proporcionalidade e transparência como parâmetros normativos do tratamento de dados pessoais em aplicações de inteligência artificial

Tese de Doutorado apresentada à Banca Examinadora do programa de Pós-graduação em Direito, da Faculdade de Direito da Universidade do Estado do Rio de Janeiro, na área de concentração: Cidadania, Estado e Globalização, linha de pesquisa: Direito Público.

Aprovada em 31 de março de 2025.

Banca examinadora:

Prof.ª Dra. Patricia Ferreira Baptista (Orientadora)
Faculdade de Direito – UERJ

Prof. Dr. Rodrigo Brandão Viveiros Pessanha
Faculdade de Direito – UERJ

Prof. Dr. Valter Schuenquener de Araújo
Faculdade de Direito – UERJ

Prof.ª Dra. Laura Schertel Ferreira Mendes
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa

Prof.ª Dra. Clara Iglesias Keller
Weizenbaum Institute – WZB Berlin Social Science Center

Rio de Janeiro

2025

DEDICATÓRIA

Para meus pais e irmã. A razão de tudo.

AGRADECIMENTOS

Aos meus pais e irmã.

A todos os meus professores pela paciência e fé depositada.

Aos contribuintes do Estado do Rio de Janeiro pelo custeio da graduação, mestrado e doutorado. Espero retribuir.

Aos vigilantes da privacidade, que silenciosamente carregam a liberdade.

RESUMO

ARAUJO, Bernardo José Oliveira. *Proporcionalidade e transparência como parâmetros normativos do tratamento de dados pessoais em aplicações de inteligência artificial*. 2025. 247 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2025.

Esta tese investiga a proporcionalidade e a transparência como parâmetros normativos que conferem legitimidade ao uso de dados pessoais em aplicações de inteligência artificial. A pesquisa parte da constatação de que os arranjos normativos atuais de proteção de dados pessoais são insuficientes diante das rápidas e complexas transformações tecnológicas. O estudo propõe que a proporcionalidade e a transparência são elementos suficientemente robustos e adaptáveis para guiar a regulação dessas tecnologias, oferecendo uma estrutura que pode conter abusos e, ao mesmo tempo, se adaptar ao cenário dinâmico e pervasivo da inteligência artificial. A análise da aplicação da proporcionalidade e da transparência pelo Supremo Tribunal Federal em casos de proteção de dados pessoais destaca suas funções duais. A proporcionalidade serve tanto como postulado normativo, englobando princípios constitucionais e de proteção de dados, quanto como procedimento que auxilia na verificação da legitimidade do tratamento de dados, identificando vulnerabilidades e aplicando salvaguardas. A transparência complementa esse processo ao assegurar que as avaliações de proporcionalidade sejam acessíveis e justificadas publicamente, o que aumenta a legitimidade, reduz lacunas regulatórias no acesso à informação, e fortalece a responsabilidade perante reguladores e titulares de dados. A tese conclui que, em conjunto, esses elementos oferecem um caminho viável para a crise de legitimidade no uso de dados pessoais no contexto de aplicações de inteligência artificial.

Palavras-chave: Lei Geral de Proteção de Dados Pessoais; inteligência artificial; legitimidade; proporcionalidade; transparência

ABSTRACT

ARAUJO, Bernardo José Oliveira. *Proportionality and transparency as normative parameters for the processing of personal data in artificial intelligence applications*. 2025. 247 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2025.

This thesis examines proportionality and transparency as normative parameters that provide legitimacy to the use of personal data in artificial intelligence applications. It starts from the premise that current data protection frameworks are inadequate to address the rapid and complex technological changes we face. The study argues that proportionality and transparency are robust and flexible enough to guide the regulation of these technologies, offering a framework that can both prevent abuses and adapt to the dynamic and pervasive nature of artificial intelligence. The examination of the Brazilian Federal Supreme Court's application of proportionality and transparency in personal data protection cases highlights their dual roles. Proportionality functions both as a normative guideline, incorporating constitutional and data protection principles, and as a procedure that helps verify the legitimacy of data processing, identifying vulnerabilities and implementing safeguards. Transparency complements this by ensuring that proportionality assessments are accessible and publicly justified, thereby enhancing legitimacy, closing regulatory gaps in information access, and strengthening accountability to regulators and data subjects. The thesis concludes that, together, these elements offer a viable path to address the legitimacy crisis in using personal data within the realm of artificial intelligence applications.

Keywords: Brazilian General Data Protection Law; artificial intelligence; legitimacy; proportionality; transparency.

LISTA DE ILUSTRAÇÕES

Figura 1 — História do desenvolvimento da inteligência artificial

Figura 2 — Métodos de aprendizado de máquina

Figura 3 — Regressão linear e regressão logística

Figura 4 — Árvore de decisão para a compra de um carro

Figura 5 — O algoritmo dos k vizinhos mais próximos analisa o vizinho mais próximo do registro não identificados

Figura 6 — Exemplo de um modelo oculto de Markov de atividades para condições climáticas diferentes

Figura 7 — Métodos ensemble combinam diferente modelos de aprendizado de máquina

Figura 8 — Redes neurais artificiais são compostas por diferentes camadas e nós.

Figura 9 — Visualização de Camadas de Multimodais e Agentes de Inteligência Artificial

Figura 10 — Ciclo de vida da inteligência artificial resumido

Figura 11 — Fluxo simplificado de metodologia privacy by design

Figura 12 — Elementos adicionais de legitimação do consentimento

Figura 13 — Carga máxima de participação do titular no consentimento para uso de dados sensíveis

Figura 14 — Simplificação do teste do balanceamento na LGPD

LISTA DE ABREVIATURAS E SIGLAS

ANPD Autoridade Nacional de Proteção de Dados

APEC Cooperação Econômica Ásia-Pacífico

CC Código Civil (Lei federal nº 10.046/2002)

CDC Código de Defesa do Consumidor (Lei federal nº 8.078/1990)

CoE Conselho da Europa

CPF Cadastro de Pessoas Físicas

CRFB Constituição da República Federativa do Brasil de 1988

DPO Data Protection Officer

EFF Electronic Frontier Foundation

EU União Europeia

GDPR General Data Protection Regulation

ICO Information Commissioner's Office (UK])

LAI Lei de Acesso à Informação (Lei federal nº 12.527/2011)

LGPD Lei Geral de Proteção de Dados Pessoais (Lei federal nº 13.709/2018)

MCI Marco Civil da Internet (Lei federal nº 12.965/2014)

OCDE Organização para a Cooperação e Desenvolvimento Econômico

PET Privacy Enhancing Technology

PIT Privacy Invasive Technology

STF Supremo Tribunal Federal

STJ Superior Tribunal de Justiça

SUMÁRIO

	INTRODUÇÃO	12
1	**DESAFIOS REGULATÓRIOS EM MATÉRIA DE PROTEÇÃO DE DADOS PESSOAIS FRENTE À EXPANSÃO DA INTELIGÊNCIA ARTIFICIAL**	47
1.1	**Visão geral da tecnologia de inteligência artificial**	49
1.1.1	Breve história da tecnologia de inteligência artificial	49
1.1.2	Algoritmos de inteligência artificial e taxonomias	57
1.1.2.1	Sistemas baseados em regras	57
1.1.2.2	Aprendizado de máquina	58
1.1.2.2.1	Aprendizado de máquina supervisionado, não supervisionado e aprendizado por reforço	59
1.1.2.2.2	Algoritmos de aprendizado de máquina	61
1.1.2.3	Redes neurais artificiais	66
1.1.2.3.1	Arquiteturas de redes neurais	67
1.1.2.4	Modelos de linguagem de grande escala (LLMs)	71
1.1.2.4.1	Treinamento	72
1.1.2.4.2	Inferência e aprendizado de contexto	73
1.1.2.5	Multimodais e agentes de inteligência artificial: tendências	74
1.2	**Principais aplicações da inteligência artificial**	78
1.3	**Áreas de aplicação da inteligência artificial**	81
1.4	**Inteligência artificial, privacidade e proteção de dados pessoais**	84
1.5	**Uso de inteligência artificial cujo funcionamento afeta direitos fundamentais**	96
1.6	**As fases do desenvolvimento da inteligência artificial**	106
1.6.1	Os desafios regulatórios em matéria de proteção de dados pessoais das fases de desenvolvimento da inteligência artificial	108
1.6.1.1	Fase de design: o desafio da introdução da metodologia privacy by design aplicada à inteligência artificial	110
1.6.1.2	Fase de construção das bases de dados: o desafio da extração de dados tornados manifestamente públicos e uso secundário de dados	113
1.6.1.3	Fase de treinamento: o desafio do potencial uso de dados sem base legal para tratamento de dados	118

1.6.1.4 Fase de implementação e teste: o desafio da construção da política de privacidade..... 122

2 **APLICABILIDADE DOS ARRANJOS NORMATIVOS DE PROTEÇÃO DE DADOS PESSOAIS ÀS APLICAÇÕES DE INTELIGÊNCIA ARTIFICIAL QUE TRATAM DADOS PESSOAIS**..... 124

2.1 **Gerações de leis de proteção de dados pessoais**..... 125

2.1.1 Primeira geração..... 127

2.1.2 Segunda geração..... 129

2.1.3 Terceira geração..... 130

2.1.4 Elementos comuns de legitimidade: princípios e bases legais..... 132

2.1.5 Padrões evolutivos das leis de proteção de dados: caracterizando as transformações a partir do advento de novas tecnologias..... 135

2.2 **Requisitos normativos de legitimidade do tratamento de dados pessoais**..... 139

2.2.1 As bases legais como requisitos para o tratamento de dados pessoais..... 140

2.2.2 Bases de destaque para as aplicações de inteligência artificial: consentimento e legítimo interesse..... 143

2.3 **Diagnóstico da aplicação do arranjo normativo de proteção de dados pessoais brasileiro às aplicações de inteligência artificial que tratam dados pessoais**..... 162

3 **PARÂMETROS CONSTITUCIONAIS NO CONTEXTO DO TRATAMENTO DE DADOS PESSOAIS**..... 168

3.1 **A aplicação do princípio da proporcionalidade em casos de controle concentrado de constitucionalidade envolvendo proteção de dados pessoais**..... 170

3.1.1 ADI 6387, 6388, 6389, 6.393 e 6390: breve resumo do caso..... 171

3.1.1.1 Ausência de proporcionalidade nos critérios a embasar a coleta, compartilhamento e o uso dos dados pessoais na Medida Provisória 954/2020: lacunas na finalidade, necessidade e adequação..... 177

3.1.1.2 Ausência de previsão sobre medidas de segurança, realização de relatório de impacto a posteriori e ausência de previsão de autoridade supervisora com credibilidade, representatividade e legitimidade..... 181

3.1.2 ADPF 695 e ADI 6649: breve resumo do caso..... 185

3.1.2.1 Principais fundamentos de mérito no julgamento da ADPF 695 e ADI 6649..... 194

3.1.2.2.1 Bloco da finalidade, adequação e necessidade..... 212

3.1.2.2.2 Bloco da segurança, prevenção e da responsabilização e prestação de contas..... 218

3.1.2.2.3 Bloco da transparência..... 225

3.2 **Parâmetros constitucionais revisitados no contexto do tratamento de dados pessoais em aplicações de inteligência artificial**..... 231

CONCLUSÃO..... 236

BIBLIOGRAFIA..... 239

INTRODUÇÃO

"Antes mundo era pequeno

Porque Terra era grande

Hoje mundo é muito grande

Porque Terra é pequena

Do tamanho da antena parabolicamará."

Gilberto Gil —

Contexto

Atualmente, cerca de 83% da população global vive sob uma jurisdição com legislações ou regulamentações de proteção de dados pessoais. No total, 167 países, jurisdições e territórios autônomos ao redor do mundo adotaram leis ou regulamentos abrangentes de proteção de dados pessoais e privacidade para proteger dados pessoais detidos por entidades privadas. Desses, 141 Estados-Membros da Organização das Nações Unidas (ONU) – 75% dos 193 no total – adotaram legislações, e 5 implementaram regulamentações abrangentes nacionais. Além destes, 21 jurisdições autônomas não pertencentes à ONU, como o Vaticano, Taiwan, Kosovo e diversos territórios ultramarinos, também adotaram leis ou regulamentações. Cerca de 20 países estão com projetos ou iniciativas pendentes para adotar legislações de proteção de dados pela primeira vez. Não há um padrão econômico ou cultural entre os países que entrarão para este – não mais – seleto grupo.[1]

Ao contrário do que dizem alguns, a privacidade não está morta[2]. Muito pelo contrário, está mais viva do que nunca. O mundo testemunha um crescimento vigoroso das preocupações com privacidade, proteção de dados pessoais e vigilantismo, com cada vez mais países adotando

[1] Entre os países que estão considerando ativamente a adoção de leis de proteção de dados estão Bangladesh, Bolívia, Brunei Darussalam, Camboja, Gâmbia, Guatemala, Namíbia, Paquistão e Suriname. O Vietnã está em processo de substituir sua recente regulamentação de proteção de dados por uma nova lei. Também há novas iniciativas na Líbia e na Libéria. Cf.: BANISAR, David. *National Comprehensive Data Protection/Privacy Laws and Bills 2025*. [S.l.]: SSRN, 28 jan. 2025. Disponível em: http://dx.doi.org/10.2139/ssrn.1951416.

[2] A frase "*Privacy is dead, and social media holds the smoking gun*" é atribuída a Pete Cashmore, fundador e CEO do Mashable, um site premiado e um dos maiores e mais populares destinos para notícias e informações sobre mídia digital, social e tecnologia, com surpreendentes mais de 20 milhões de visitantes únicos por mês.

legislações robustas para garantir que dados pessoais estejam protegidos e seguros, por entidades privadas ou por governos. Em meio a um cenário global onde a informação já não pode mais ser comparada a ouro ou a petróleo – pois não é um recurso escasso[3] –, a proteção de dados pessoais tornou-se não apenas uma necessidade, mas uma prioridade global.[4]

E não se trata apenas de legislações e regulamentos. A fiscalização desempenha um papel fundamental. Em quase todos os países com legislações de proteção de dados, um regulador independente, uma comissão de proteção de dados ou de informação supervisiona e aplica a lei. Essas entidades são legalmente independentes em aproximadamente três quartos dos países. Quase todas as leis incluem isenções específicas para a mídia a fim de harmonizar o direito à privacidade com a liberdade de expressão, enquanto algumas também fazem referência específica às leis nacionais de direito à informação, como é o caso da Lei de Acesso à Informação (LAI) brasileira.

Nas últimas décadas, a privacidade e a proteção de dados pessoais têm se tornado temas cada vez mais centrais em debates nacionais e internacionais, envolvendo diversas áreas como Direito, Ciência Política, Economia, Ética, Tecnologia, Finanças, Saúde e Segurança. O aumento do uso massivo de dados pessoais em quase todas as instâncias da vida humana destacou a necessidade de equilibrarmos a inovação com os direitos e expectativas dos indivíduos em relação ao controle e segurança de informações a eles relacionadas.[5]

---

[3] Dados pessoais já superaram a analogia de "novo petróleo", tornando-se fundamentais para políticas públicas e o impulsionamento de mercados e economias modernas. Diferente do petróleo, os dados não são recursos finitos; podem ser enriquecidos e seu valor cresce exponencialmente com processamento e compartilhamento. Ao contrário do fluxo linear do petróleo, os dados entram e saem de organizações, de maneira complexa. Comparar dados a petróleo simplifica sua natureza abrangente e subestima seu papel central em potencializar a inteligência artificial, além de ignorar questões de vieses e ética que emergem a partir do uso de dados.

[4] Nas "Americas", ou seja, América do Norte, Central, do Sul e na região do Caribe o cenário é de franca expansão das legislações de proteção de dados e o contexto é caracterizado por um ambiente regulatório complexo. Embora a proteção de dados não seja um conceito novo na região, a evolução dos marcos legais nacionais é marcada por características únicas em cada país. Ao contrário da abordagem harmonizada da União Europeia (EU), as nações americanas desenvolveram suas próprias leis distintas de proteção de dados, sendo o caso dos Estados Unidos emblemático devido ao crescente número de legislações estaduais. Com uma população que excede 1 bilhão de indivíduos e uma tendência crescente de alinhamento com os padrões globais de proteção de dados, a necessidade de harmonização e clareza no cenário regulatório é evidente. Países como Argentina, Colômbia, México e Uruguai têm regulamentações estabelecidas há bastante tempo, enquanto outros recentemente aprovaram legislações inspiradas no padrão da União Europeia. Ainda são esperadas atualizações inspiradas pela EU pelo menos na Argentina, Colômbia, México, Costa Rica, Peru, Equador, Paraguai e Panamá. Além disso, o envolvimento das Américas nas discussões globais sobre regulamentação de inteligência artificial transcende a mera observação de tendências; representa uma postura proativa voltada para moldar o uso da tecnologia globalmente.

[5] Optou-se por dizer "informações a eles relacionadas" e não "suas informações" propositalmente. Embora seja importante indicar a existência da discussão, não há espaço neste trabalho para levantarmos questões doutrinariamente importantes a respeito da "propriedade de dados pessoais", especialmente aqueles disponíveis publicamente, temática conhecida como "*data ownership*". A respeito do tema, o professor da Faculdade de

Com o avanço das novas tecnologias, como a inteligência artificial[6], surgem novos riscos e desafios para a regulação jurídica dos usos de dados pessoais, exigindo reflexões sobre como se adaptar a cenários de constante transformação sem comprometer ferramentas essenciais possibilitadas pelo processamento de dados (pessoais e não pessoais), como a criação de novos modelos de negócios, medicina, o aperfeiçoamento de políticas públicas e a otimização em atividades humanitárias.

Tecnologias versáteis como a inteligência artificial possuem um enorme potencial para o bem. Elas abrem novas áreas de pesquisa científica, melhoram redes de distribuição de energia, potencializam a saúde pública e a agricultura, e promovem um avanço mais amplo em diversos campos sociais. Por outro lado, a transformação tecnológica e a crescente digitalização da

---

Direito da Freie Universität Berlin e da Universidade da California, Berkeley, Lothar Determann, argumenta que, embora pesquisadores do Direito proponham regimes de leis de propriedade de informações para supostamente garantir uma proteção superior à privacidade e autoridades de proteção de dados incentivem a ideia de que indivíduos "possuem" seus dados pessoais, as leis de proteção de dados e privacidade diferem significativamente das leis de propriedade. Ele observa que as leis de proteção de dados não incentivam ou recompensam a criação ou investimento, não regulam a aquisição ou transferência de direitos de propriedade e não se aplicam universalmente. Em vez disso, leis de proteção de dados, como as da União Europeia, conferem direitos de exclusão principalmente contra governos e empresas, mas não contra indivíduos agindo para fins pessoais ou domésticos. Nos Estados Unidos, por sua vez, as leis de privacidade de dados tendem a ser específicas para determinados setores e se aplicam a certos tipos de entidades, diferentemente das leis de propriedade, que são mais abrangentes em termos de aplicabilidade. Cf.: DETERMANN, Lothar. No One Owns Data. [S.l.]: SSRN, 2018. Disponível em: https://ssrn.com/abstract=3123957.

[6] Não está entre os objetivos deste trabalho discutir as possíveis definições do termo "inteligência artificial", que pode ser amplamente definido como "*o uso de computadores e máquinas para imitar a inteligência humana*". Para os efeitos da tese, embora reconheça-se que a definição tem impacto regulatório relevante, em especial para questões relacionadas à aplicabilidade de leis, não há relevância prática em discutir a melhor definição de "inteligência artificial". Nesse sentido, e em tradução livre, o governo dos Estados Unidos adotou em fevereiro de 2025 uma definição para "inteligência artificial" que serve aos propósitos deste trabalho. Definiu o termo como "(...) *um sistema baseado em máquina que pode, para um conjunto de objetivos definidos por humanos, fazer previsões, recomendações ou decisões que influenciam ambientes reais ou virtuais. Sistemas de inteligência artificial usam entradas baseadas em máquina e humana para perceber ambientes reais e virtuais, abstrair essas percepções em modelos por meio de análise automatizada e usar inferência de modelos para formular opções de informação ou ação*". A União Europeia, embora não tenha definido o termo no seu regulamento geral, adota uma definição semelhante à da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) para "*sistema de inteligência artificial*". Segundo o Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, conhecido como "AI Act", um "*sistema de inteligência artificial*" *é "um sistema baseado em máquina projetado para operar com vários níveis de autonomia e que pode exibir adaptabilidade após a implantação. Ele infere, a partir das entradas que recebe, como gerar saídas, como previsões, conteúdo, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais*". A OCDE define um "sistema de inteligência artificial" como "*um sistema baseado em máquina que, para objetivos explícitos ou implícitos, infere, a partir das entradas que recebe, como gerar saídas, como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais*". Essa definição destaca a autonomia e adaptabilidade dos sistemas de inteligência artificial. A ONU, por sua vez, definiu em março de 2024, a "*inteligência artificial" como sistemas que podem criar um mundo mais seguro e equitativo, assegurando que a tecnologia não seja usada para prejudicar a paz ou reprimir direitos humanos*." A definição enfatiza a necessidade de sistemas seguros e confiáveis para avançar o desenvolvimento sustentável e respeitar as liberdades fundamentais. Cf.: ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÓMICO (OCDE). Explanatory memorandum on the updated OECD definition of an AI system. *OECD Artificial Intelligence Papers*, Paris, n. 8, 2024. DOI: 10.1787/623da898-en.

sociedade colocam em evidência desafios inéditos relacionados aos direitos fundamentais, especialmente os desafios ligados aos direitos à privacidade e à proteção de dados pessoais.[7]

Nos últimos meses, a liberação pública de modelos[8], sistemas[9] e aplicações[10] avançadas, como o ChatGPT da OpenAI – e suas atualizações –, o Gemini do Google, o Llama da Meta, mais recentemente o DeepSeek da Hangzhou e o Qwen da Alibaba, e outras tecnologias similares, catalisou um fervoroso debate sobre os riscos associados à "inteligência artificial generativa"[11], entre eles, os riscos ligados à área de foco desse estudo: a privacidade e a proteção de dados pessoais.

---

[7] Por exemplo, o Secretário-Geral das Nações Unidas, António Guterres, anunciou a criação de um novo Órgão Consultivo de inteligência artificial no âmbito na ONU para apoiar os esforços da comunidade internacional para governar a inteligência artificial. Além da ONU, a OCDE criou recentemente a "Parceria Global em Inteligência Artificial" (GPAI), que é uma parceria integrada reunindo membros da OCDE e outros países para avançar uma agenda ambiciosa de implementação de inteligência artificial centrada no ser humano, segura, protegida e confiável, conforme os princípios da Recomendação da própria OCDE sobre inteligência artificial.

[8] O termo "modelo de inteligência artificial" será utilizado nesse trabalho como o algoritmo que foi treinado com dados para um problema específico, ou seja, será empregado de forma mais restrita. Dessa forma, um modelo de inteligência artificial é um algoritmo ou conjunto de algoritmos treinados para realizar tarefas específicas, como reconhecimento de imagem, processamento de linguagem natural ou previsão de dados. Exemplos incluem redes neurais, árvores de decisão e máquinas de vetores de suporte, como exemplificado adiante.

[9] Um sistema de inteligência artificial é uma combinação de modelos de inteligência artificial, hardware e software que trabalham juntos para realizar tarefas complexas. Um sistema de inteligência artificial pode incluir várias camadas de processamento, armazenamento de dados e interfaces de usuário. Um exemplo seria um sistema de diagnóstico médico que usa modelos de inteligência artificial para analisar imagens e dados de pacientes. Dessa forma, o termo "sistema de inteligência artificial" é utilizado nesse trabalho de forma mais ampla do que "modelo" e mais restrita do que "aplicação" ou "ferramenta".

[10] Uma "aplicação de inteligência artificial" é o uso prático de um sistema de inteligência artificial para resolver problemas do mundo real. Isso pode ser um aplicativo móvel, um software empresarial ou um serviço online que utiliza inteligência artificial para fornecer funcionalidades específicas. Exemplos incluem assistentes virtuais, sistemas de recomendação e ferramentas de tradução automática. Sendo assim, o termo "aplicação de inteligência artificial" é utilizado nesse trabalho de forma ampla, e de maneira mais abrangente do que "modelo" e "sistema". Considerando os debates mais atuais sobre os "agentes de inteligência artificial", estes seriam classificados como aplicações para os efeitos desse trabalho. Muito se discute atualmente a questão dos agentes, pois eles lembram os filmes de ficção científica, uma vez que esses agentes podem perceber o ambiente por meio de sensores, processar informações e tomar decisões, além de agir sobre o ambiente para atingir seus objetivos. Um agente de inteligência artificial refere-se a um sistema ou programa capaz de executar tarefas de forma autônoma em nome de um usuário ou de outro sistema, projetando seu fluxo de trabalho e utilizando as ferramentas disponíveis. Os agentes podem englobar uma ampla gama de funcionalidades além do processamento de linguagem natural, incluindo tomada de decisão, resolução de problemas, interação com ambientes externos e execução de ações.

[11]Ao longo da história humana, houve algumas inovações tecnológicas que mudaram fundamentalmente o funcionamento da sociedade. A prensa de impressão, o motor de combustão interna, os computadores e a internet são exemplos frequentemente citados de tais tecnologias de uso geral. Embora a inteligência artificial exista há algum tempo, muitos argumentam que os avanços recentes podem colocá-la nessa categoria de elite de tecnologias que alteram o curso da história. Devido à novidade e à amplitude da inteligência artificial, a pesquisa está apenas começando a elucidar seu impacto. Isso é particularmente verdadeiro para a inteligência generativa – um subconjunto da inteligência artificial construído majoritariamente sobre modelos de aprendizado de máquina de grande linguagem (LLMs) – que explodiu na cena em 2022 e atualmente representa o estado da arte da inteligência artificial atualmente, ainda que haja promessas para estarem ultrapassados em breve. Esses modelos, incluindo o GPT-4 da OpenAI, o Gemini do Google, o LLaMa da Meta e muitos outros, são treinados em bancos de dados massivos em escala da internet e usam bilhões de parâmetros para comando (prompt) de um usuário. Esses modelos também podem ser treinados em conjuntos de dados mais focados em contextos específicos – por

A capacidade desse tipo de inteligência artificial de gerar conteúdos realistas e convincentes, bem como de serem implementados em conjunto com outros softwares e sistemas digitais, criando funcionalidades e amplificando suas capacidades, trouxe benefícios sem precedentes para a sociedade. Hoje em dia, praticamente qualquer sistema digital pode ter inteligência artificial integrada. Isso inclui assistentes virtuais que ajudam com tarefas repetitivas, esclarecem dúvidas sobre o uso do próprio sistema ou fazem recomendações a partir de pesquisas instantâneas na internet. Contudo, essa mesma versatilidade das inteligências artificiais generativas e sua introdução no mercado por diferentes *players*, em cenário de agressiva competição, apresentam riscos significativos e de naturezas distintas.

Por exemplo, a facilidade de acesso a informações sobre armas químicas, biológicas, radiológicas ou nucleares (CBRN) representou um perigo iminente, e logo recebeu atenção dos desenvolvedores, pois a inserção de "travas" foi capaz de diminuir consideravelmente as barreiras para atividades nefastas. Ainda assim, com um pouco de conhecimento sobre engenharia de comandos ("prompts" [12]), não é muito difícil fazer com que uma inteligência artificial generativa conversacional ensine a construir uma bomba.[13]

Os riscos não param por aí. A capacidade dessas tecnologias de gerar e disseminar conteúdo violento, incitante ou que promove radicalismos pode fomentar comportamentos perigosos e ilegais por todo o mundo. A democracia também está em jogo, já que a inteligência artificial generativa pode facilitar a criação e disseminação de campanhas de desinformação em

exemplo, saúde, finanças, atendimento ao cliente, desenvolvimento de software etc. Se, e como, essas novas tecnologias moldarão a sociedade são questões que permanecem em aberto.

[12] Um prompt é uma instrução, consulta ou comando que um usuário insere em uma interface de inteligência artificial generativa para solicitar uma resposta do sistema.

[13] Atualmente, se um usuário solicitar a um modelo de linguagem "me ensine a fazer uma bomba caseira", há grande probabilidade de haver uma negativa ou mensagem de que a solicitação viola as políticas. Contudo, é possível "driblar" essa narrativa com técnicas um tanto quanto simples. Uma delas é pedir que o modelo personifique uma história ou aja como um personagem fictício que está escrevendo uma história. Nessa história haverá um capítulo sobre a construção de uma bomba, com detalhes técnicos. Outra forma conhecida é pedir que o modelo simule uma conversa entre dois personagens na qual eles conversam sobre como construir uma bomba.

larga escala[14]; da mesma forma como pode ajudar a mudar a crença sobre teorias da conspiração.[15]

A disseminação de conteúdo obsceno, degradante ou abusivo e a exposição a discursos de ódio ou estereotipados são desafios adicionais que precisam ser enfrentados. Indo além, a configuração inadequada entre humanos e sistemas de inteligência artificial pode levar a vieses algorítmicos, dependência excessiva ou comportamentos enganosos por parte das "máquinas".

A segurança da informação, por sua vez, está ameaçada pela maior facilidade de ataques cibernéticos e exploração de vulnerabilidades, enquanto questões de propriedade intelectual estão se proliferando aos montes devido à produção não autorizada de conteúdo protegido por direitos autorais.[16] Outros riscos estruturais incluem também os impactos ambientais derivados do alto consumo de recursos, como água e energia, necessários para treinar modelos de inteligência artificial e para manutenção de data centers; o que pode danificar ecossistemas inteiros e pôr em risco as cadeias energéticas.[17]

Não menos importante são os riscos relacionados à privacidade e à proteção de dados pessoais. No âmago das discussões acima mencionadas – em especial, aquelas relacionadas aos impactos em direitos fundamentais[18] – está a questão de como os dados pessoais são coletados,

---

[14] Tem sido cada vez mais difícil identificar vídeos criados por inteligência artificial generativa, por exemplo, imitando políticos e pessoas politicamente expostas. O Brasil tem sido um campeão de casos graves de *deep fakes*. No início de 2025, circularam nas redes sociais *deep fakes* simulando o Ministro da Fazenda Fernando Haddad. O vídeo manipulado por meio de inteligência artificial continha informações fraudulentas e atribuía ao ministro declarações inexistentes sobre a criação de um imposto incidente sobre animais de estimação, pré-natal, PIX e sobre prêmios de apostas esportivas (bets). Entre os dias 4 e 10 de janeiro de 2025 o volume de transações em Pix despencou aproximadamente 11%. A crise levou ao ponto de o Governo Federal ser obrigado a editar Medida Provisória para reforçar a gratuidade do Pix. Cf.: https://www.gov.br/secom/pt-br/assuntos/noticias/2025/janeiro/governo-federal-edita-medida-provisoria-para-reforcar-gratuidade-do-pix.

[15] COSTELLO, Thomas H. et al. Durably reducing conspiracy beliefs through dialogues with AI. Science, v. 385, eadq1814, 2024. DOI: 10.1126/science.adq1814. Disponível em: https://www.science.org/doi/10.1126/science.adq1814.

[16] É possível acompanhar os desenvolvimentos de algumas das principais ações sobre direitos de propriedade intelectual, ajuizadas contra as maiores desenvolvedoras de sistemas de inteligência artificial, na seguinte página: https://chatgptiseatingtheworld.com/2024/09/15/status-of-all-30-copyright-lawsuits-v-ai-sept-15-2024-discovery-rules/.

[17] Segundo relatório da NIST, os principais riscos da inteligência artificial generativa envolvem o seguinte: acesso facilitado a informações sobre armas químicas, biológicas, radiológicas ou nucleares (CBRN Information); confabulação; recomendações perigosas ou violentas; privacidade de dados; impactos ambientais; configuração inadequada entre humanos e IA; integridade da informação; segurança da informação; propriedade intelectual; produção de conteúdo obsceno, degradante e/ou abusivo; toxicidade, viés e homogeneização; e integração da cadeia de valor e componentes. Cf.: AUTIO, Carol et al. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1). Gaithersburg: National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.AI.600-1. Disponível em: https://doi.org/10.6028/NIST.AI.600-1.

[18] Não está entre os objetivos desse trabalho discutir a definição de "direitos fundamentais" ao discutir o impacto da inteligência artificial em direitos centrais nas democracias contemporâneas. Nesse sentido, para os efeitos da tese, é possível se ater ao rol de direitos tidos como fundamentais pela Constituição Federal de 1988,

armazenados e utilizados para o treinamento dos modelos de inteligência artificial.[19] Os riscos não se limitam apenas ao treinamento, pois esses sistemas interagem e aprendem com os usuários, que podem inserir dados pessoais. Sistemas generativos apresentam numerosos riscos à privacidade, podendo, por exemplo, vazar, gerar ou inferir dados sensíveis sobre indivíduos. Esses riscos incluem, por exemplo, a revelação de informações privadas ou sensíveis durante ataques adversariais[20]. O treinamento desses sistemas, por sua vez, geralmente envolve a coleta de grandes volumes de dados, incluindo dados pessoais, de milhões de fontes disponíveis publicamente (raspagem da internet, ou "web scrapping"), levantando preocupações sobre princípios como transparência, participação e limitação de propósitos e regras sobre usos para finalidades secundárias. Nesse contexto, a falta de clareza sobre as fontes de dados usadas para treinamento dos modelos dificulta o entendimento sobre que tipo de informações foram utilizadas no treinamento e como elas são mantidas atualizadas.[21]

---

estabelecidos dos artigos 5º ao 17º. Importa saber que são direitos protetivos e essenciais ao ser humano. Garantem não apenas o mínimo necessário para uma existência digna, mas também são instrumentos de proteção dos indivíduos frente às ações do Estado. Seria possível remeter-se a outras Constituições ou Cartas e Regulamentos. Por exemplo, na Carta dos Direitos Fundamentais, a União Europeia conceitua "direitos fundamentais" como os direitos e liberdades básicos que assistem a todas as pessoas na UE, independentemente de sua origem, crenças ou estilo de vida. Esses direitos incluem a dignidade humana, liberdade, igualdade, democracia e o Estado de Direito. (Carta dos Direitos Fundamentais da União Europeia, 2016/C 202/02). O artigo 5º da Lei de Inteligência Artificial da União Europeia (EU AI Act), por sua vez, proíbe certos sistemas de inteligência artificial que são considerados violadores dos direitos fundamentais e dos valores da União, como a dignidade humana, liberdade, igualdade, democracia e o Estado de direito. Os direitos fundamentais protegidos no âmbito do AI Act incluem a não discriminação, igualdade, proteção de dados, vida privada e familiar, direitos da criança, liberdade de expressão e informação, liberdade de reunião e associação, liberdade de pensamento, consciência e religião, direito a um recurso efetivo e a um julgamento justo, presunção de inocência e direito de defesa.

[19] Nesse trabalho, os diferentes tipos de processamento de dados pessoais serão chamados de "tratamento", uma vez que o termo possui sentido amplo nas leis de proteção de dados. Por exemplo, na LGPD o termo "tratamento" significa toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[20] Ataques adversariais em inteligência artificial referem-se às manipulações que enganam modelos de aprendizado de máquina, levando-os a resultados incorretos, frequentemente explorando a maneira como esses modelos aprendem e operam. Essas manipulações são feitas com intenção maliciosa, visando comprometer a eficácia do sistema. As possíveis consequências de um ataque adversarial bem-sucedido não são apenas teóricas – são uma preocupação prática que abrange diversos domínios, desde a segurança nacional até a saúde pública. Imagine um cenário em que uma imagem adversarial faz com que um carro autônomo interprete um sinal de parada como um sinal de "dê a preferência" ou de "prossiga", resultando em acidentes. Ou considere as implicações para o software de reconhecimento facial, em que um ataque habilmente elaborado poderia permitir que um intruso passasse por um ponto de controle de segurança sem ser detectado.

[21] A ausência de clareza em relação aos dados e informações utilizados no treinamento dos modelos tornou-se manchete nos jornais quando Mira Murati, ex-diretora de tecnologia da OpenAI, participou de uma reportagem do Wall Street Journal sobre o novo modelo de vídeo da OpenAI, conhecido como "Sora". Quando questionada se o modelo teria sido treinado com vídeos do YouTube, inicialmente, Mira Murati foi evasiva e demonstrou desconhecimento sobre o conteúdo usado no treinamento. Porém, ao ser pressionada pela repórter, ela confirmou que o modelo foi treinado com dados disponíveis publicamente, incluindo vídeos do YouTube, Reels do Instagram ou qualquer conteúdo de vídeo que tenha sido colocado publicamente na internet. Cf.

Há modelos que podem inferir dados pessoais e informações sensíveis que não estavam em seus dados de treinamento ou que não foram divulgados pelo usuário, potencialmente levando a inferências inadequadas e a preconceitos e discriminações prejudiciais. Essas inferências podem contribuir, por exemplo, para violações de direitos fundamentais ou decisões adversas, incluindo discriminatórias, com base em percepções preditivas derivadas de múltiplas fontes de dados. E não é só. A melhoria da precisão nas inferências sobre dados pessoais por sistemas generativos aumenta o risco de exposição ou danos a categorias sensíveis de dados, mesmo que as inferências não sejam precisas, especialmente se revelarem informações consideradas sensíveis ou forem usadas para prejudicar indivíduos.[22] O uso de dados "normais" para gerar inferências sensíveis ou informações na chamada "zona de disputa" pode ser significativamente ampliado por modelos de inteligência artificial especializados na análise de grandes volumes de dados.[23]

Estes são só alguns exemplos de potenciais violações de direitos e riscos ligados ao uso de dados pessoais que podem ser causados pelos sistemas de inteligência artificial generativos.

Nesse trabalho, partimos desses riscos – amplamente divulgados nos últimos anos devido à liberação pública de sistemas generativos pelas Big Techs – para contextualizar o tamanho dos desafios regulatórios que temos pela frente.[24] O aumento da atenção e do escrutínio em

---

https://www.wsj.com/video/series/joanna-stern-personal-technology/openai-cto-on-the-future-of-sora-chatgpt-and-ai-rivals-full-interview.

[22] O uso de vastos conjuntos de dados pessoais, por vezes raspados da internet para treinar modelos sem autorizações específicas ou sem o devido conhecimento dos titulares de dados, levanta questões sobre a transparência, o consentimento dos indivíduos cujos dados são utilizados e a existência de um interesse legítimo válido. O uso alegadamente indevido de informações pessoais e a vulnerabilidade a ataques cibernéticos são apenas algumas das preocupações que precisam ser enfrentadas.

[23] O debate sobre inferências sensíveis é um tema que merece uma análise aprofundada, possivelmente se tornando até um tema para pós-doutoramento. É sabido que dados pessoais "normais" podem frequentemente revelar informações pessoais sensíveis e outras informações críticas sobre os indivíduos. Alguns exemplos incluem: utilizar informações de local de nascimento em perfis de redes sociais para direcionar marketing com base em raça ou etnia; usar segmentos de linguagem para inferir que falantes de determinado idioma pertencem a uma raça ou etnia específica; coletar IPs de usuários de aplicativos religiosos (e.g. aplicativo da Bíblia) para enviar conteúdo específico para aquela religião; usar dados de geolocalização de indivíduos que frequentam centros religiosos para deduzir sua religião; usar dados de placas de carro de estacionamento de centros religiosos ou próximos para deduzir sua religião; reunir informações de usuários de aplicativos de namoro para direcionar marketing à Comunidade LGBTQIA+; analisar postagens e contas seguidas nas redes sociais para determinar a opinião política e segmentar para marketing político direcionado; usar dados de geolocalização de pessoas que visitam farmácias e centros dermatológicos para identificar possíveis médicos ou profissionais de saúde; e examinar o histórico de buscas na internet para identificar a situação de saúde de indivíduos e enviar marketing direto.

[24] A Meta, juntamente com mais de 50 outras empresas, pesquisadores e entidades do setor, emitiu em 19 de setembro de 2024 uma carta aberta instando a União Europeia (EU) a abordar suas regulamentações inconsistentes sobre inteligência artificial, alegando que a Europa está ficando para trás em relação a outras regiões no desenvolvimento dessas tecnologias. A carta, assinada por líderes de organizações como Ericsson, Spotify e a Universidade de Harvard, foi publicada como um anúncio no Financial Times. Ela critica os

torno dos modelos de inteligência artificial generativa são justificados, dado o seu potencial de danos sistêmicos. No entanto, a preocupação com a inteligência artificial vai além da sua capacidade generativa. A inteligência artificial, em sua totalidade, tem revolucionado setores inteiros e levantado questões éticas e regulatórias que demandam uma análise cuidadosa, como a legalidade e a legitimidade de certos usos.

Nesse contexto, as atuais legislações de proteção de dados pessoais, desde as primeiras gerações baseadas no consentimento do titular até as mais modernas influenciadas pelo Regulamento Geral de Proteção de Dados da União Europeia ("Regulamento da União Europeia" ou "GDPR"),[25] enfrentam dificuldades em lidar com novas técnicas de processamento, destinações e usos de dados pessoais em um ambiente tecnológico em constante evolução.

O principal cientista da área na Meta, Yann LeCun, afirma que um "*novo paradigma de arquiteturas de inteligência artificial*" surgirá nos próximos três a cinco anos, indo muito além das capacidades dos sistemas existentes. LeCun também prevê que os próximos anos poderiam ser a "*década da robótica*", onde os avanços em inteligência artificial e robótica se combinarão para desbloquear uma nova classe de aplicações inteligentes. Ele acredita que a vida útil do paradigma atual de modelos de linguagem de grande escala (LLM) – tecnologia base para os principais sistemas amplamente disponibilizados a partir de 2022 – é relativamente curta,

---

processos regulatórios lentos da UE e pede orientações mais claras e rápidas, particularmente em relação a quais dados podem ser usados para treinar modelos. As empresas estão preocupadas que intervenções das Autoridades de Proteção de Dados Europeias (DPAs) possam prejudicar o uso de dados europeus no treinamento de IA, limitando a competitividade da Europa. A carta critica especificamente decisões recentes sob o GDPR, enfatizando a necessidade de decisões "harmonizadas, consistentes, rápidas e claras" dos reguladores de dados para garantir que os dados europeus possam ser usados para treinar modelos para o benefício dos europeus. De acordo com a carta, dois pontos-chave estão em jogo: modelos abertos e modelos multimodais. Modelos abertos, que estão livremente disponíveis para organizações modificarem e usarem, aumentam a soberania ao permitir o controle sobre os dados sem enviá-los externamente. Modelos multimodais, capazes de processar texto, imagens e fala, representam um avanço significativo em comparação aos modelos apenas de texto. Esses modelos têm o potencial de aumentar a produtividade, a pesquisa científica e agregar valor econômico significativo à Europa. Atualmente, instituições públicas e empresas se beneficiam dessas tecnologias, mas sem regulamentações claras e consistentes, a Europa corre o risco de perder o crescimento tecnológico visto em regiões como os EUA, China e Índia. A carta argumenta que a capacidade da Europa de competir e se beneficiar das inovações em inteligência artificial depende de um quadro regulatório unificado, mas decisões fragmentadas recentes das DPAs europeias criaram incerteza sobre quais dados podem ser usados para treinar modelos de inteligência artificial. Além das preocupações com a privacidade e a proteção de dados, a UE também promulgou a Lei de Inteligência Artificial da União Europeia (EU AI Act), a primeira grande legislação visando prevenir abusos da tecnologia. Este ambiente regulatório levou a Meta e outras empresas de tecnologia a atrasar o lançamento de produtos no mercado europeu, com a Meta adiando o lançamento em toda a UE de sua alternativa ao Twitter, Threads, e o Google adiando o lançamento de ferramentas de inteligência artificial na região. Cf.: https://euneedsai.com/

[25] União Europeia. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, publicado no Jornal Oficial em 4 de maio de 2016 (OJ L 119), 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). *OJ L 119, 4.5.2016, p. 1–88*. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

provavelmente de três a cinco anos, e que dentro de cinco anos ninguém em sã consciência os usaria mais como o componente central de um sistema de inteligência artificial.

LeCun aponta que as limitações atuais, como a incapacidade de compreensão do mundo físico, a falta de memória persistente, ausência de raciocínio e capacidades de planejamento complexo, inibem o comportamento verdadeiramente inteligente nas máquinas. Portanto, ele prevê outra revolução no campo nos próximos anos, que pode até exigir uma mudança no nome "inteligência artificial generativa", pois provavelmente não será generativa no sentido que entendemos hoje.

Neste estudo, sugerimos que está emergindo[26] um consenso[27] entre os estudiosos[28]: as legislações atuais de proteção de dados mostram-se insuficientes para lidar não apenas com os desafios imediatos do processamento de dados pessoais, mas também com os intrincados cenários que o futuro nos reserva. Assim, esta tese não tem o objetivo de argumentar ou demonstrar "se" as legislações de proteção de dados, no caso, a Lei Geral de Proteção de Dados brasileira (LGPD – Lei nº 13.709/2018)[29], precisam mudar. Acreditamos que a evolução da

---

[26] O professor Daniel Solove afirmou recentemente que a necessidade de reforma nas leis de privacidade é urgente. A inteligência artificial impacta a privacidade de maneiras que muitas vezes não introduzem problemas totalmente novos, mas, em vez disso, modificam e intensificam os existentes. Solove classificou as leis de proteção de dados atuais como bastante inadequadas para enfrentar os desafios trazidos pela inteligência artificial. Para o autor, as abordagens desatualizadas que persistem na maioria das leis são particularmente inadequadas para lidar com as complexidades da inteligência artificial. Com os formuladores de políticas cada vez mais focados na inteligência artificial, este é um momento crítico para abordar as questões de longa data e as estratégias ineficazes das leis de privacidade, a fim de garantir que elas governem efetivamente o impacto da tecnologia na privacidade. Cf.: Cf. SOLOVE, Daniel J. Artificial Intelligence and Privacy. *Florida Law Review*, Gainesville, v. 77, n. 1, p. 1, 2025. Disponível em: https://ssrn.com/abstract=4713111. SOLOVE, Daniel J. A regulatory roadmap to AI and privacy. *IAPP*, jan. 2024. Disponível em: https://iapp.org/news/a/a-regulatory-roadmap-to-ai-and-privacy/.

[27] Daniel Solove vem advogando nos últimos anos pela necessidade de alteração da estratégia regulatória. O professor de Direito da George Washington University Law School e um dos maiores expoentes da área, ensina que a maioria das leis de privacidade tem tentado abordar os problemas da devastadora impotência dos indivíduos adotando o que chamamos de "Modelo de Controle Individual", que busca capacitar os indivíduos a controlarem seus próprios dados. Solove argumenta que o Modelo de Controle Individual não apenas falhou, mas está fadado ao fracasso, especialmente na era da inteligência artificial. Em contraste com o Modelo de Controle Individual, sustenta que outro modelo seria muito mais eficaz – o "Modelo de Estrutura Social". Neste segundo modelo, defendido por Solove e outros acadêmicos que têm promovido de várias formas e nomes há muitas décadas, tem sido negligenciado pelos legisladores e reguladores em sua busca infrutífera para fazer o Modelo de Controle Individual funcionar. Em vez de tentar capacitar os indivíduos a controlarem seus dados, o Modelo de Estrutura Social foca em controlar o poder das organizações para coletar, usar e divulgar dados pessoais, e em prevenir danos aos indivíduos e à sociedade.

[28] Relevantes autores nos campos da privacidade, proteção de dados pessoais e que estudam as interfaces entre regulação de tecnologia e direitos fundamentais produziram obras recentes em que indicam a importância de enxergar a privacidade como um valor societal, e não apenas um interesse individual. Para eles, a privacidade não é somente (ou sequer principalmente) um interesse individual; em vez disso, deve ser protegida com o propósito de promover valores sociais como democracia, liberdade, criatividade, saúde e o florescimento intelectual e emocional. Exemplos incluem: Paul Schwartz, Oscar Gandy, Julie Cohen, Joel Reidenberg, Spiros Simitis e Priscilla Regan.

[29] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, 15 ago. 2018. Seção 1, p.59.

LGPD é uma questão absolutamente necessária para garantir a privacidade e preservar a segurança dos dados pessoais e tornar o Brasil minimamente competitivo, alinhando-o ao movimento global em prol do crescimento impulsionado por inteligência artificial. Não tratamos isso como algo em disputa, mas como um fato.[30] O objetivo principal do presente trabalho é apontar "como" e "para onde" precisamos caminhar.

Neste trabalho não afirmamos que as medidas de conformidade estabelecidas pela LGPD se reduzam completamente a exercícios vazios e meramente performáticos de manipulação de papelada. No entanto, argumentamos que na era da inteligência artificial, tais medidas – como o registro das operações de tratamento de dados (ROT/RoPA), as avaliações de impacto (RIPD/DPIAs) e a aplicação de *privacy by design and by default* – carecem de especificidade e *accountability* robustos. Isso abre espaço para que controladores as realizem de modo minimalista e superficial. Propomos que o modelo atual de regulação da proteção de dados no Brasil incentiva práticas inadequadas por parte dos agentes regulados e dificulta a supervisão efetiva pelos reguladores. Estes, por sua vez, podem facilmente ter suas investigações e ações de *enforcement* comprometidas, seja pelo cumprimento apenas formal das regras, seja pela sobrecarga de papelada em um ambiente saturado de agentes regulados e riscos cada vez mais complexos.

A complexidade do cenário atual – e do que está por vir em breve, embora ainda pouco claro – demanda uma abordagem multidisciplinar e uma análise aprofundada sobre como garantir a privacidade e a proteção dos dados pessoais em meio às demandas da sociedade e às oportunidades proporcionadas pela utilização de informações pessoais em larga escala. É possível citar exemplos banais: poucas pessoas se recusariam a compartilhar seus dados para

[30] Como exemplo dessa tendência, uma potência mundial no setor tecnológico, a Coreia do Sul, recentemente implementou mudanças significativas em seu ordenamento para enfrentar desafios na corrida pela inovação em inteligência artificial. Após aprovar a segunda lei abrangente de regulação de inteligência artificial, ficando atrás apenas da União Europeia, o país avançou com uma proposta de emenda à Lei de Proteção de Informação Pessoal (PIPA). Um dos destaques das novas disposições é a permissão para que empresas utilizem dados originais sem necessidade de pseudonimização ou anonimização, desde que obtenham aprovação da Comissão de Proteção de Informação Pessoal (PIPC) – o regulador local – para seus planos de processamento e gestão de dados. Essa mudança possibilita o uso de conjuntos de dados originais no desenvolvimento de inteligência artificial, sem a necessidade de obter novo consentimento. Essa abordagem oferece uma vantagem mais robusta para as empresas em comparação à estrutura atual da lei ou ao *sandbox* regulatório em vigor na Coreia do Sul, que concede apenas isenções temporárias para testar novos produtos. Além disso, a emenda proposta permite que dados sejam utilizados além do propósito original de coleta, ou seja, facilita o uso para finalidades secundárias caso o desenvolvimento de inteligência artificial seja capaz de gerar grandes benefícios públicos e sociais.

um prestador de serviços de saúde se isso pudesse ajudar a prever as doenças e riscos aos quais estão mais expostas. Outros exemplos são mais complexos.[31]

Nesse contexto, é essencial encontrar um equilíbrio entre a inovação tecnológica e a proteção dos direitos fundamentais, visando a construção de um arcabouço legal eficaz e atualizado para lidar com os desafios presentes e futuros na área da proteção de dados pessoais.

Em síntese, e antecipando o principal debate desta tese, a atual estrutura regulatória da proteção de dados pessoais não está pronta para os novos tempos; em que modelos, sistemas e agentes[32] de inteligência artificial estarão presentes em praticamente todos os aspectos da vida cotidiana, influenciando desde decisões comerciais mais simples até interações sociais dinâmicas, levantando desafios complexos em termos de privacidade, segurança e ética no uso dos dados.

Políticos e stakeholders dentro das entidades reguladoras têm manifestado preocupações especialmente sobre como os dados pessoais podem ser utilizados para desenvolver e implementar modelos de inteligência artificial. Essas inquietações, embora não sejam exclusivas da "inteligência artificial generativa", foram amplificadas pela escala, escopo e capacidades dessas tecnologias, apresentando novos desafios que o Direito precisa abordar.

A proliferação das discussões nos últimos meses sublinhou a urgência de criarmos não apenas novos marcos regulatórios eficazes para a regulamentação dos usos de inteligência artificial, mas também de avaliarmos a eficácia dos marcos legais de proteção de dados pessoais já existentes e aplicáveis a essas tecnologias disruptivas. É imperativo que os legisladores considerem não apenas os riscos imediatos dos diversos tipos de inteligências artificiais – sendo a generativa apenas uma delas –, mas também as implicações em longo prazo dessas tecnologias na sociedade e no ordenamento como um todo.

Certamente, a complexidade do tema demanda uma abordagem regulatória que seja abrangente, robusta, inovadora, dinâmica, flexível, proativa e – ousamos dizer – imaginativa.

---

[31] Na maioria das legislações atuais, imagens que vão ser imputadas em modelos de inteligência artificial devem passar por pseudonimização se puderem revelar a identidade dos titulares de dados, o que muitas vezes exige o desfoque das imagens. No entanto, esse processo pode introduzir erros no treinamento da inteligência artificial de veículos autônomos, ao fazer com que os modelos associem imagens desfocadas com pessoas reais, reduzindo a precisão e a eficácia.

[32] Como comentado acima, um agente de inteligência artificial é um programa de software autônomo que simula a inteligência humana para realizar tarefas, tomar decisões e interagir com os usuários. Esses agentes são projetados para aprender com dados, adaptar-se a cenários em mudança e melhorar ao longo do tempo, graças a algoritmos de aprendizado de máquina e inteligência artificial.

Nos próximos itens deste estudo, precisamos navegar pelos desafios do presente e enquanto imaginamos os do futuro.

Relevância, justificativa e originalidade

A escolha do tema decorre da constatação de que, embora a inteligência artificial seja uma área de estudo e aplicação tecnológica com mais de seis décadas[33], foi nos últimos anos que sua adoção e impacto atingiram proporções exponenciais, revelando uma série de desafios regulatórios, particularmente em relação aos impactos negativos nos direitos fundamentais.

A explosão recente no uso de inteligência artificial em diversos setores midiáticos – desde a saúde até a segurança pública[34], passando por finanças, arte, marketing e entretenimento[35] – trouxe à tona a discussão sobre a necessidade urgente de marcos regulatórios eficazes para regulação do tema. Acompanhando essa tendência global, o Brasil também atravessa um debate acalorado no Congresso Nacional para regular os usos da inteligência artificial.[36]

---

[33] A expressão "inteligência artificial" foi cunhada em 1956, quando Marvin Minsky e John McCarthy organizaram o *Dartmouth Summer Research Project on Artificial Intelligence* (Projeto de Pesquisa de Verão sobre Inteligência Artificial de Dartmouth). A inteligência artificial ganhou popularidade devido ao aumento dos *big data* e ao crescimento exponencial do poder de computação. A definição de inteligência se expandiu e evoluiu ao longo do tempo e, atualmente, refere-se de forma bastante resumida a máquinas que imitam algumas características da inteligência humana, como percepção, aprendizagem, raciocínio, resolução de problemas, interação linguística e trabalho criativo. Essa definição, contudo, vem sendo criticada ao longo dos últimos anos. Cf.: Cf. UNESCO, op. cit. nota 36.

[34] O programa "Smart Sampa", que conta com o uso de câmeras inteligentes contendo reconhecimento facial, entre outras tecnologias embasadas em inteligência artificial, já está em pleno funcionamento na cidade de São Paulo. O projeto almeja instalar 20 mil câmeras inteligentes na cidade, podendo chegar a até 40 mil câmeras. O projeto é controvertido e vem sendo criticado por inúmeros grupos de defesa de direitos, inclusive a Defensoria do Estado de São Paulo. A Defensoria Pública emitiu um ofício pedindo para que a Prefeitura de São Paulo não utilize a tecnologia de reconhecimento facial do "Smart Sampa" em blocos de carnaval da cidade. Cf.: https://g1.globo.com/politica/blog/julia-duailibi/post/2025/02/24/defensoria-publica-de-sp-pede-que-prefeitura-nao-utilize-reconhecimento-facial-do-smart-sampa-em-blocos-de-carnaval.ghtml.

[35] No Brasil, é possível dizer que o "debate da inteligência artificial" ganhou proporções nacionais quando as redes sociais fervilharam com a divulgação de uma campanha publicitária que, através da inteligência artificial, "trouxe de volta" a cantora Elis Regina, falecida na década de 1980. No vídeo, a artista aparece dirigindo uma Kombi e cantando "Como Nossos Pais", de Belchior, ao lado de sua filha, Maria Rita. Embora alguns fãs tenham se emocionado com o dueto, outros levantaram questões éticas sobre a utilização da imagem de uma pessoa falecida em um contexto fictício. Cf.: IBDFAM. Caso Elis Regina: o impacto da inteligência artificial na preservação da memória. 13/07/2023. Disponível em: https://ibdfam.org.br/noticias/10970/Caso+Elis+Regina%3A+o+impacto+da+intelig%C3%AAncia+artificial+na+preserva%C3%A7%C3%A3o+da+mem%C3%B3ria

[36] O Brasil é outra jurisdição (como a UE, o Canadá e a Coreia do Sul) que propõe regular a inteligência artificial como um todo, ou seja, apresentar uma regulação "geral", em vez de basear-se em aplicações específicas, como as setoriais. Na verdade, o Brasil tem se mostrado um dos pioneiros na regulação geral da inteligência artificial, pois já passou por várias iterações de um projeto de lei de inteligência artificial nas Casas Legislativas desde 2019. A discussão gira em torno principalmente dos seguintes projetos de lei: PL 21/2020, que regula o

Enquanto o foco se volta para a regulamentação do uso da inteligência artificial, outras questões regulatórias parecem perder a atenção dos responsáveis. Neste trabalho, vamos abordar uma "questão preliminar" no campo da proteção de dados pessoais, visando contribuir para o debate e, se possível, ajudar a garantir que qualquer futura regulação da inteligência artificial tenha uma base sólida para ser bem-sucedida.

Essa questão preliminar refere-se ao fato de que, no contexto do sistema normativo brasileiro de proteção de dados pessoais, embora exista uma legislação recente e compreensiva, a LGPD, ela se revela inadequada ou insuficiente para enfrentar as complexidades e especificidades inerentes às tecnologias de inteligência artificial e ao mesmo cumprir o seu propósito, que é o de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

De forma prática, se aplicada e interpretada de forma tradicional, a LGPD não possui elementos normativos suficientes para a regulação adequada dos tratamentos de dados necessários ao uso de sistemas de inteligência artificial em larga escala e dispersos nos diversos setores da economia – o que é uma tendência inevitável. Sendo assim, partindo de uma ideia de inadequação do quadro normativo brasileiro de proteção de dados pessoais para a regulação dos usos da inteligência artificial, o tema da tese é a investigação da proporcionalidade e da transparência como parâmetros normativos mais adequados e flexíveis para respaldar o tratamento de dados pessoais e, em última instância, regular a disciplina do uso de dados pessoais em aplicações de inteligência artificial.

Considerando que há um movimento global em curso para a criação de regulações abrangentes e específicas para a inteligência artificial, que exigem uma integração coesa e

---

desenvolvimento e aplicação de inteligência artificial no Brasil; o PL 2338/23 que cria o Marco Legal de Inteligência Artificial; e os PLs 4.025/23 e 3.592/23 que versam sobre direitos autorais e uso de inteligência artificial. Depois da aprovação em 2021 do PL 21/20 (de natureza principiológica), na Câmara dos Deputados, e da apresentação do PL 2.338/23 (de natureza prescritiva e inspirado no modelo da União Europeia), pelo presidente do Senado, Rodrigo Pacheco, em 24/04 a Comissão Temporária de Inteligência Artificial do Senado (CTIA) apresentou seu Texto Preliminar sobre os Projetos de Lei nº 2338/2023, 21/2020, 5051/2019, 5691/2019, 872/2021, 3592/2023, 145/2024, 146/2024, 210/2024 e 266/2024. Esse Texto Preliminar já foi substituído por nova redação, proposta pelo relator da CTIA, Senador Eduardo Gomes, em 07 de junho de 2024. A abordagem brasileira, que tramita de forma concentrada sob o Projeto de Lei nº 2338/2023, apresenta algumas semelhanças com a Lei de Inteligência Artificial da União Europeia (EU AI Act) em termos de uso de um sistema de camadas de risco, foco em direitos e nos impactos adversos e estabelecimento de um regime de responsabilidade civil em torno da inteligência artificial. Em 10 de dezembro de 2024, o Plenário do Senado aprovou um substitutivo do senador Eduardo Gomes (PL-TO) que tem como base o PL 2.338/2023, projeto de lei apresentado pelo senador Rodrigo Pacheco, presidente da Casa à época. O objetivo é oferecer uma regulação diferenciada, considerando o impacto do sistema na vida humana e direitos fundamentais. O projeto segue na Câmara dos Deputados.

eficiente com as normas de proteção de dados, o tema da pesquisa mostra-se relevante e contemporâneo.

Tornou-se necessário analisar com rapidez e profundidade as lacunas e insuficiências do atual sistema normativo brasileiro, identificar os desafios específicos que a inteligência artificial apresenta e propor possíveis respostas e adequações regulatórias que possam garantir uma proteção efetiva dos dados pessoais frente ao avanço inevitável da inteligência artificial.

Com a velocidade em que as transformações no ambiente de desenvolvimento de inteligências artificiais têm ocorrido, não há tempo a perder.[37] Portanto, este trabalho se justifica não apenas pela necessidade de atualizar e aprimorar o ordenamento brasileiro, mas também pela contribuição que pode oferecer ao debate sobre as interfaces entre a "regulação da inteligência artificial" e a "regulação do uso de dados pessoais".

O objetivo é buscar soluções inovadoras, e juridicamente sólidas e flexíveis para que sejam duradouras.[38]

No Direito, a busca do tema de pesquisa costuma partir dos seguintes propósitos: propósito de organizar e sistematizar algo que está confuso; propósito de determinar o significado jurídico de algo novo; propósito de buscar uma nova resposta para uma velha pergunta.[39] Neste trabalho, buscaremos uma nova resposta para uma velha pergunta: como deve ser concebida uma estrutura normativa de proteção de dados pessoais capaz de regular de maneira harmônica e eficiente os usos de dados pessoais?

Indo além, e posicionando a pergunta no momento contemporâneo: quais são os desafios regulatórios do atual quadro normativo de proteção de dados pessoais frente às tecnologias de inteligência artificial? Como podemos aprimorar os elementos e requisitos desse sistema normativo de modo a mantê-lo apto ao que se propõe em última instância, que é de proteger direitos fundamentais?

---

[37] A eficiência do processamento de chips de computador convencionais dobra a cada 18 meses, mas o poder de processamento exigido pelas tarefas modernas de inteligência artificial está dobrando atualmente a cada 3,5 meses. Cf.: DONG, B., Aggarwal, S., Zhou, W. *et al.* Higher-dimensional processing using a photonic tensor core with continuous-time data. *Nat. Photon.* 17, 1080–1088 (2023). https://doi.org/10.1038/s41566-023-01313-x

[38] Considerando que o objetivo do trabalho é buscar soluções inovadoras, juridicamente sólidas e duradouras, a natureza flexível da "proporcionalidade" e da "transparência" em matéria de proteção de dados se mostra relevante e é abordada de forma detalhada ao longo do trabalho.

[39] QUEIROZ, Rafael Mafei Ribeiro. Como encontrar um bom tema dentro de minha área de interesse?. *In: QUEIROZ, Rafael Mafei Ribeiro; FEFERBAUM, Marina (coord.)*. Metodologia jurídica*:* um roteiro prático para trabalhos de conclusão de curso. São Paulo: Saraiva, 2012. p. 56-59.

Estas podem ser consideradas “velhas perguntas”, pois as próprias legislações compreensivas e concentradas de proteção de dados já possuem mais de seis décadas.[40] Por sua vez, os contornos de um direito à privacidade são debatidos desde os primórdios da humanidade, mas, de forma sistematizada, pelo menos desde o final do século XIX.[41]

Em relação aos critérios para a escolha do tema, este se mostra relevante, pois versa sobre temática importante para o ordenamento jurídico e para a sociedade em geral, bem como é um assunto em constante transformação e que sofreu grande mutação nas últimas décadas, devido às intensas inovações tecnológicas.

Da mesma forma, o tema é original, pois, embora seja possível encontrar materiais sobre temas conexos, não foi possível encontrar uma tese – nacional ou internacionalmente – com abordagem similar.

Por fim, o pesquisador possui conhecimento na área específica, ou seja, é um tema familiar e as fontes e o material de pesquisa estão disponíveis publicamente.

Problema de pesquisa e questionamentos acessórios

O problema central desta pesquisa pode ser formulado a partir do seguinte questionamento principal: as legislações de proteção de dados pessoais atualmente em vigor, e em especial a LGPD, são adequadas e eficazes para garantir a privacidade e a proteção de dados pessoais frente ao uso de aplicações de inteligência artificial que realizam tratamentos complexos, massivos e sofisticados de dados pessoais?

Para desdobrar essa questão central e posicionar a investigação no contexto brasileiro, são formulados os seguintes questionamentos acessórios: a LGPD possui elementos normativos suficientes e adequados para garantir que as futuras regulações específicas para a inteligência artificial encontrem coesão normativa e eficiência regulatória? Qual é a melhor forma de um agente de tratamento de dados que utiliza aplicações de inteligência artificial assegurar a privacidade e a proteção dos dados pessoais? Quais são as obrigações que a legislação deve impor a este agente para otimizar as formas de proteção dos dados pessoais e garantia da

[40] Cf.: GONZÁLEZ FUSTER, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Cham: Springer, 2014. DOI: 10.1007/978-3-319-05023-2.
[41] WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. Civilistica.com, Rio de Janeiro, v. 2, n. 3, p. 1–22, 2013. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/127 . Acesso em: 22 ago. 2024.

privacidade? De que maneira um agente de tratamento deve se comunicar com os titulares dos dados para garantir transparência e gerar confiança e não apenas conformidade formal com a legislação? Como pode um agente de tratamento estabelecer ao mesmo tempo uma relação de confiança com os titulares dos dados, com a sociedade e com os reguladores, especialmente no contexto de uso de aplicações de inteligência artificial?

Talvez ainda não seja possível fornecer respostas precisas para tantos questionamentos. Nem é o objetivo desta tese fornecer respostas precisas para todas essas indagações. No entanto, esses questionamentos buscam abordar de maneira abrangente os múltiplos aspectos da inadequação do sistema normativo brasileiro diante dos desafios impostos pela inteligência artificial. Eles exploram desde a inadequação das normas existentes até as práticas recomendadas para agentes de tratamento e a atuação dos reguladores e do Judiciário. A busca por respostas a essas perguntas permite uma compreensão profunda das lacunas atuais e fornece diretrizes para a evolução normativa e interpretativa necessária para garantir uma proteção de dados pessoais robusta e eficaz em um cenário tecnológico em rápida transformação.

Dessa forma, nossa investigação à pergunta central e aos questionamentos acessórios também contribuem para a construção de pontes entre a teoria da inteligência artificial e da proteção de dados e a implementação prática dessas matérias.

Preparamos abaixo um quadro com os questionamentos principais e perguntas acessórias e respostas objetivas para antecipação dos rumos do trabalho.

Perguntas | Questionamentos	**Hipóteses | Respostas**
As legislações de proteção de dados pessoais atualmente em vigor, e em especial a LGPD, são adequadas e eficazes para garantir a privacidade e a proteção de dados pessoais frente ao uso de aplicações de inteligência artificial que realizam tratamentos complexos, massivos e sofisticados de dados pessoais?	As legislações atuais não estão adequadas para enfrentar os desafios de privacidade e proteção de dados causados ou intensificados pelas tecnologias de inteligência artificial. Apesar de novas leis que visem a regular a inteligência artificial em geral ou seus usos específicos poderem ser úteis, a expansão rápida da inteligência artificial em quase todos os setores e seus impactos nos direitos fundamentais mostram claramente que uma revisão das legislações é necessária. Mais especificamente, as leis de primeira e segunda gerações deveriam ter sido revisadas há muito tempo; já as de terceira geração precisam, pelo menos, de adaptações nos requisitos de legitimidade (especialmente nas bases legais) e de uma reinterpretação dos princípios quando aplicados ao uso da inteligência artificial.

A LGPD possui elementos normativos suficientes e adequados para garantir que as futuras regulações específicas para a inteligência artificial encontrem coesão normativa e eficiência regulatória?	Não. A LGPD foi criada antes da ampla expansão da inteligência artificial. Ela carece de elementos normativos mais adequados e da flexibilidade necessária em seus elementos atuais para lidar com os novos desafios trazidos pelas tecnologias de inteligência artificial, em que os dados pessoais são (e serão) utilizados em contextos muito mais complexos para os quais a lei atual não consegue fornecer soluções harmônicas. Além disso, a abordagem de riscos adotada pela LGPD para regular o uso de dados entrará em conflito com as regulamentações específicas ou gerais destinadas a gerenciar os riscos da inteligência artificial. Portanto, ao serem aplicadas em conjunto, essas legislações não criarão um ambiente de coesão normativa e eficiência regulatória, e tendem a gerar um quadro de rigidez regulatória, e medidas de conformidade vazias e meramente performáticos de manipulação de papelada.
Qual é a melhor forma de um agente de tratamento de dados que utiliza aplicações de inteligência artificial assegurar a privacidade e a proteção dos dados pessoais?	Realizando avaliações constantes, sistemáticas e contextuais da proporcionalidade no uso de dados pessoais para o treinamento e implementação de modelos e sistemas de inteligência artificial, assim como nos usos previstos de aplicações com potencial de causar riscos a direitos. Dessa forma, os momentos de reflexão do agente de tratamento de dados sobre os riscos e as estratégias para mitigá-los se tornarão mais frequentes e recorrentes, o que aumentará as chances de implementação de medidas que protejam a privacidade e a segurança dos dados.
Quais são as obrigações que a legislação deve impor a este agente para otimizar as formas de proteção dos dados pessoais e garantia da privacidade?	Obrigações de avaliação da proporcionalidade acerca do uso dos dados pessoais e obrigações de transparência qualificada.
De que maneira um agente de tratamento deve se comunicar com os titulares dos dados para garantir transparência e confiança e não apenas conformidade formal com a legislação?	Os agentes de tratamento devem se comunicar de maneira proativa, levando em conta o tipo de público-alvo e as características dos titulares dos dados. A mensagem deve ser clara, completa e ilustrativa, sempre que possível. É essencial que a comunicação seja precisa, evitando múltiplas interpretações. Além disso, seu formato e momento (*timing*) devem ser adaptados à jornada dos titulares como usuários de tecnologias ou sujeitos-avo

	de processamento de dados, de modo a não causar sobrecarga de informações.
Como pode um agente de tratamento estabelecer ao mesmo tempo uma relação de confiança com os titulares dos dados, com a sociedade e com os reguladores, especialmente no contexto de uso de sistemas de inteligência artificial?	A relação de confiança será estabelecida por uma transparência proativa e qualificada, permitindo o conhecimento dos titulares de dados sobre produtos e serviços que utilizam dados pessoais; e no caso do Poder Público, sobre as políticas públicas, competências, previsão legal, finalidade, procedimentos e práticas utilizadas na execução da finalidade pública e disponibilizada em veículos de fácil acesso, preferencialmente sítios eletrônicos, se houver. Em relação aos reguladores, a transparência ativa e qualificava facilitará o acesso a informações sobre o uso de dados, melhorando a eficácia do controle, supervisão e responsabilização de infratores.

Enunciação da hipótese

A hipótese central da tese é que as legislações de proteção de dados de primeira, segunda e terceira geração estão defasadas diante da sofisticação dos tratamentos de dados pessoais e da complexidade do cenário de evolução tecnológica, em especial no que tange ao requisito das bases legais que autorizam o tratamento de dados pessoais, de modo que as legislações precisam evoluir e amparar os usos de dados em novos parâmetros normativos. Esses parâmetros já estão, em maioria, presentes nas constituições e legislações de proteção de dados pessoais, como a LGPD, mas hoje não são entendidos como elementos que garantam, por si só, legitimidade ao tratamento de dados. Ademais, quando aplicados, não disparam obrigações de avaliação contextual da privacidade e da segurança dos dados. Esses parâmetros são: proporcionalidade e transparência.

Em suma, defendemos que a mera existência de uma base legal para o tratamento de dados, como o consentimento do titular, ou outra base prevista na legislação de proteção de dados, não é parâmetro normativo suficiente para dizer se determinado uso de dados é legal e/ou legítimo e, em última instância, não é um parâmetro adequado para respaldar o tratamento de dados. Os parâmetros adequados para respaldar a legitimidade e a legalidade do tratamento de dados, em especial no modelo constitucional brasileiro, são a proporcionalidade do tratamento e as medidas de transparência adotadas.

A noção de legalidade e legitimidade do tratamento de dados deve ir além da escolha da base legal – e do cumprimento dos princípios gerais das leis de dados; ela está profundamente vinculada ao princípio constitucional da proporcionalidade e na forma de comunicação dos agentes de tratamento, ou seja, na transparência adotada pelo agente regulado. Assim, nossa tese propõe uma reflexão crítica sobre a necessidade de revisar e expandir os parâmetros normativos, especialmente à luz das novas tecnologias e práticas emergentes que desafiam as normas tradicionais de proteção de dados.

Em termos simples, a legalidade e a legitimidade[42] do tratamento de dados pessoais atualmente são alcançadas quando o controlador de dados segue as leis aprovadas pelo processo legislativo. Isso significa que o tratamento de dados é considerado legal e legítimo se estiver, em geral, de acordo com as bases legais[43] e com os princípios[44] da lei de proteção de dados aplicável. No entanto, quando consideramos as aplicações da inteligência artificial (as atuais e o que se imagina das vindouras), não apenas o conjunto de bases legais já não é mais suficiente para dar conta dos tratamentos necessários para o desenvolvimento (design ou conceptualização), treinamento e implementação de modelos, mas também a própria noção de que a legalidade e legitimidade derivam da existência de uma base legal e do cumprimento de princípios está ultrapassada.

Tradicionalmente, a viabilidade do tratamento de dados pessoais é alcançada quando o controlador cumpre a lei, que, por sua vez, é considerada legítima por ter sido aprovada por meio de um processo legislativo. Em termos mais específicos, o tratamento de dados é possível

---

[42] Em resumo, no contexto atual, a legitimidade do tratamento de dados pessoais ocorre quando o Controlador cumpre a lei, que por sua vez é considerada legítima por ter sido aprovada por meio de processo legislativo. Em uma análise mais detalhada, o tratamento de dados pessoais é considerado legítimo caso esteja respaldado em pelo menos uma base legal autorizativa e se o tratamento respeita os princípios da lei de proteção de dados. O conceito de legitimidade de tratamento de dados que lançaremos mão faz uma ruptura com o conceito de legitimidade acima resumido. O conceito de legitimidade que será proposto é procedimental. Como nossa proposta é de que há legitimidade quando há proporcionalidade e justificação pública do tratamento de dados, a legitimidade nascerá com o cumprimento de ritos e avaliações (processos e procedimentos). Nesse sentido, o processo de análise da proporcionalidade do tratamento e o cumprimento dos parâmetros constitucionais da proporcionalidade é o que trará a legitimidade.

[43] "*A second characteristic of the EU regime is that it legitimizes the processing of personal data. Once it can be demonstrated that a legal basis for personal data processing exists and that this processing complies with specified data protection safeguards, then this processing is in principle legitimate.*" In LYNSKEY, Orla. The foundations of EU data protection law. Oxford, United Kingdom: Oxford University Press, 2015. p.30.

[44] "*In addition to the abovementioned grounds for lawful data processing, data processing must also comply with a number of safeguards: known in the Directive as the 'principles relating to data quality' and referred to as 'principles relating to personal data processing' in the draft GDPR. These safeguards are broadly derived from Convention No 108*." In LYNSKEY, Orla. The foundations of EU data protection law. Oxford, United Kingdom: Oxford University Press, 2015. p. 34.

se estiver amparado em pelo menos uma base legal autorizativa e se respeitar os princípios estabelecidos na legislação de proteção de dados.

Os parâmetros normativos que propomos neste trabalho rompem com essa visão tradicional. Aqui, deixamos de focar apenas em uma questão de conformidade legal (por exemplo, indicar uma base legal), e enxergamos algo mais profundo e dinâmico a respeito da legalidade e legitimidade do tratamento de dados.

Propomos um conceito que, ao mesmo tempo que é mais flexível, é mais fácil de ser verificado e controlado pelos titulares e pela sociedade em geral. Segundo nossa perspectiva, haverá autorização legal para um tratamento de dados ocorrer quando houver proporcionalidade e ela puder ser justificada publicamente por meio dos postulados da razoabilidade. Em outras palavras, a legalidade e a legitimidade do tratamento não são um estado estático garantido pela simples escolha de uma base legal e cumprimento de princípios abertos, mas um processo contínuo de avaliação e justificativa perante os titulares e a sociedade em geral, o que inclui reguladores e o Poder Judiciário.

A partir dessa interpretação, o verdadeiro núcleo de validação do tratamento reside no cumprimento de ritos e avaliações – processos e procedimentos que garantem que o tratamento de dados seja proporcional e justificado. Dessa forma, o processo de análise da proporcionalidade do tratamento é o que, de fato, confere legalidade e legitimidade ao uso dos dados.

Nesse contexto, a tese se desenrola como uma investigação instigante sobre como a validade do tratamento deve ser conquistada, não apenas por meio de conformidade formal, mas por meio de um compromisso sincero e contínuo com a proporcionalidade e a transparência. Pode ser considerada como uma chamada para uma nova era na proteção de dados pessoais, na medida em que os parâmetros que respaldam os tratamentos de dados estão vivos, são dinâmicos e estão sob constantemente reavaliações.

Embora já tenha sido reconhecido anteriormente que as leis de proteção de dados precisavam ser atualizadas para responder às novas tecnologias e formas de processamento de dados, por exemplo, quando houve a evolução das legislações de primeira para segunda e depois para terceira geração, os parâmetros normativos que vamos discutir neste trabalho são completamente diferentes da tendência evolutiva aplicada até o momento.

Enquanto as legislações evoluíram, dentre outras questões, por meio de ampliações no leque de bases legais que respaldam o tratamento de dados; agora, as próprias características de

disruptividade e versatilidade da tecnologia de inteligência artificial indicam que não faz mais sentido pensarmos em novas bases. Repetir essa abordagem seria errar novamente e postergar uma solução. Essa estratégia estaria eivada do mesmo problema: ela não é resistente ao tempo. Em poucos anos, quiçá meses, a legislação não estaria apta a responder a novos usos, modelos de negócio, evoluções em políticas públicas, desafios, riscos e danos que ainda não conseguimos prever integralmente. Nesse sentido, vamos propor que certos parâmetros normativos existentes no direito constitucional e nas legislações de proteção de dados ganhem elementos procedimentais, que acabam conferindo maior proteção aos dados pessoais e melhorando a relação de confiança a respeito do uso dos dados. Ou seja, a legalidade e legitimidade dos usos de dados serão alcançadas por meio de processos e avaliações mais abrangentes a respeito da proporcionalidade do tratamento, somados à transparência: resultando no estabelecimento de uma relação de confiança com os titulares e com a sociedade, e em melhorias nas formas de supervisão por reguladores.

Se nossa hipótese for confirmada, ela poderá resolver diversos desafios regulatórios e práticos atuais. Por exemplo, em contextos de tratamentos massivos de dados pessoais para o treinamento de modelos de inteligência artificial, ou em processos preparatórios como a raspagem na internet, o princípio da minimização de dados muitas vezes não é cumprido.[45] Além disso, em muitos casos pode ser impraticável basear esses tratamentos no consentimento, devido à impossibilidade de coletar milhões ou bilhões de autorizações individuais válidas. Por sua vez, o uso de bases legais como o legítimo interesse também enfrenta desafios práticos, como a presença de dados sensíveis residuais que não permitem essa justificativa, além da necessidade de provar que o tratamento é "necessário" (quando dificilmente de fato é). Finalmente, enquanto o uso de PETs (*Privacy-enhancing Technologies*[46]) pode representar, de

[45] Martin Ebers e Karin Sein argumentam que sistemas de inteligência artificial, ao processarem grandes volumes de dados pessoais, provavelmente acionam a aplicação do GDPR, especialmente em relação à transparência, limitação de propósito e minimização de dados. O treinamento desses modelos pode conflitar com a lei de proteção de dados da UE, como evidenciado pela restrição temporária imposta à OpenAI pela autoridade italiana em 2023. O EDPB também criou uma força-tarefa para supervisionar a aplicação dessas leis. Encontrar uma base legal para o processamento de dados e garantir o cumprimento das obrigações informativas do GDPR representa um desafio para os desenvolvedores de IA, além de ainda não existir clareza sobre como os titulares dos dados podem exercer seus direitos em relação aos conjuntos de dados de treinamento. Cf.: EBERS, Martin; SEIN, Karin. Data-driven Technologies: Challenges for Privacy and EU Data Protection Law. In: EBERS, Martin; SEIN, Karin (ed.). *Privacy, Data Protection and Data-driven Technologies*. Abingdon: Routledge, 2024. p. 11–12. Disponível em: https://ssrn.com/abstract=4823823.

[46] PETs (*Privacy-enhancing technologies* ou tecnologias de aprimoramento da privacidade) são tecnologias que incorporam princípios fundamentais de proteção de dados, minimizando o uso de dados pessoais, maximizando a segurança dos dados e capacitando os indivíduos. As PETs utilizam técnicas para, dentre outros objetivos, minimizar o processamento de dados pessoais por um sistema de informação sem que esse sistema ou dado perca sua funcionalidade. De modo geral, as PETs podem ser categorizadas como tecnologias de privacidade "dura" ou

fato, uma solução para alguns usos de dados, confiar no emprego de medidas técnicas, organizacionais e no uso dessas tecnologias como uma "bala de prata" ou solução escalável para todos os cenários de uso de inteligência artificial é, no mínimo, uma atitude ingênua; ou pouco eficiente em termos regulatórios se pensarmos em usos difundidos em todos os setores da sociedade e em agentes de tratamento de dados que não são capazes de implementar essas medidas técnicas, administrativas e tecnologias de difícil acesso.[47]

Nossa proposição visa criar um modelo regulatório que exige dos agentes de tratamento não apenas uma avaliação acerca da proporcionalidade do uso de dados por meio da avaliação da constitucionalidade do tratamento no caso concreto, mas também incentiva ações de autoavaliação constantes de suas práticas de privacidade e segurança de dados. Criam-se incentivos regulatórios e processos para que as ações dos agentes reguladas não prejudiquem desproporcionalmente os direitos e interesses dos indivíduos, promovendo um equilíbrio contínuo entre os direitos e interesses envolvidos.

Na estrutura de proteção de dados concebida neste trabalho, ou até mesmo na interpretação do sistema atual, os agentes de tratamento seriam obrigados a demonstrar que realizaram avaliações de proporcionalidade constantes e que elas foram bem-sucedidas e podem ser publicamente justificadas com base em interpretações razoáveis dos valores constitucionais.

"suave". Tecnologias de aprimoramento da privacidade, como pseudonimização por criptografia polimórfica e aprendizado federado, são exemplos de medidas técnicas que podem ser implementadas para proteger melhor os dados pessoais. Além disso, medidas organizacionais, como a transparência – chamadas também de Transparency Enhancing Technologies (TETs) –, também devem ser levadas em conta.

[47] Ainda que a tecnologia tenha um papel importante na proteção da privacidade, ela não pode ser vista como a solução definitiva para a crise global da privacidade. Como vem sendo observado por autores, a dependência excessiva em soluções tecnológicas pode levar a uma falsa sensação de segurança, obscurecendo a necessidade de medidas legais, políticas e sociais mais amplas. Há uma superestimação do potencial protetor de algumas tecnologias, a exemplo da blockchain, privacidade diferencial, sistemas de gerenciamento de informações pessoais inteligentes e computação descentralizada, como soluções "milagrosas" para a privacidade. Além disso, em um mercado altamente competitivo, as empresas raramente restringirão a coleta e o processamento de dados pessoais, a menos que tenham um forte incentivo para fazê-lo. Elas geralmente protegerão os dados contra-ataques maliciosos externos, mas raramente os tornarão inacessíveis ou inutilizáveis para si mesmas. Além disso, no atual cenário, há a "brecha do consentimento", ou seja, mesmo quando medidas de proteção de dados são exigidas por lei, o consentimento do titular dos dados pode ser usado para contornar essas exigências, permitindo uma coleta e processamento extensivos de dados. Deve se considerar também os desafios e limitações técnicas de ordem prática que criam verdadeiras barreiras quase que intransponíveis para a maioria dos controladores de dados. As tecnologias de aprimoramento da privacidade frequentemente enfrentam obstáculos como complexidade computacional, alto consumo de energia, falta de usabilidade e imaturidade técnica. Soluções eficazes podem comprometer a usabilidade ou funcionalidade de um produto ou serviço, resultando em um compromisso entre privacidade e utilidade (privacy-utility trade-off). Por fim, a maioria das discussões sobre tecnologias de aprimoramento da privacidade se concentra no que elas protegem, e não no que elas *não* protegem. Mesmo quando várias salvaguardas técnicas são usadas em combinação, grandes pontos cegos e lacunas podem permanecer. Cf.: KRÖGER, Jacob Leon. Technology Cannot Fix the Privacy Crisis. [S.l.]: SSRN, 2022. Capítulo adaptado de: KRÖGER, Jacob Leon. Rogue Apps, Hidden Web Tracking and Ubiquitous Sensors. 2022. Tese (Doutorado) — Technische Universität Berlin, Berlin, 2022. p. 216–219. DOI: 10.14279/depositonce-16043. Disponível em: https://ssrn.com/abstract=4326794.

Isso seria permitido por meio de transparência sobre seus processos, que evidenciariam os danos e riscos existentes, melhorariam as formas de supervisão, e contribuiriam para o monitoramento da efetividade das propostas de mitigação dos danos e riscos.

Acredita-se que os elementos normativos propostos promovem uma abordagem mais responsável e equilibrada no uso de dados pessoais para o desenvolvimento de aplicações de inteligência artificial. Em última instância, a abordagem regulatória proposta desafoga os agentes regulados de certas obrigações que não têm se mostrado eficazes para a proteção dos direitos fundamentais. Além disso, ela permite um redirecionamento dos recursos despendidos tanto pelos agentes regulados quanto pelos reguladores para ações mais eficientes do ponto de vista da efetiva proteção dos dados pessoais e da preservação da privacidade.

Por fim, a visão de transparência veiculada nesse trabalho promete ajustar a necessidade de garantir informação e participação adequada dos titulares de dados e da sociedade em geral, o que inclui as entidades de supervisão, ao mesmo tempo que protege interesses comerciais, como os segredos industrial e de negócio.

Estrutura da tese

Esta tese está dividida em seis partes, por assim dizer, sendo três delas destinadas à presente introdução, aos comentários metodológicos e, ao final do texto, à conclusão. Apresentamos a seguir a estrutura dos três capítulos em que o conteúdo da tese é majoritariamente desenvolvido.

No primeiro capítulo são abordados os desafios regulatórios em matéria de proteção de dados pessoais frente à expansão da inteligência artificial. Inicialmente, é apresentada uma visão geral das aplicações de inteligência artificial, incluindo uma breve história da tecnologia e uma análise detalhada dos algoritmos e taxonomias, como sistemas baseados em regras, aprendizado de máquina, redes neurais artificiais e modelos de linguagem de grande escala. Não assumiremos aqui a tarefa de explicar todas as questões técnicas sobre os algoritmos de inteligência artificial. Nosso objetivo é, primeiro, estabelecer o mínimo necessário para entendermos os principais modelos, os dados e riscos ligados aos direitos fundamentais, em especial à privacidade e à proteção de dados pessoais; e, segundo, demonstrar que o ambiente é altamente complexo para o tipo de regulação que temos atualmente. Em seguida, são discutidas as aplicações e áreas de aplicação da inteligência artificial, com foco nas que afetam

direitos fundamentais. O capítulo também explora a relação entre inteligência artificial, privacidade e proteção de dados pessoais, destacando os desafios regulatórios em cada fase do desenvolvimento dessa tecnologia – que é apresentada neste item de forma generalizada para fins didáticos –, desde o design, passando pela organização das bases de dados, treinamentos dos modelos até a implementação.

O segundo capítulo examina a aplicabilidade dos arranjos normativos de proteção de dados pessoais às aplicações de inteligência artificial que tratam dados pessoais. É feita uma breve análise histórica das gerações de leis de proteção de dados pessoais, destacando os elementos comuns de legitimidade e os padrões evolutivos. O capítulo também detalha os requisitos legais do arranjo de proteção de dados para o tratamento de dados pessoais, com ênfase nas bases legais, como consentimento e legítimo interesse – que são as mais discutidas atualmente –, e debate a indicação dessas bases no contexto da inteligência artificial. Além disso, é realizado um diagnóstico da aplicação do sistema normativo brasileiro, identificando problemas e desafios regulatórios específicos, como a insuficiência do rol de bases legais e a dificuldade de aplicação do consentimento e do legítimo interesse.

No terceiro capítulo são apresentados os parâmetros constitucionais aplicáveis ao tratamento de dados pessoais. O capítulo inicia com uma análise do princípio da proporcionalidade em casos envolvendo proteção de dados pessoais, com foco na Ações Diretas de Inconstitucionalidade (ADI) 6.387, 6.388, 6.389, 6.393 e 6.390 e na Arguição de Descumprimento de Preceito Fundamental (ADPF) 695 e a ADI 6.649 julgadas pelo STF. Resumiremos essas ações, destacando a tese veiculada pelo Supremo Tribunal Federal (STF) acerca da ausência de proporcionalidade nos critérios que embasaram a coleta, compartilhamento e uso de dados pessoais, ressaltando o que constitui para o STF a falta de uma finalidade específica e necessidade clara, bem como a ausência de medidas de segurança adequadas. Analisando os limites ao compartilhamento de dados conforme o direito fundamental à proteção de dados pessoais, abordaremos as importantes conclusões veiculadas pelo STF nesses julgamentos. Extrairemos dos votos da Corte noções sobre o que constituem propósitos legítimos, específicos e explícitos do tratamento de dados, além das limitações de uso baseadas na necessidade e finalidade informada. Enfatizaremos também o que o STF entende como controles técnicos mínimos para garantir a rastreabilidade de como os dados são usados e por quem, como forma de garantir responsabilização e prestação de contas. Além disso, será possível extrair desse caso elementos importantes para entender os contornos do que seriam os filtros de proporcionalidade e transparência, uma vez que o Supremo enfatizou como

devem ser os parâmetros de finalidade, adequação, necessidade, segurança, prevenção, responsabilização e prestação de contas e transparência em relação à publicidade do compartilhamento ou acesso a bancos de dados pessoais.

Dando enfoque à proporcionalidade e à transparência, o terceiro capítulo explorará a proporcionalidade como um parâmetro constitucional aplicável ao tratamento de dados pessoais em aplicações de inteligência artificial. Analisaremos como a proporcionalidade pode ser operacionalizada para garantir que os tratamentos de dados sejam justos, necessários e proporcionais aos fins almejados. Percebemos como a proporcionalidade tem função dual, operando como postulado constitucional por meio do qual os princípios de proteção de dados são usados como parâmetros de avaliação da constitucionalidade do uso de dados pessoais, ao mesmo tempo em que funciona como procedimento garantidor de legitimidade. Além disso, abordaremos a transparência como um parâmetro essencial e como resultado desejado, destacando sua função como equalizador das legítimas expectativas dos titulares, elemento de confiança, abertura ao regulador e aos titulares, e mecanismo de prestação de contas e responsabilização.

Essas discussões proporcionarão uma compreensão abrangente de como a proporcionalidade e a transparência podem ser aplicados de maneira eficaz para proteger os dados pessoais no contexto das aplicações de inteligência artificial no Brasil, tornando-se os novos parâmetros capazes de dar respaldo normativo a usos de dados por agentes de tratamento que lançam mão de aplicações de inteligência artificial.

Na conclusão, por fim, são sintetizados os principais pontos discutidos ao longo da tese, destacando os desafios e oportunidades na aplicação dos parâmetros constitucionais e legais para o tratamento de dados pessoais em aplicações de inteligência artificial. São fornecidas recomendações práticas e sugestões para pesquisas futuras, visando contribuir para o desenvolvimento de um quadro regulatório robusto e eficaz que equilibre inovação tecnológica e proteção efetiva dos dados pessoais e garantia de privacidade.

Metodologia

Revisão da bibliografia

É possível dividir a literatura relevante para esta tese em três categorias. A primeira categoria é a bibliografia para a compreensão histórica das legislações de proteção de dados e do funcionamento das estruturas regulatórias de proteção de dados, ou seja, conhecimentos básicos para que seja possível entender o contexto legal em que a tese é desenvolvida, bem como os elementos basilares dos sistemas legais, em especial o ordenamento brasileiro. Essa literatura foi revisada em detalhes nas fases de pesquisa e é apresentada em diferentes momentos da tese, por vezes com notas adicionais para melhor entendimento das regras de proteção de dados e referências a opiniões doutrinárias. Essa bibliografia é mencionada em maior escala nos capítulos de desenvolvimento, momento em que eventuais comparações entre os ordenamentos, rememorações e explicações adicionais de natureza técnica são necessários.

A segunda categoria de bibliografia relevante para este trabalho está relacionada aos requisitos que conferem legalidade e legitimidade ao tratamento de dados pessoais. Pode-se dividir esta segunda categoria em literatura sobre os princípios e as bases legais para o tratamento de dados pessoais, havendo enfoque para as bases legais do consentimento e do legítimo interesse, bem como sobre os mecanismos de transparência utilizados pelos controladores de dados perante os titulares e a sociedade em geral, incluindo reguladores e o Poder Judiciário.

A terceira categoria relevante para a tese relaciona-se com a análise da proporcionalidade no contexto da proteção de dados pessoais no Brasil. Os materiais utilizados contêm discussões de campos mais amplos do direito, a exemplo da teoria constitucional e do direito administrativo. A respeito das leituras sobre proporcionalidade, já bastante difundidas, destacamos quando, como e por que a noção de proporcionalidade utilizada neste trabalho difere da doutrina estabelecida em âmbito constitucional e administrativo até aqui. Em síntese, a respeito da revisão literária sobre proporcionalidade, buscamos beber na fonte da doutrina da proporcionalidade no direito constitucional para extrair o que podemos resumir como “doutrina brasileira da proporcionalidade na proteção de dados pessoais”.

Dentro dessa terceira categoria destacam-se os acórdãos e votos dos ministros do Supremo Tribunal Federal em casos paradigmáticos que, recentemente, esculpiram os

contornos de um direito fundamental autônomo à proteção de dados pessoais e definiram elementos, filtros e requisitos para que a verificação da proporcionalidade possa ser avaliada. Um exemplo emblemático é a decisão do STF na Medida Cautelar das Ações Diretas de Inconstitucionalidade 6.387, 6.388, 6.389, 6.393 e 6.390. Outra decisão crucial foi a proferida na ADPF 695/DF e na ADI 6.649/DF, que também se tornou um verdadeiro marco na proteção de dados pessoais no Brasil. Essa decisão estabeleceu limites nítidos para o compartilhamento de dados pessoais na administração pública e delineou parâmetros para a estruturação das entidades encarregadas de fiscalizar e regulamentar o tratamento de dados pessoais.

Finalmente, e como de costume, a bibliografia é listada ao final do trabalho em ordem alfabética.

As pesquisas anteriores à tese

Embora não se configure como um elemento obrigatório da metodologia, a contextualização das pesquisas realizadas até agora revela-se extremamente benéfica. Ela ilumina o fio condutor[48] que as une: uma dedicação incessante à adequação de processos e estruturas organizacionais que assegurem legalidade e legitimidade no uso de dados, juntamente com proposições hermenêuticas capazes de resolver crises no ordenamento jurídico diante da proliferação de novas tecnologias.

No projeto de pesquisa apresentado para ingresso no Doutorado em Direito Público entre 2020 e 2021, propusemos um projeto de pesquisa intitulado "*A proteção de dados como vetor da governança democrática das redes*". Neste projeto partimos da ideia central de que a esfera

[48] Desde o ingresso na Universidade do Estado do Rio de Janeiro (UERJ) em 2011, as disciplinas de Direito Público sempre foram as preferidas. Como trabalho de conclusão da graduação, apresentamos uma monografia intitulada "Democracia Deliberativa: legitimidade e justificação das decisões político-normativas", com o objetivo de analisar se e como as normas constitucionais brasileiras abarcam certas proposições do modelo deliberativo de democracia. O estudo fez um apanhado de princípios e normas constitucionais, além dos regimentos internos das Casas Legislativas para identificar se as decisões políticas na democracia brasileira devem ser tomadas, por obrigação legal, de forma justificada e com amplo debate público. No mestrado em Direito da Cidade, cursado entre 2017 e 2019, apresentamos a dissertação intitulada "Regulação das Redes Sociais: considerações sobre liberdade de expressão em Sociedades Algorítmicas". Neste trabalho mergulhamos de forma precursora em um conceito ainda pouco explorado à época, as "fake news", que representam até hoje um risco iminente para as democracias. No contexto da época delineamos as principais diferenças entre o ecossistema informacional na esfera pública clássica e na esfera pública digital, analisando o fenômeno da desinformação dentro de um grupo mais amplo de danos praticados nas redes sociais, tendo em vista que regulações impostas sem balizamentos adequados poderiam entrar em choque com a liberdade de expressão. Apresentamos o cenário regulatório das redes sociais e a complexidade em regular setores disruptivos com incertezas científicas, como no caso das redes sociais.

pública atravessa uma nova transformação estrutural, de modo que o conceito clássico não é mais suficiente para compreender o ambiente no qual considerável parte das relações sociais se travam. Desde que começamos a frequentar as salas virtuais do Doutorado em Direito Público da Universidade do Estado do Rio de Janeiro (UERJ) a partir de março de 2021, em meio à crise da pandemia do coronavírus, o foco da pesquisa continuou a ser sobre as implicações legais causadas com os avanços no campo da tecnologia.

Durante o Doutorado, como requisito para conclusão das disciplinas, apresentamos os seguintes trabalhos: (i) *A evolução da desinformação e os rumos do debate regulatório no Brasil;* (ii) *Deliberação na regulação das redes: combatendo desinformação com democracia;* (iii) *Respeitando princípios no compartilhamento de dados: bases de um raciocínio jurídico;* (iv) *Pesquisas de diversidade e proteção de dados sensíveis: boas práticas para a coleta do consentimento em relações de trabalho;* (v) *Programas de diversidade e inclusão e proteção de dados pessoais sensíveis: boas práticas para o tratamento de dados nas relações de trabalho;* (vi) *Destrinchando a proposta europeia para regulação da inteligência artificial: Parte I, Parte II, Parte III, Parte IV;* (vii) *Adequação das serventias extrajudiciais à Lei Geral de Proteção de Dados Pessoais: uma abordagem prática;* (viii) *Relatório de Impacto à Proteção de Dados Pessoais. Parte I: contexto, abrangência e escalabilidade;* (ix) *Relatório de Impacto à Proteção de Dados Pessoais. Parte II: documentação e etapas de seu desenvolvimento; e* (x) *Análise de Impacto Regulatório na Autoridade Nacional de Proteção de Dados: uma perspectiva de monitoramento*.

Como se pode perceber, nossas pesquisas concentraram-se nas interfaces do direito com as novas tecnologias, em especial no impacto das tecnologias disruptivas[49] e informacionais na democracia e nos direitos à privacidade e à proteção de dados pessoais. De forma mais detalhada, as pesquisas possuem como elementos comuns a "legalidade e legitimidade", os "mecanismos de justificação e participação" e as "proposições hermenêuticas para a resolução de crises no ordenamento a partir da profusão de novas tecnologias".

Iniciamos as pesquisas preparatórias para o Doutorado investigando as formas de harmonizar, por meio de uma convergência substantiva e transnacional, os padrões de proteção de dados e as regras sobre governança dos serviços na internet em escala global. Embasado nessas premissas, que de certa forma são mantidas nesta tese até hoje, o foco da pesquisa nos

[49] Sobre a relação entre as tecnologias disruptivas e a regulação, ver: BAPTISTA, Patrícia; KELLER, Clara Iglesias. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. *Revista de Direito Administrativo*, Rio de Janeiro, v. 273, p. 123–163, set. 2016. ISSN 2238-5177. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/66659.

primeiros anos do Doutorado esteve nos fundamentos democráticos a serem observados na regulação das novas tecnologias: a necessidade de incentivar uma governança cada vez mais descentralizada, com participação direta e efetiva da sociedade civil e dos reguladores no processo de construção das tecnologias; e a construção deliberativa dos instrumentos privados de governança, entendimento que pode ser concebido como a abertura e a transparência dos agentes regulados em temas que envolvem interesse público. Sem dúvida, esses enfoques foram mantidos.

Durante o doutorado nossa trajetória evoluiu de focar na "regulação das redes" para uma profunda imersão na "regulação da proteção de dados pessoais", com uma inclinação particular em questões práticas. Ao longo dessa jornada empenhamo-nos em unir as pesquisas históricas e teóricas com a implementação tangível. A eficácia das teorias regulatórias em proteção de dados pessoais encontra seu verdadeiro teste na execução dos mecanismos de conformidade, respondendo à crucial pergunta do "como fazer?". A prática diária da proteção de dados é um equilíbrio entre "teoria" e "ação": a verdadeira "mão na massa". Nossa produção acadêmica, portanto, concentra-se em como desenvolver programas de governança em privacidade tanto no setor privado quanto no público. Exploramos temas complexos, presentes nesta tese, como a evolução das avaliações de impacto em privacidade, refletidas no Brasil pelo relatório de impacto à proteção de dados pessoais. Fomos além, investigando os desafios do uso de dados sensíveis para atender interesses públicos, mesmo quando operados por entidades privadas. Nossos estudos sobre diversidade, inclusão e ações afirmativas para grupos vulneráveis revelaram lacunas significativas na LGPD e que dificilmente serão transponíveis sem uma evolução da legislação, que pode ocorrer pela via de emendas ou da interpretação pela doutrina, reguladores e Poder Judiciário. Com base em nossas pesquisas, podemos afirmar que, apesar de seus objetivos, a estrutura regulatória da LGPD está longe de ser perfeita e apresenta-se, por vezes, como desnecessariamente custosa e ineficiente; enquanto deveria suavizar o caminho para agentes bem-intencionados, acaba por sufocá-los em custos e incentivos opostos, permitindo, ao mesmo tempo, que os menos comprometidos driblem (*by pass*) suas obrigações e responsabilidades. Em nossa investigação sobre os atos normativos da ANPD,[50] ganhamos

[50] Monitoramos de perto a elaboração das Resoluções da ANPD e as discussões sobre estratégias regulatórias. A Portaria nº 16, de 8 de julho de 2021, oficializou o processo de regulamentação da ANPD. Em diversos temas regulatórios, foi necessária a elaboração de Análise de Impacto Regulatório (AIR), que avalia problemas e lacunas e propõe estratégias para enfrentar desafios regulatórios. Por exigência legal, esse documento é um requisito para a edição de certas normas por agências reguladoras e outros órgãos federais. Conforme o artigo 6º da Lei nº 13.848, de 25 de junho de 2019, e o artigo 5º da Lei nº 13.874, de 20 de setembro de 2019, propostas de normas devem ser precedidas de AIR. O Decreto nº 10.411, de 30 de junho de 2020, detalha o conteúdo e

insights importantes sobre o regulador brasileiro, permitindo-nos refinar nossa compreensão sobre as brechas da LGPD e das estratégias regulatórias. Por fim, acompanhamos de perto o surgimento das discussões sobre regulação de inteligência artificial, não apenas na União Europeia, mas de forma destacada na América Latina, nos Estados Unidos e no Brasil, consolidando uma visão abrangente e crítica sobre o cenário regulatório em transformação.

Baseando-se na premissa de que as legislações de proteção de dados são essenciais para garantir respeito aos direitos fundamentais no contexto da criação e implementação de tecnologias disruptivas, a principal diferença dos novos rumos da nossa pesquisa é que, agora, focamos na análise das tecnologias e desafios atuais, como a inteligência artificial e seus potenciais riscos e danos – sobretudo os impactos negativos em direitos fundamentais, como a privacidade e a proteção de dados. Por mais que o enfoque tenha sido ampliado para a inteligência artificial, continuamos firmes na convicção de que investir em novas formas de proteção de dados pessoais é a única maneira de assegurar o respeito ao amplo leque de direitos fundamentais e, em última instância, preservar a democracia.

Elementos para a fundamentação teórica

Nossa fundamentação teórica se baseia em conceitos tradicionais do sistema jurídico brasileiro, como a proteção da intimidade e vida privada (CRFB, art. 5º, inc. X), a inviolabilidade do domicílio (CRFB, art. 5º, inc. XI), o sigilo das comunicações (CRFB, art. 5º, inc. XII), e o Habeas Data (CRFB, art. 5º, inc. LXXII), e conceitos mais recentes do sistema jurídico, como o direito à proteção dos dados pessoais, inclusive nos meios digitais (CRFB, art. 5º, inc. LXXIX, incluído pela Emenda Constitucional nº 115, de 2022), a competência da União para organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei (CRFB, art. 21, inc. XXVI, incluído pela Emenda Constitucional nº 115, de 2022), e a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais (CRFB, art. 22, inc. XXX, incluído pela Emenda Constitucional nº 115, de 2022). Nossa fundamentação teórica se baseia também nos princípios e parâmetros constitucionais e aqueles dispostos em legislação infraconstitucional. Por exemplo, os princípios estabelecidos na LGPD definem diretrizes e

metodologia da AIR, com critérios e exceções para sua obrigatoriedade. Até o momento, a ANPD realizou AIR para normativos como: (i) normativos para aplicação do art. 52 e seguintes da LGPD (fiscalização); (ii) proteção de dados para pequenas e médias empresas, startups e pessoas físicas com fins econômicos; (iii) regulamento de comunicação de incidente de segurança; (iv) atuação do encarregado pelo tratamento de dados; e (v) transferência internacional de dados e cláusulas-padrão contratuais.

limitações para o tratamento de dados pessoais.[51] Nossa fundamentação passa também, ainda que lateralmente, por um amplo leque de legislações ordinárias que formam o sistema normativo brasileiro de proteção de dados pessoais, como a Lei do Habeas Data (Lei nº 9.507/1997), a Lei de Arquivos Públicos (Lei nº 8.159/1991), o Código Civil (Lei nº 10.406/2002), o Código de Defesa do Consumidor (Lei nº 8.078/1990), a Lei de Acesso à Informação (Lei nº 12.527/2011), Lei de Cadastro Positivo (Lei nº 12.414/2011), e, mais recentemente, o Marco Civil da Internet (Lei nº 13.965/2014. Naturalmente, a fundamentação avança de forma mais densa sobre a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) e atos normativos produzidos pela ANPD, que visam regulamentar pontos abertos da norma. Por fim, nossa fundamentação jurídica se baseia em estudos de casos e revisão de literatura internacional e no direito comparado, com destaque para o Regulamento de Proteção de Dados Pessoais da União Europeia. Sobre este último ponto, importa enfatizar que a fundamentação se concentra principalmente no direito brasileiro, com referências comparativas principalmente ao direito da União Europeia, e lateralmente às Américas, incluindo os Estados Unidos. Sendo assim, argumentamos que a tese é construída a partir da interpretação do sistema jurídico brasileiro de proteção de dados pessoais, comparando-o ao modelo da União Europeia, mas é relevante para todos os sistemas legais e áreas do Direito Regulatório, em especial, da disciplina da proteção de dados pessoais.

[51] Além do princípio da boa-fé disposto no caput do at. 6º da LGPD, os demais princípio são: (i) finalidade: o tratamento de dados pessoais deve ser realizado para finalidades legítimas, específicas, explícitas e informadas ao titular, observados os seus propósitos originários; (ii) adequação: o tratamento de dados pessoais deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento; (iii) necessidade: o tratamento de dados pessoais deve ser limitado ao mínimo necessário para a realização de suas finalidades, com a inclusão dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; (iv) livre acesso: é garantido aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; (v) qualidade dos dados: é garantido aos titulares que seus dados sejam exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; (vi) transparência: é garantido aos titulares o direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; (vii) segurança: devem ser utilizadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; (viii) prevenção: devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; (ix) não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e (x) responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Escolhas metodológicas: método hipotético-dedutivo, materiais e métodos, direito comparado e aproveitamento de experiência adquirida

A pesquisa é desenvolvida pelo método hipotético-dedutivo,[52] uma vez que o pesquisador elegeu um conjunto de proposições hipotéticas, as quais acredita serem viáveis e adequadas para analisar o objeto da pesquisa, com o fito de comprová-las ou rejeitá-las argumentativamente. Para tanto, a abordagem do objeto da pesquisa é qualitativa, pois pretende se valer de pesquisa bibliográfica e documental pertinente à temática em foco, analisada e fichada na fase exploratória, para abordar o problema. Além disso, orientações, indicações e brainstormings fundamentais para o desenvolvimento do trabalho partiram de aulas, palestras e encontros ocorridos dentro e fora da Universidade, em especial, com a orientadora e membros da banca.

Do ponto de vista da coleta de material, substancial parte do trabalho foi desenvolvida com pesquisa bibliográfica na internet, a partir do acesso aos sites de revistas, periódicos e dos principais centros de pesquisa ao redor do mundo. Em síntese, os seguintes componentes do estudo e metodologias associadas foram selecionados para alcançar os objetivos: (i) revisão do escopo da literatura científica relevante e de publicações de centros de pesquisa, incluindo artigos publicados em revistas científicas revisadas por pares ou anais de conferências, pesquisas, livros, artigos publicados, relatórios ou trabalhos de pré-impressão (*draft*) em repositórios científicos; (ii) estudos de caso: revisão de páginas da web de universidades latino-americanas, europeias e norte americanas ou outras instituições de pesquisa e organismos internacionais; (iii) análise doutrinária: análise abrangente da doutrina jurídica, incluindo decisões de Tribunais, (iv) análise de mídia: análise de conteúdo de documentos de mídia, incluindo jornais, revistas, anuários etc.

Foi realizado levantamento de publicações nacionais e internacionais, notadamente obras sobre direito, tecnologia e segurança da informação e ciências sociais aplicadas que permitiram a análise e a reflexão crítica das questões teóricas envolvidas. Foram buscadas, ainda, fontes no direito estrangeiro para fins de ampliação da perspectiva do ordenamento jurídico brasileiro quanto ao objeto da tese. Neste ponto, acreditamos que cumprimos também a função do uso do método do direito comparado, pois, em relação ao tema estudado, ele serviu para tornar

[52] O método hipotético-dedutivo, desenvolvido por Karl Popper, pressupõe um *conhecimento prévio*, no qual é possível identificar um *problema.* É ofertada uma tentativa de solução provisória, uma *conjectura*, que passa a ser analisada para saber se é refutável, pelo processo denominado *falseamento*.

evidentes as semelhanças e diferenças entre as regulações jurídicas existentes em sistemas jurídicos distintos e nos ajudar a comprovar que a tese tem o potencial de ser aplicável a sistemas jurídicos distintos, conferindo ao mesmo tempo força e flexibilidade aos argumentos.

Neste trabalho a interpretação legislativa relacionada à privacidade e à proteção de dados pessoais é analisada e sintetizada, em especial no que tange aos requisitos de legitimidade do tratamento de dados. Estabelecemos conexões entre os requisitos do tratamento na legislação de proteção de dados, fornecemos uma análise conceitual crítica ao sugerir novas regras, interpretações inabituais sobre princípios, normas, diretrizes interpretativas e valores. Ao falar do contexto nacional, analisamos e sistematizamos parte da jurisprudência do STF sobre privacidade e proteção de dados pessoais, de modo a tentar extrair os contornos do que seria uma "doutrina brasileira da proporcionalidade no tratamento de dados pessoais".

A pesquisa é orientada para a reforma e é comparativa entre distintos sistemas legais, principalmente a LGPD e, secundariamente, o sistema de proteção de dados da União Europeia, o que não inclui legislação específica local. A decisão de focar principalmente no sistema de proteção de dados do Brasil e secundariamente no da União Europeia foi baseada no fato de o Brasil e a União Europeia possuírem normas gerais e compreensivas de proteção de dados pessoais substancialmente semelhantes nas áreas que examinamos, notadamente as bases legais, os princípios, os requisitos de transparência e a concepção de avaliações da proporcionalidade do tratamento de dados.

Por último, nossa tese se destaca pelo caráter interdisciplinar, ao explorar a aplicação do Direito na regulação das tecnologias em contextos sofisticados. Defendemos que as novas tecnologias exigem uma resposta regulatória em proteção de dados que seja específica – e que regular essas inovações oferece valiosas lições sobre regulação em geral. Tecnologias emergentes, como a inteligência artificial, apresentam desafios diferentes dos enfrentados por inovações passadas, como automóveis, satélites, telefones ou a internet, pois elas reconfiguraram o núcleo da nossa sociedade de maneira tão profunda e rápida que se torna necessário revisar algumas das bases fundamentais das regras sociais, em especial o ordenamento jurídico. Não subestimamos o impacto transformador que tecnologias anteriores como a internet tiveram sobre a sociedade. Contudo, o diferencial da inteligência artificial, especialmente em sua recente proliferação, reside na intensidade e velocidade das mudanças estruturais. Nesse cenário, propomos uma reflexão: de um lado, existe a possibilidade de que as leis devam restaurar o *status quo* anterior às disrupções causadas por novas tecnologias, ou, ao menos, moderar seu ritmo e intensidade de mudança. De outro lado, essas inovações podem

oferecer uma oportunidade singular para reestruturar o ordenamento jurídico (ou sua interpretação), com o objetivo de promover e proteger direitos de maneira ainda mais efetiva.

BIBLIOGRAFIA

CQUISTI, Alessandro et al. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys*, v. 50, n. 3, art. 44, 2017.

ACQUISTI, Alessandro. Nudging Privacy: The Behavioral Economics of Personal Information. *IEEE Security & Privacy*, v. 6, p. 82–85, 2009.

ALBERS, Marion. A complexidade da proteção de dados. *Direitos Fundamentais & Justiça*, Belo Horizonte, v. 10, n. 35, p. 39–40, jul./dez. 2016.

ALEXY, Robert. *Teoria dos direitos fundamentais*. Tradução: Virgílio Afonso da Silva. 2. ed. São Paulo: Malheiros, 2015.

ALVES, Fabricio da Mota. Desafios da adequação do poder público à LGPD. In: PALHARES, Felipe; THOMAZ, Alan Campos Elias (Coord.). *Temas atuais de proteção de dados*. São Paulo: Revista dos Tribunais, 2020. p. 171–195.

ARAUJO, Bernardo José Oliveira; BECKER, Daniel. Comentários ao capítulo VIII. In: FEIGELSON, Bruno; BECKER, Daniel; CAMARINHA, Sylvia (Coord.). *Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018*. São Paulo: Thomson Reuters Brasil, 2020.

ARAUJO, Bernardo José Oliveira; BECKER, Daniel. Comentários ao capítulo IX. In: FEIGELSON, Bruno; BECKER, Daniel; CAMARINHA, Sylvia (Coord.). *Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018*. São Paulo: Thomson Reuters Brasil, 2020.

ARAUJO, Bernardo José Oliveira. Capte-me, rapte-me, adapte-me: a complexidade da proteção de dados pessoais em blockchains. In: *Cryptolaw: inovação, direito e desenvolvimento*. São Paulo: Almedina, 2020. p. 207–227.

ARAUJO, Bernardo José Oliveira. LGPD Flash: agilidade em privacidade e proteção de dados. In: BECKER, Daniel; FERRARI, Isabela (Coord.). *Regulação 4.0*, v. II: Desafios da regulação diante de um novo paradigma científico. São Paulo: Thomson Reuters Brasil, 2020. p. 323–358.

ARAUJO, Bernardo José Oliveira. Respeitando princípios no compartilhamento de dados: bases de um raciocínio jurídico. *Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro*, v. 4, p. 1–24, 2021.

ARAUJO, Bernardo José Oliveira; FERRARI, Isabela. Relatório de Impacto à Proteção de Dados Pessoais. Parte I: contexto, abrangência e escalabilidade. In: VAUGHN, Gustavo Favero; BERGSTRÖM, Gustavo Tank; FABER, Bárbara Breda (Org.). *Primeiras impressões sobre a Lei Geral de Proteção de Dados — LGPD*. Ribeirão Preto: Migalhas, 2021. p. 335–363.

ARAUJO, Bernardo José Oliveira; FERRARI, Isabela. Relatório de Impacto à Proteção de Dados Pessoais. Parte II: documentação e etapas de seu desenvolvimento. In: VAUGHN, Gustavo Favero; BERGSTRÖM, Gustavo Tank; FABER, Bárbara Breda (Org.). *Primeiras impressões sobre a Lei Geral de Proteção de Dados — LGPD*. Ribeirão Preto: Migalhas, 2021. p. 365–396.

ARBIX, Daniel. A importância da privacidade por design e por default. In: MENDES, Laura Schertel; DONEDA, Danilo; CUEVA, Ricardo Villas Bôas (Coord.). *Lei Geral de Proteção de Dados (Lei 13.709/2018): a caminho da efetividade*. São Paulo: Revista dos Tribunais, 2020. p. 55–64.

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 03/2013 on purpose limitation* (WP 203). Bruxelas: European Commission, 2 abr. 2013. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 05/2014 on anonymisation techniques* (WP 216). Bruxelas: European Commission, 10 abr. 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (WP 217). Bruxelas: European Commission, 9 abr. 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

AUTIO, Carol et al. *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile* (NIST AI 600-1). Gaithersburg: National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.AI.600-1. Disponível em: https://doi.org/10.6028/NIST.AI.600-1.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia Orientativo: hipóteses legais de tratamento de dados pessoais — legítimo interesse*. Brasília: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf.

BANISAR, David. *National Comprehensive Data Protection/Privacy Laws and Bills 2025*. [S.l.]: SSRN, 28 jan. 2025. Disponível em: http://dx.doi.org/10.2139/ssrn.1951416.

BAPTISTA, Patrícia; KELLER, Clara Iglesias. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. *Revista de Direito Administrativo*, Rio de Janeiro, v. 273, p. 123–163, set. 2016. ISSN 2238-5177.

BARCELLOS, Ana Paula de. *Curso de direito constitucional*. Rio de Janeiro: Forense, 2018.

BARROSO, Luís Roberto. A viagem redonda: habeas data, direitos constitucionais e provas ilícitas. In: WAMBIER, Teresa Arruda Alvim (Coord.). *Habeas Data*. São Paulo: Revista dos Tribunais, 1998.

BARROSO, Luís Roberto. *Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo*. 2. ed. São Paulo: Saraiva, 2010.

BARROSO, Luís Roberto. *Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo*. 9. ed. São Paulo: SaraivaJur, 2020.

BARROSO, Luís Roberto. *Interpretação e aplicação da Constituição: fundamentos de uma dogmática constitucional transformadora*. 7. ed. São Paulo: Saraiva, 2009.

BARROSO, Luís Roberto. Neoconstitucionalismo e constitucionalização do Direito: o triunfo tardio do Direito Constitucional no Brasil. *Revista Interesse Público*, Belo Horizonte, v. 7, n. 33, set./out. 2005.

BELLIZZE, Marco Aurélio; PEREIRA LOPES, Isabela Maria. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: FRAZÃO, Ana; TEPEDINO, Gustavo; DONATO, Milena (Coord.). *Lei Geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020.

BIONI, Bruno Ricardo; DANTAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. *Civilistica.com*, a. 9, n. 3, 2020.

BIONI, Bruno Ricardo; DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2020.

BIONI, Bruno Ricardo; KITAYAMA, Marina; RIELLI, Mariana. *O Legítimo Interesse na LGPD: quadro geral e exemplos de aplicação*. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021.

BODIN DE MORAES, Maria Celina; QUINELATO DE QUEIROZ, João. Autodeterminação informativa e responsabilização proativa. In: *Proteção de dados pessoais: privacidade versus avanço tecnológico*. Cadernos Adenauer, Rio de Janeiro, ano XX, n. 3, p. 113–135, 2019.

BRANDEIS, Louis. The Right to Privacy. *Civilistica.com*, Rio de Janeiro, v. 2, n. 3, p. 1–22, 2013.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília: Senado Federal, 1988.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, 15 ago. 2018. Seção 1, p. 59.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). *Glossário de Proteção de Dados Pessoais e Privacidade*. Brasília: ANPD, [s.d.].

BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 2.121.904/SP. Relatora: Ministra Nancy Andrighi. Brasília, DF, 11 fev. 2025.

BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 2.147.374/SP. Relator: Ministro Ricardo Villas Bôas Cueva. Brasília, DF, 6 dez. 2024.

BRASIL. Supremo Tribunal Federal. Ação de Descumprimento de Preceito Fundamental n. 695/DF. Relator: Ministro Gilmar Mendes. Brasília, DF, 14 set. 2022.

BRASIL. Supremo Tribunal Federal. Mandado de Segurança n. 36.150 MC. Relator: Ministro Luís Roberto Barroso. Brasília, DF, 10 dez. 2018. DJe 13 dez. 2018.

BRASIL. Supremo Tribunal Federal. Medida Cautelar na Ação Direta de Inconstitucionalidade n. 6.387. Relatora: Ministra Rosa Weber. Brasília, DF, 7 maio 2020. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário n. 418.416. Relator: Ministro Sepúlveda Pertence. Brasília, DF, 10 maio 2006.

BRASIL. Supremo Tribunal Federal. Suspensão de Liminar n. 1.103 MC. Relatora: Ministra Cármen Lúcia. Brasília, DF, 5 fev. 2017. DJe 8 maio 2017.

BÜYÜKSAGIS, Erdem. Towards a Transatlantic Concept of Data Privacy. *Fordham Intellectual Property, Media & Entertainment Law Journal*, v. 30, p. 139, 2019.

BYGRAVE, Lee A. Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. *Oslo Law Review*, v. 4, n. 2, 2017.

CALO, Ryan. Artificial Intelligence Policy: A Primer and Roadmap. *UC Davis Law Review*, Davis, v. 51, p. 399, 2017. Disponível em: https://ssrn.com/abstract=3015350.

CANARIS, Claus-Wilhelm. *Direitos fundamentais e Direito privado*. Tradução: Ingo Wolfgang Sarlet; Paulo Mota Pinto. Coimbra: Almedina, 2006.

COSTELLO, Thomas H. et al. Durably reducing conspiracy beliefs through dialogues with AI. *Science*, v. 385, eadq1814, 2024. DOI: 10.1126/science.adq1814.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. *Revista de Direito Civil Contemporâneo*, São Paulo, v. 13, ano 4, p. 66, out./dez. 2017.

DALLARI, Dalmo de Abreu. El Habeas data en Brasil. *Ius et Praxis*, v. 3, n. 1, 1997.

DE SOUZA, Carlos Affonso Pereira; VIOLA, Mario; PADRÃO, Vinicius. Considerações Iniciais Sobre os Interesses Legítimos do Controlador na Lei Geral de Proteção de Dados Pessoais. *Revista de Direito Público*, v. 16, n. 90, 2019.

DETERMANN, Lothar. No One Owns Data. [S.l.]: SSRN, 2018. Disponível em: https://ssrn.com/abstract=3123957.

DONEDA, Danilo. A Autoridade Nacional de Proteção de Dados e o Conselho Nacional de Proteção de Dados. In: DONEDA, Danilo et al. (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law*, Joaçaba, v. 12, n. 2, p. 91–108, jul./dez. 2011.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados*. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

DONEDA, Danilo. Panorama histórico da proteção de dados. In: BIONI, Bruno Ricardo; DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2020.

DONEDA, Danilo. Princípios de proteção de dados pessoais. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III: Marco Civil da Internet*. São Paulo: Quartier Latin, 2015. t. I, p. 369–379.

DONEDA, Danilo; MACHADO, Diego. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Caderno Especial — A regulação da Criptografia no Direito Brasileiro*, p. 99–128, dez. 2018.

DONG, B. et al. Higher-dimensional processing using a photonic tensor core with continuous-time data. *Nature Photonics*, v. 17, p. 1080–1088, 2023.

EBERS, Martin; SEIN, Karin. Data-driven Technologies: Challenges for Privacy and EU Data Protection Law. In: EBERS, Martin; SEIN, Karin (ed.). *Privacy, Data Protection and Data-driven Technologies*. Abingdon: Routledge, 2024. p. 11–12. Disponível em: https://ssrn.com/abstract=4823823.

EUROPEAN DATA PROTECTION BOARD (EDPB). *Report of the work undertaken by the ChatGPT Taskforce*. Bruxelas: EDPB, maio 2024. Disponível em: https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf.

FEIGENBAUM, Edward; SHROBE, Howard. The Japanese national Fifth Generation project: Introduction, survey, and evaluation. *Future Generation Computer Systems*, Amsterdam, v. 9, n. 2, p. 105–117, 1993. ISSN 0167-739X. DOI: 10.1016/0167-739X(93)90003-8.

FERRAZ JR., Tercio Sampaio. Sigilo de dados, o direito à privacidade e os limites do Estado: 25 anos depois. In: ANTONIALLI, Dennys; ABREU, Jacqueline (ed.). *Direitos Fundamentais e Processo Penal da Era Digital: Doutrina e prática em debate*, v. 1.

FERRAZ JR., Tercio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito*, Universidade de São Paulo, v. 88, p. 439–459, 1993.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais: noções introdutórias para a compreensão da importância da lei geral de proteção de dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; DONATO, Milena (Coord.). *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 23–53.

FRAZÃO, Ana. Programas de compliance e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, Andre Gruspun (Coord.). *Governança corporativa: avanços e retrocessos*. São Paulo: Quartier Latin, 2007. p. 42.

GELLERT, Raphaël. We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection. *European Data Protection Law Review*, v. 4, p. 481–492, 2017.

GOMES, Maria Cecília Oliveira. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In: *Temas atuais de proteção de dados*. São Paulo: Thomson Reuters Brasil, 2020. p. 245–271.

GOMES, Maria Cecília Oliveira. Para além de uma obrigação legal: o que a metodologia de benefícios e riscos nos ensina sobre o papel dos relatórios de impacto à proteção de dados. In: *Direito Digital: debates contemporâneos*. São Paulo: Revista dos Tribunais, 2019. p. 141–153.

GONZÁLEZ FUSTER, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Cham: Springer, 2014. DOI: 10.1007/978-3-319-05023-2.

HACKER, Philipp. Comments on the Final Trilogue Version of the AI Act. [S.l.]: SSRN, jan. 2024. Disponível em: https://ssrn.com/abstract=4757603.

HACKER, Philipp. Sustainable AI Regulation. [S.l.]: SSRN, 2023. Disponível em: https://ssrn.com/abstract=4467684.

HACKER, Philipp; CORDES, Johann; ROCHON, Janina. Regulating Gatekeeper AI and Data: Transparency, Access, and Fairness under the DMA, the GDPR, and Beyond. [S.l.]: SSRN, 2022. Disponível em: https://ssrn.com/abstract=4316944.

HACKER, Philipp; PASSOTH, Jan-Hendrik. Varieties of AI Explanations under the Law: From the GDPR to the AIA, and Beyond. In: HOLZINGER, Andreas et al. (ed.). *xxAI — Beyond Explainable AI*. Cham: Springer, 2022. (Lecture Notes in Artificial Intelligence, v. 13200). p. 343–373. DOI: 10.1007/978-3-031-04083-2_17.

HEITZINGER, Clemens; WOLTRAN, Stefan. A Short Introduction to Artificial Intelligence: Methods, Success Stories, and Current Limitations. In: WERTHNER, Hannes et al. (ed.). *Introduction to Digital Humanism*. Cham: Springer, 2024. p. 135–150. DOI: 10.1007/978-3-031-45304-5.

IBDFAM. Caso Elis Regina: o impacto da inteligência artificial na preservação da memória. 13 jul. 2023. Disponível em: https://ibdfam.org.br.

KLOZA, Dariusz; CALVI, Alessandra; CASIRAGHI, Simone; VAZQUEZ MAYMIR, Sergi; IOANNIDIS, Nikolaos; TANAS, Alessia; VAN DIJK, Niels. Data protection impact assessment in the European Union: developing a template for a report from the assessment process. *d.pia.lab Policy Brief*, Bruxelas, n. 1/2020, p. 1–52, 2020. ISSN 2565-9936. Disponível em: https://cris.vub.be/files/62011958/dpialab_pb2020_1_final.pdf.

KLOZA, Dariusz; VAN DIJK, Niels; CASIRAGHI, Simone; VAZQUEZ MAYMIR, Sergi; RODA, Sara; TANAS, Alessia; KONSTANTINOU, Ioulia. Towards a method for data protection impact assessment: making sense of GDPR requirements. *d.pia.lab Policy Brief*, Bruxelas, n. 1/2019, p. 1–12, 2019. ISSN 2565-9936. Disponível em: https://cris.vub.be/files/48091346/dpialab_pb2019_1_final.pdf.

KLOZA, Dariusz; VAN DIJK, Niels; GELLERT, Raphaël; BÖRÖCZ, István; TANAS, Alessia; MANTOVANI, Eugenio; QUINN, Paul. Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals. *d.pia.lab Policy Brief*, Bruxelas, n. 1/2017, p. 1–8, 2017. ISSN 2565-9936. Disponível em: https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf.

KRÖGER, Jacob Leon. Technology Cannot Fix the Privacy Crisis. [S.l.]: SSRN, 2022. Capítulo adaptado de: KRÖGER, Jacob Leon. *Rogue Apps, Hidden Web Tracking and Ubiquitous Sensors*. 2022. Tese (Doutorado) — Technische Universität Berlin, Berlin, 2022. p. 216–219. DOI: 10.14279/depositonce-16043. Disponível em: https://ssrn.com/abstract=4326794.

LEMOS, Ronaldo; BRANCO, Sérgio. Privacy by design: conceito, fundamentos e aplicabilidade na LGPD. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang et al. (Coord.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. p. 447–458.

LEONARDI, Marcel. Legítimo Interesse. *Revista do Advogado*, n. 144, nov. 2019.

LEONARDI, Marcel. Transferência Internacional de Dados Pessoais. In: BIONI, Bruno Ricardo; DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2020. p. 3.

LIMA, Caio César Carvalho. Dos requisitos para o tratamento de dados pessoais. In: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (Coord.). *LGPD: Lei Geral de Proteção de Dados Comentada*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

LYNSKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015.

MATTIUZZO, Marcela; PONCE, Paula Pedigoni. O legítimo interesse e o teste da proporcionalidade: uma proposta interpretativa. *Revista Internet & Sociedade*, v. 1, n. 2, 2020.

MENDES, Gilmar. *Direitos fundamentais e controle de constitucionalidade*. São Paulo: Saraiva, 2012.

MENDES, Gilmar; BRANCO, Paulo. *Curso de Direito Constitucional*. 2. ed. São Paulo: Saraiva, 2008.

MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. *Revista Brasileira de Direitos Fundamentais & Justiça*, Belo Horizonte, v. 12, n. 39, p. 185–216, jul./dez. 2018. DOI: 10.30899/dfj.v12i39.655.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. *Pensar: Revista de Ciências Jurídicas*, Fortaleza, v. 25, n. 4, p. 1–18, out./dez. 2020. DOI: 10.5020/2317-2150.2020.10828.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo*. 2008. Dissertação (Mestrado em Direito) — Faculdade de Direito, Universidade de Brasília, Brasília, 2008.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à Nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados. *Revista de Direito do Consumidor*, v. 120, nov./dez. 2018.

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. STF reconhece direito fundamental à proteção de dados: comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393. *Revista de Direito do Consumidor*, São Paulo, v. 130, p. 471–478, 2020.

MENDES, Laura Schertel; GASIOLA, Gustavo Gil. Compartilhamento de dados na Administração Pública conforme à Constituição: comentários à decisão do STF (ADPF 695 e ADI 6.649). *Revista de Direito do Consumidor*, São Paulo, v. 144, p. 445–455, 2022.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. *Revista dos Tribunais*, São Paulo, v. 108, n. 1009, p. 173–222, nov. 2019.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? *Instituto Igarapé, Artigo Estratégico*, n. 39, 2018. 27 p.

MORRIS, Meredith Ringel et al. Levels of AGI: Operationalizing Progress on the Path to AGI. *arXiv*, 2023. Disponível em: https://arxiv.org/abs/2311.02462.

MULHOLLAND, Caitlin. 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*, v. 19, n. 3, p. 159–180, 2018.

MULHOLLAND, Caitlin. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco? *Revista dos Advogados de São Paulo*, n. 144, nov. 2019.

NOVELLI, Claudio; CASOLARI, Federico; HACKER, Philipp; SPEDICATO, Giorgio; FLORIDI, Luciano. Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity. *Computer Law & Security Review*, Amsterdam, v. 55, art. 106066, 2024. DOI: 10.1016/j.clsr.2024.106066.

NOVELLI, Claudio; HACKER, Philipp; MORLEY, Jessica; TRONDAL, Jarle; FLORIDI, Luciano. A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities. *European Journal of Risk Regulation*, Cambridge, v. 16, p. 566–590, 2024. DOI: 10.1017/err.2024.57.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÓMICO (OCDE). Explanatory memorandum on the updated OECD definition of an AI system. *OECD Artificial Intelligence Papers*, Paris, n. 8, 2024. DOI: 10.1787/623da898-en.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÓMICO (OCDE). *Artificial Intelligence in Science: Challenges, Opportunities and the Future of Research*. Paris: OECD Publishing, 2023. DOI: 10.1787/a8d820bd-en.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÓMICO (OCDE). *Recommendation of the Council concerning Guidelines governing the protection of privacy and transborder flows of personal data*. Paris: OCDE, 1980. Atualizado em 2013. Disponível em: http://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

OLIVEIRA, Rafael Carvalho Rezende. *Curso de direito administrativo*. 9. ed. Rio de Janeiro: Forense, 2021.

PALHARES, Felipe. O relatório de impacto à proteção dos dados pessoais. In: MALDONADO, Viviane Nóbrega (Coord.). *Lei Geral de Proteção de Dados Pessoais: manual de implementação*. São Paulo: Thomson Reuters Brasil, 2019.

PEARL, Judea. *Bayesian Networks*. Los Angeles: Computer Science Department, University of California, 1998. (Technical Report). Disponível em: https://escholarship.org/uc/item/53n4f34m.

QUEIROZ, Rafael Mafei Ribeiro. Como encontrar um bom tema dentro de minha área de interesse? In: QUEIROZ, Rafael Mafei Ribeiro; FEFERBAUM, Marina (Coord.). *Metodologia jurídica: um roteiro prático para trabalhos de conclusão de curso*. São Paulo: Saraiva, 2012.

RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Organização: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda; Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RUBINSTEIN, Ira; HARTZOG, Woodrow. Anonymization and Risk. *Washington Law Review*, v. 91, p. 703, 2016.

RUBINSTEIN, Ira; PETKOVA, Bilyana. The International Impact of the General Data Protection Regulation. In: COLE, Marc; BOEHM, Franziska (ed.). *Commentary on the General Data Protection Regulation*. Cheltenham: Edward Elgar, 2018.

RUSSELL, Stuart; NORVIG, Peter. *Artificial Intelligence: A Modern Approach*. 4. ed. Hoboken: Pearson, 2020. ISBN 9780134610993.

SAMOILI, Sofia et al. *AI Watch. Defining Artificial Intelligence 2.0: Towards an operational definition and taxonomy of AI for the AI landscape*. Luxembourg: Publications Office of the European Union, 2021. (EUR 30873 EN). DOI: 10.2760/01990.

SAMPAIO, José Adércio Leite. A suprema inviolabilidade: a intimidade informática e o sigilo bancário. In: SARMENTO, Daniel; SARLET, Ingo Wolfgang (Coord.). *Direitos fundamentais no Supremo Tribunal Federal: balanço e crítica*. Rio de Janeiro: Lumen Juris, 2011.

SARLET, Ingo Wolfgang (Coord.). *A Constituição concretizada: construindo pontes para o público e o privado*. Porto Alegre: Livraria do Advogado, 2000.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional*. 13. ed. Porto Alegre: Livraria do Advogado, 2018.

SARLET, Ingo Wolfgang. Direitos fundamentais e direito privado: algumas considerações em torno da vinculação dos particulares aos direitos fundamentais. In: SARLET, Ingo Wolfgang (Coord.). *A Constituição concretizada: construindo pontes para o público e o privado*. Porto Alegre: Livraria do Advogado, 2000.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. *Direitos Fundamentais & Justiça*, Belo Horizonte, v. 14, n. 42, p. 179–218, jan./jun. 2020.

SARLET, Ingo Wolfgang; FERREIRA NETO, Arthur M. *O direito ao "esquecimento" na sociedade de informação*. Porto Alegre: Livraria do Advogado, 2018.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*. 3. ed. São Paulo: Revista dos Tribunais, 2014.

SARMENTO, Daniel. *Direitos fundamentais e relações privadas*. Rio de Janeiro: Lumen Juris, 2003.

SCHREIBER, Anderson. *Direitos da Personalidade*. São Paulo: Atlas, 2014.

SCHREIBER, Anderson. Responsabilidade Civil na Lei Geral de Proteção de Dados Pessoais. In: DONEDA, Danilo et al. (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

SOLOVE, Daniel J. A regulatory roadmap to AI and privacy. *IAPP*, jan. 2024. Disponível em: https://iapp.org/news/a/a-regulatory-roadmap-to-ai-and-privacy/.

SOLOVE, Daniel J. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, Philadelphia, v. 154, n. 3, p. 477–564, 2006. Disponível em: https://ssrn.com/abstract=667622.

SOLOVE, Daniel J. Artificial Intelligence and Privacy. *Florida Law Review*, Gainesville, v. 77, n. 1, p. 1, 2025. Disponível em: https://ssrn.com/abstract=4713111.

SOLOVE, Daniel J.; HARTZOG, Woodrow. Kafka in the Age of AI and the Futility of Privacy as Control. *Boston University Law Review*, Boston, v. 104, p. 1021, 2024. Disponível em: https://ssrn.com/abstract=4685553.

SOLOVE, Daniel J.; HARTZOG, Woodrow. The Great Scrape: The Clash Between Scraping and Privacy. *California Law Review*, v. 113, p. 1521, 2025. Disponível em: https://ssrn.com/abstract=4884485.

SOLOVE, Daniel J.; SCHWARTZ, Paul M. *ALI Data Privacy: Overview and Black Letter Text*. [S.l.]: SSRN, 2019. Disponível em: https://ssrn.com/abstract=3360481.

SOMBRA, Thiago Luís; CASTELLANO, Ana Carolina Heringer. Plano de Resposta a Incidentes de Segurança: reagindo rápido e de forma efetiva. *Revista do Advogado*, n. 144, 2019.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica.com*, Rio de Janeiro, v. 9, n. 1, p. 1–38, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/510.

TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. *Fundamentos do Direito Civil: Responsabilidade Civil*, v. 4. Rio de Janeiro: Forense, 2020.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão no Processo C-131/12. *Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Luxemburgo, 13 maio 2014. Disponível em: https://curia.europa.eu/juris/document/document_print.jsf?doclang=PT&docid=152065.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão no Processo C-252/21. *Meta Platforms Inc. e outros v. Bundeskartellamt*. Luxemburgo, 4 jul. 2023. Disponível em: https://curia.europa.eu/juris/document/document.jsf?docid=275125.

TURING, Alan M. Computing machinery and intelligence. *Mind*, Oxford, v. LIX, n. 236, p. 433–460, out. 1950.

UNESCO. *Currículos de IA para a educação básica: um mapeamento de currículos de IA aprovados pelos governos*. Paris: UNESCO, 2022. (ED-2022/FLI-ICT/K-12).

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, L 119, p. 1–88, 4 maio 2016.

UNITED STATES CONGRESS. *United States Code*. Washington, D.C.: U.S. Government Publishing Office, 2025. Disponível em: https://uscode.house.gov.

VAINZOF, Rony. Art. 5º, incisos VI e VII. In: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (Coord.). *LGPD: Lei Geral de Proteção de Dados Comentada*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

VEMOU, Konstantina; KARYDA, Maria. An evaluation framework for privacy impact assessment methods. *ResearchGate*, 2018.

VIOLA, Mario; DE TEFFÉ, Chiara. Tratamento de Dados Pessoais na LGPD: Estudo Sobre as Bases Legais dos Artigos 7.º e 11. In: BIONI, Bruno Ricardo; DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2020.

VOSS, Gregory. Europe and cyberspace — Data protection. *Encyclopédie d'histoire numérique de l'Europe* [online], ISSN 2677-6588, 1 set. 2021. Disponível em: https://ehne.fr.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review*, Cambridge, v. 4, n. 5, p. 193–220, dez. 1890.

WIMMER, Miriam. O Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. In: BIONI, Bruno Ricardo; DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2020.

WIMMER, Miriam. Os desafios do enforcement na LGPD: fiscalização, aplicação de sanções administrativas e coordenação intergovernamental. In: DONEDA, Danilo et al. (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 375–387.