CENTRO UNIVERSITÁRIO CURITIBA – UNICURITIBA PROGRAMA DE MESTRADO EM DIREITO EMPRESARIAL E CIDADANIA

PEDRO RYCARDO COUTO DA SILVA

A EFICÁCIA JURÍDICA CONSTITUCIONAL DA LGPD DIANTE DOS VALORES FUNDAMENTAIS DA PESSOA NO BRASIL E SEUS REFLEXOS NO ÂMBITO EMPRESARIAL

Curitiba, 2025

PEDRO RYCARDO COUTO DA SILVA

A EFICÁCIA JURÍDICA CONSTITUCIONAL DA LGPD DIANTE DOS VALORES FUNDAMENTAIS DA PESSOA NO BRASIL E SEUS REFLEXOS NO ÂMBITO EMPRESARIAL

Projeto de dissertação apresentado ao Programa de Pós- Graduação em Direito, como requisito parcial do programa de Mestrado. Área de concentração: estudo do Direito Empresarial em paralelo com a Cidadania. Linhas de Pesquisa: ATIVIDADE EMPRESARIAL E CONSTITUIÇÃO: inclusão e sustentabilidade.
Orientador: Prof. Dr. Clayton Reis.

Curitiba, 2025

PEDRO RYCARDO COUTO DA SILVA

A EFICÁCIA JURÍDICA CONSTITUCIONAL DA LGPD DIANTE DOS VALORES FUNDAMENTAIS DA PESSOA NO BRASIL E SEUS REFLEXOS NO ÂMBITO EMPRESARIAL

Dissertação apresentada ao Programa de Pós-Graduação Stricto Sensu em Direito Empresarial e Cidadania do Centro Universitário Curitiba – UNICURITIBA, como requisito parcial para a obtenção do título de Mestre em Direito.

Aprovada em: ____ de _____ de 2025.

Presidente:

_____

Prof. Dr. Clayton Reis - Orientador

_____

Professor Doutor Luiz Eduardo Gunther - Membro Interno

_____

Professor Doutor Marco Alves - Membro Externo

_____

Professor Doutor Horácio Monteschio - Membro Externo

Curitiba, 2025

Dedico este trabalho a ...

Deus, fonte inesgotável de força e sabedoria, por me proporcionar esta conquista.

Aos meus amados pais, Agenor e Cleyde, por me colocarem no mundo e me oportunizarem condições para o estudo, incentivando-me continuamente com amor, paciência e dedicação—minha gratidão eterna.

À minha querida esposa Carmen e aos meus filhos Levi, Davi e Matteo, por serem a minha inspiração constante, meu porto seguro e por me mostrarem, diariamente, o verdadeiro sentido da vida.

Ao meu estimado orientador, Professor Clayton Reis, pela orientação generosa, apoio inestimável e ensinamentos imprescindíveis durante toda esta caminhada acadêmica.

Estendo meu reconhecimento a todos os professores do mestrado, em especial à Professora Viviane Séllos e à Professora Lindaura, que me despertaram paixão pela vida acadêmica, motivando-me a buscar novos desafios e trilhar o caminho do Doutorado.

A todos que, direta ou indiretamente, contribuíram para esta conquista, o meu sincero e profundo agradecimento.

RESUMO

Esta pesquisa investiga a eficácia jurídica constitucional da Lei Geral de Proteção de Dados Pessoais (LGPD) à luz dos valores fundamentais da pessoa no Brasil, especialmente diante dos desafios impostos pelo ambiente digital contemporâneo. A análise parte da premissa de que os dados pessoais assumiram papel central nas dinâmicas econômicas, sociais e políticas do século XXI, conferindo-lhes um valor estratégico que exige proteção normativa robusta e eficaz. Com base em referencial teórico multidisciplinar e em jurisprudência nacional e internacional, o trabalho examina como a LGPD se articula com os princípios constitucionais da dignidade da pessoa humana, da privacidade, da liberdade e da igualdade. A abordagem metodológica adotada é qualitativa e teórico-normativa, com ênfase na análise crítica da legislação brasileira, dos marcos regulatórios internacionais, como o GDPR europeu, e das decisões dos tribunais superiores. São discutidos temas como o valor econômico dos dados, a responsabilidade civil decorrente de violações à privacidade, a proteção de direitos patrimoniais e extrapatrimoniais dos titulares de dados, bem como a suficiência das sanções previstas para garantir a efetividade da proteção legal. O trabalho também aprofunda a discussão sobre o papel da Autoridade Nacional de Proteção de Dados (ANPD) e os impactos da LGPD na construção de uma cidadania digital. Conclui-se que, embora a LGPD represente um marco legislativo importante, sua eficácia jurídica plena depende de fatores estruturais, culturais e institucionais, sendo imprescindível o fortalecimento da educação digital, da fiscalização e da cultura de respeito aos direitos informacionais. A proteção de dados é reafirmada, portanto, como um direito fundamental de natureza transversal, indispensável à consolidação do Estado Democrático de Direito na era da informação.

Palavras-chave: LGPD. Dados pessoais. Responsabilidade civil. Direitos fundamentais. Privacidade. Dignidade da pessoa humana. Cidadania digital.

ABSTRACT

This research investigates the constitutional legal effectiveness of the Brazilian General Data Protection Law (LGPD) in light of the fundamental values of the individual in Brazil, especially considering the challenges imposed by the contemporary digital environment. The analysis starts from the premise that personal data has assumed a central role in the economic, social, and political dynamics of the 21st century, granting it a strategic value that demands robust and effective normative protection. Based on a multidisciplinary theoretical framework and national and international jurisprudence, the study examines how the LGPD aligns with the constitutional principles of human dignity, privacy, freedom, and equality. The methodological approach adopted is qualitative and theoretical-normative, with emphasis on critical analysis of Brazilian legislation, international regulatory frameworks—such as the European GDPR—and decisions by higher courts. Topics such as the economic value of data, civil liability arising from privacy violations, the protection of patrimonial and non-patrimonial rights of data subjects, and the adequacy of legal sanctions to ensure effective protection are discussed. The paper also deepens the discussion on the role of the Brazilian National Data Protection Authority (ANPD) and the impacts of the LGPD on the construction of digital citizenship. It concludes that, although the LGPD represents an important legislative milestone, its full legal effectiveness depends on structural, cultural, and institutional factors, making it essential to strengthen digital education, oversight mechanisms, and a culture of respect for informational rights. Data protection is thus reaffirmed as a fundamental, transversal right, indispensable to the consolidation of the Democratic Rule of Law in the information age.

Keywords: LGPD. Personal data. Civil liability. Fundamental rights. Privacy. Human dignity. Digital citizenship.

Sumário

INTRODUÇÃO

A proteção de dados pessoais é uma das questões mais prementes do século XXI, configurando-se como um dos direitos fundamentais mais desafiados pela revolução digital. A crescente utilização de tecnologias baseadas em big data[1] e inteligência artificial (IA) transformou a privacidade em um recurso escasso, elevando a necessidade de regulamentação adequada para lidar com o processamento massivo de informações pessoais. No Brasil, a Lei Geral de Proteção de Dados (LGPD), promulgada em 2018, estabelece um marco jurídico que busca proteger a dignidade da pessoa humana em um contexto de transformações tecnológicas sem precedentes (BIONI, 2019).

É imperioso relatar que a relevância da LGPD reside em sua capacidade de articular a proteção de dados pessoais com os valores fundamentais consagrados pela Constituição Federal de 1988, como a privacidade, a igualdade e a liberdade, o que é o cerne desta dissertação. Inspirada na *General Data Protection Regulation* (GDPR)[2] europeia, a LGPD representa um avanço legislativo significativo, ao criar regras específicas para o tratamento de dados em todas as esferas, promovendo a autodeterminação informativa e a transparência nas relações entre indivíduos e organizações (DONEDA, 2019). Contudo, o impacto dessa legislação vai além do seu aspecto regulatório, exigindo uma reflexão sobre sua eficácia jurídica e seu papel na consolidação de uma cidadania digital.

Desse modo, o avanço da economia digital, descrita por autores como Shoshana Zuboff (2015) como "capitalismo de vigilância", coloca os dados pessoais no centro das relações econômicas e sociais. Empresas utilizam algoritmos sofisticados para monitorar, prever e influenciar comportamentos, o que intensifica a exploração de informações pessoais como recurso estratégico. Nesse contexto, a LGPD emerge como uma tentativa de resguardar os

[1] Big Data refere-se ao conjunto de dados massivos, variados e gerados em alta velocidade, que demandam tecnologias avançadas para coleta, armazenamento, processamento e análise. Sua utilização abrange diversas áreas, como negócios, saúde, ciência e segurança, mas também levanta preocupações éticas e jurídicas relacionadas à privacidade e ao uso responsável dos dados pessoais.

[2] A **General Data Protection Regulation (GDPR)**, ou Regulamento Geral de Proteção de Dados da União Europeia, é um marco regulatório em vigor desde 25 de maio de 2018. Ele estabelece diretrizes para o tratamento de dados pessoais dentro da União Europeia e em transações envolvendo cidadãos europeus, independentemente da localização geográfica do controlador. A GDPR promove princípios como transparência, limitação de finalidade, minimização de dados e responsabilidade, impondo severas sanções para o descumprimento de suas normas.

direitos fundamentais dos cidadãos brasileiros, limitando os abusos de poder por parte de agentes privados e estatais. A proteção de dados, assim, não é apenas um instrumento jurídico, mas também **uma manifestação concreta da dignidade humana no mundo digital** (SARLET; SAAVEDRA, 2020).

Além disso, a proteção de dados pessoais transcende o âmbito individual, configurando-se como uma questão de interesse coletivo. A privacidade, conforme argumenta Stefano Rodotá (2009), é essencial para a construção de sociedades democráticas, ao assegurar a liberdade de expressão e a autonomia individual frente a poderes coercitivos. Dessa forma, a LGPD desempenha um papel crucial na preservação do **pluralismo** e da **igualdade**, valores indispensáveis para a manutenção da ordem democrática brasileira.

A proteção jurídica dos dados pessoais também deve ser analisada em um contexto de **assimetrias estruturais no Brasil**. A desigualdade econômica e a exclusão digital amplificam os desafios na implementação da LGPD, uma vez que grande parte da população permanece alheia aos seus direitos informativos. A concentração de poder tecnológico nas mãos de poucas empresas e governos acentua os riscos de violações à privacidade e à dignidade humana, tornando a eficácia jurídica da LGPD um tema de extrema relevância para a redução das desigualdades e a promoção da justiça social (CASTELLS, 1999).

A relação entre a LGPD e os valores fundamentais da pessoa exige uma análise mais ampla sobre como os dispositivos da lei dialogam com princípios constitucionais. A autodeterminação informativa, um dos pilares da legislação, é intrinsecamente conectada ao direito à privacidade e ao livre desenvolvimento da personalidade. Além disso, o **princípio da dignidade humana** serve como fundamento ético e jurídico para limitar o uso indiscriminado de dados pessoais por agentes econômicos, fortalecendo a posição do indivíduo frente às estruturas de poder (MENDES, 2020; DONEDA, 2019).

No setor público, a aplicação da LGPD apresenta desafios adicionais, sobretudo no que tange à transparência e à responsabilização no uso de dados pelo Estado. A coleta e o tratamento de informações por instituições públicas, muitas vezes sem consentimento ou controle por parte dos cidadãos, levantam questões éticas e jurídicas sobre o equilíbrio entre eficiência administrativa e proteção de direitos fundamentais. Nesse sentido, a LGPD também funciona

como uma barreira contra práticas autoritárias e abusivas, promovendo maior **accountability**[3] e controle social sobre as atividades do poder público (FAIRFIELD; ENGEL, 2015).

Outro aspecto relevante é o impacto da LGPD na promoção de uma cultura de privacidade no Brasil. Pesquisas indicam que, apesar de seu potencial transformador, grande parte das organizações ainda desconhece ou não adota plenamente as exigências da legislação. Essa lacuna prática compromete sua eficácia e evidencia a necessidade de fortalecer os mecanismos de fiscalização e conscientização sobre o tema (CARDOSO, 2020). A implementação efetiva da LGPD depende, portanto, de uma articulação entre sociedade civil, governo e setor privado para consolidar uma cultura de respeito à privacidade e aos valores fundamentais.

No plano internacional, a proteção de dados **ganha status de direito humano, reconhecido por organismos como a Organização das Nações Unidas (ONU) e a UNESCO**. A LGPD insere o Brasil em um movimento global de fortalecimento dos direitos informativos, alinhando-se a iniciativas como a GDPR e contribuindo para a construção de um marco normativo internacional para a regulação da economia digital. Contudo, essa integração também impõe desafios, como a necessidade de harmonizar legislações e superar barreiras culturais e econômicas que dificultam a aplicação uniforme das normas (RODOTÁ, 2009; BIONI, 2019).

A relevância da temática é, portanto, inegável. A LGPD não apenas reflete uma resposta jurídica às demandas de proteção de dados, mas também representa um instrumento de afirmação dos valores constitucionais em um mundo cada vez mais digitalizado. Ao proteger a privacidade e promover a dignidade humana, a legislação fortalece a cidadania e contribui para a construção de uma sociedade mais justa e equitativa. Nesse sentido, a análise da eficácia jurídica da LGPD diante dos valores fundamentais da pessoa no Brasil não é apenas pertinente, mas essencial para compreender as transformações do direito no século XXI.

[3] **Accountability** é um conceito oriundo do direito anglo-saxão que se refere à obrigação de prestação de contas, sendo amplamente utilizado em contextos de governança corporativa e proteção de dados. Na LGPD, o princípio da accountability (art. 6º, X) exige que os agentes de tratamento demonstrem a adoção de medidas eficazes para garantir a conformidade com as normas legais, promovendo transparência e responsabilidade perante os titulares de dados e as autoridades competentes.

1 A CONSTRUÇÃO HISTÓRICA DO CONCEITO JURÍDICO DE PROTEÇÃO DE DADOS

A proteção de dados pessoais tornou-se uma necessidade crescente com o avanço da tecnologia e o aumento exponencial da coleta de informações individuais. A história desse direito fundamental remonta ao período pós-Segunda Guerra Mundial, quando as primeiras legislações sobre privacidade começaram a surgir em resposta ao uso de tecnologias para controle populacional. A **Alemanha** foi pioneira nesse movimento, estabelecendo a primeira lei de proteção de dados no estado de Hesse, em 1970. Essa iniciativa refletia a preocupação com a utilização de sistemas computacionais para armazenar e manipular informações sensíveis.

A Convenção 108 do Conselho da Europa, adotada em 1981, marcou um divisor de águas na consolidação do direito à proteção de dados. Esse tratado internacional estabeleceu princípios como a legalidade, a transparência e a proporcionalidade no uso de informações pessoais, sendo considerado o primeiro instrumento vinculante sobre o tema. Esses marcos foram fundamentais para a consolidação de legislações mais abrangentes, como a Diretiva 95/46/CE da União Europeia, que regulamentou o tratamento de dados pessoais nos países-membros e estabeleceu bases para cooperação internacional.

As primeiras iniciativas de legislar sobre o tema, no Brasil, nasceram na década de 1970. Mas foi a Constituição Federal de 88 que trouxe uma evolução importante do direito à privacidade e à proteção de dados pessoais para o ordenamento brasileiro, prevendo os direitos fundamentais à intimidade, à privacidade, ao sigilo das comunicações e o instituto do habeas data[4].

Em 2004, a matéria foi trazida pela primeira vez ao debate no âmbito do Mercosul. Em seguida, leis setoriais como o Marco Civil da Internet e a Lei de Acesso à Informação trouxeram novos rumos importantes em relação ao assunto no País. Esses diferentes instrumentos aliados a princípios e diretrizes internacionais formaram a gênese da matéria e influenciaram a

[4] DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR. Otávio Luís; BIONI, Bruno (coord.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021, p. 3 – 20.

promulgação da LGPD, publicada em 2018 como norma geral de proteção de dados pessoais para o Brasil.

A LGPD é o resultado de amplo debate multissetorial que expôs uma necessidade da sociedade em um ambiente globalizado e de ampla conexão do indivíduo com a tecnologia. A Lei foi bem recebida pelo setor privado, por trazer regras atuais ao setor, bem como as melhores práticas da área ao serviço público, de modo a orientar a proteção dos titulares de dados.

No Brasil, a proteção de dados pessoais evoluiu de forma mais lenta e fragmentada. Até a promulgação da Lei Geral de Proteção de Dados (LGPD) em 2018, não havia um marco regulatório específico e abrangente. Antes disso, a proteção de dados era tratada em legislações setoriais, como o Código de Defesa do Consumidor e o Marco Civil da Internet, que ofereciam garantias limitadas e muitas vezes insuficientes para acompanhar a crescente complexidade do ambiente digital.

A LGPD surgiu como uma resposta à necessidade de alinhar o Brasil aos padrões internacionais, especialmente à General Data Protection Regulation (GDPR), aprovada na União Europeia em 2016. Inspirada nesse modelo, a legislação brasileira incorporou princípios fundamentais, como a finalidade e a transparência, estabelecendo obrigações claras para controladores e operadores de dados. Além disso, a LGPD criou a Autoridade Nacional de Proteção de Dados (ANPD), responsável pela regulamentação e fiscalização da norma.

O avanço tecnológico trouxe não apenas benefícios, mas também riscos significativos, como o aumento dos vazamentos de dados. Esses incidentes evidenciam a fragilidade dos sistemas de segurança e a necessidade de mecanismos robustos para proteger as informações pessoais. No Brasil, episódios como o vazamento de dados de mais de 223 milhões de cidadãos em 2021[5] expuseram informações sensíveis, incluindo números de CPF e histórico de crédito, gerando prejuízos econômicos e sociais incalculáveis.

Internacionalmente, casos como o escândalo do Facebook-Cambridge Analytica[6]

[5] **Vazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber.** G1, 28 jan. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em: 20 de outubro de 2024.
[6] **Cambridge Analytica: entenda o escândalo que abalou o Facebook.** BBC News Brasil, 19 mar. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 10 de outubro de 2024.

demonstraram o potencial de uso indevido de dados para manipulação de comportamentos e decisões políticas. Esses eventos reforçam a importância de legislações como a LGPD, que busca equilibrar a inovação tecnológica com a preservação dos direitos fundamentais. No entanto, a eficácia dessas normas depende de sua implementação prática e da conscientização dos agentes envolvidos.

A LGPD introduziu medidas importantes para prevenir e mitigar vazamentos de dados, como a **exigência de comunicação imediata de incidentes à ANPD e aos titulares**. Essas disposições visam aumentar a transparência e a responsabilização no tratamento de dados, promovendo maior segurança e confiança no ambiente digital. Contudo, a aplicação efetiva da lei enfrenta desafios significativos, como a falta de infraestrutura adequada e o desconhecimento generalizado sobre seus dispositivos.

A proteção de dados é uma questão global, mas suas implicações locais são profundas. No Brasil, a desigualdade socioeconômica e a exclusão digital amplificam os desafios na implementação da LGPD, tornando ainda mais urgente a necessidade de promover uma cultura de proteção de dados. Isso exige não apenas a aplicação rigorosa da lei, mas também iniciativas educativas que capacitem cidadãos e empresas a compreenderem e respeitarem os princípios da norma.

Além disso, a evolução histórica da proteção de dados está intrinsecamente ligada ao conceito de cidadania digital. Garantir que todos os cidadãos tenham controle sobre suas informações é essencial para a preservação da dignidade humana e do livre desenvolvimento da personalidade. A LGPD desempenha um papel crucial nesse sentido, ao estabelecer mecanismos que reforçam a autonomia individual e promovem a igualdade no acesso aos direitos informativos.

A proteção de dados também é essencial para fortalecer a democracia em tempos de transformação digital. A manipulação de informações pessoais para influenciar decisões eleitorais ou moldar comportamentos de consumo compromete os princípios democráticos e exige uma resposta jurídica contundente. Nesse sentido, a LGPD contribui para a construção de um ambiente mais ético e transparente, no qual os direitos dos titulares são respeitados.

Os vazamentos de dados, contudo, continuam a ser uma ameaça significativa. Mesmo com a existência de legislações robustas, a implementação prática dessas normas é frequentemente prejudicada pela resistência de organizações em adaptar-se às novas exigências. No Brasil, pesquisas indicam que grande parte das empresas ainda não está em conformidade com a LGPD, expondo-se a riscos legais e reputacionais. Vejamos:

> Levantamento realizado pelo Grupo Daryus consultoria especializada no tema, indica que 80% das empresas no Brasil ainda não estão completamente adequadas à LGPD; 35% dizem estar parcialmente adequadas e 24% em fase inicial de adequação.
>
> Realizado em setembro de 2023, o levantamento contempla 200 profissionais de organizações em 16 áreas de atuação, além de órgãos governamentais, em 27 estados brasileiros; 34% são companhias de grande porte com mais de mil funcionários.
>
> Jeferson D'Addario, CEO do Grupo Daryus, comenta que a empresa que se adequa à LGPD, além de cumprir uma regra, contribui com o ecossistema corporativo. "É um trabalho importante para as organizações e deve ser contínuo, já que a informação é um bem valioso para as empresas diante de possíveis ameaças no ambiente digital", destaca.
>
> A preocupação em relação à conformidade e adequação à LGPD é eminente, visto que a **Autoridade Nacional de Proteção de Dados (ANPD)**, autarquia especial responsável por fiscalizar a lei, projeta, para 2023, a publicação do Regulamento de Dosimetria e Aplicação de Sanções Administrativas contra as empresas que não cumprirem a legislação. "Ou seja, muito em breve, teremos notícias das primeiras sanções aplicadas pela agência com base na LGPD", projeta Alexander Coelho, advogado especializado em direito digital e proteção de dados e sócio do escritório Godke Advogados.[7]

[7] FEBRABAN. *LGPD está fora da realidade de 80% das empresas no Brasil, diz estudo*. Disponível em: https://febrabantech.febraban.org.br/blog/lgpd-esta-fora-da-realidade-de-80-das-empresas-no-brasil-diz-estudo. Acesso em: 23 out. 2024.

Desse modo, pode-se afirmar que a proteção de dados não é apenas uma questão técnica, mas também uma questão ética e social. Como aponta Stefano Rodotá, o uso de informações pessoais deve ser orientado por princípios que respeitem a dignidade humana e promovam o bem-estar coletivo. Essa abordagem reforça a necessidade de um arcabouço jurídico que seja ao mesmo tempo eficaz e adaptável às mudanças tecnológicas.

O alinhamento da LGPD com os valores constitucionais brasileiros, como a dignidade da pessoa humana e a igualdade, é um passo essencial para garantir sua eficácia. Esses princípios oferecem uma base sólida para interpretar e aplicar a norma, garantindo que ela não se limite a proteger dados, mas também a promover uma sociedade mais justa e equitativa.

O futuro da proteção de dados no Brasil depende de uma combinação de fatores, incluindo o fortalecimento da ANPD, o engajamento da sociedade civil e o compromisso das empresas em adotar práticas de conformidade. Além disso, a cooperação internacional é fundamental para enfrentar desafios transnacionais, como o tráfico de dados e os ataques cibernéticos.

Assim, a evolução histórica da proteção de dados revela um processo contínuo de adaptação às transformações sociais e tecnológicas. Desde os primeiros marcos na Europa até a promulgação da LGPD, esse movimento reflete a crescente importância da privacidade como um direito fundamental. No entanto, os desafios impostos pelos vazamentos de dados mostram que ainda há muito a ser feito para garantir a plena proteção dos direitos informativos no Brasil.

A eficácia da LGPD depende não apenas de sua aplicação prática, mas também de sua capacidade de gerar uma mudança cultural que valorize a privacidade como um bem comum. Esse é o desafio que permanece à frente, e sua superação será decisiva para o futuro da proteção de dados no país.

1.1 A ORIGEM DO INSTITUTO E SEU DESENVOLVIMENTO NO DIREITO EUROPEU

O livro **"1984"**, de George Orwell, apresenta uma distopia em que uma sociedade é

governada por um regime totalitário que controla os pensamentos e todos os dados dos cidadãos, como imagens e sons. Escrito entre 1947 e 1948, no período pós-Segunda Guerra Mundial, a obra é um alerta contra o controle exacerbado da privacidade pelos governos modernos. Orwell, ao escrever a obra, projetou as possíveis consequências do avanço tecnológico, demonstrando preocupação com a manipulação dessas inovações pelo Estado.

Essa projeção futura de Orwell foi amplamente reconhecida, especialmente com o sucesso da obra, traduzida para diversos países e adaptada culturalmente, como no reality show **"Big Brother"**, inspirado no "Grande Irmão", figura central do romance. Este personagem simboliza o líder que controla a sociedade e todos os dados, reforçando o temor coletivo sobre o uso de informações privadas. O impacto do livro reside no fato de que ele toca profundamente no receio humano em relação à privacidade e ao controle das informações mais íntimas.

A preocupação com o controle da privacidade confirma que o direito à proteção de dados está intrinsecamente ligado ao direito à autodeterminação individual, refletindo a dignidade humana. Por essa razão, a proteção da privacidade é um princípio basilar de diversas declarações de direitos fundamentais, como o artigo 5º da Constituição Federal de 1988. Todavia, à época de sua promulgação, os desafios relacionados ao tratamento de dados pessoais eram modestos comparados aos avanços tecnológicos e às necessidades regulatórias que surgiram nas décadas seguintes.

Na Europa, o desenvolvimento desse direito ocorreu de forma mais estruturada e precoce, sendo a proteção de dados reconhecida como uma extensão do direito à privacidade desde a Convenção Europeia de Direitos Humanos, de 1950, que consagrou o artigo 8º, estabelecendo o direito ao respeito pela vida privada e familiar. Este direito evoluiu com a Convenção de Estrasburgo, de 1981, e foi consolidado com a Diretiva 95/46/CE, que regulamentou o tratamento de dados pessoais e serviu de modelo para legislações em todo o mundo.

A adoção da **Carta de Direitos Fundamentais da União Europeia**, em 2000, e sua posterior vinculação como direito primário, com o Tratado de Lisboa, em 2009, representaram marcos importantes no desenvolvimento desse instituto. O artigo 8º da Carta estabelece o direito à proteção de dados pessoais como um direito fundamental autônomo, consagrando princípios como tratamento leal e consentimento informado. Esses instrumentos impulsionaram a criação

do **Regulamento Geral de Proteção de Dados (GDPR)**, em 2016, que consolidou a regulação europeia como referência global.

No Brasil, a proteção de dados ganhou destaque somente com a Lei nº 13.709, de 14 de agosto de 2018, conhecida como **Lei Geral de Proteção de Dados (LGPD)**. Inspirada no GDPR, a LGPD busca proteger os direitos fundamentais de liberdade e privacidade, regulando o tratamento de dados pessoais no território nacional e impondo obrigações tanto ao setor público quanto ao privado. Apesar de tardia, a LGPD marca o início de uma era regulatória no Brasil, alinhando-se ao movimento global de proteção de dados.

A proteção de dados como instituto jurídico encontra suas *raízes* na Europa, onde o reconhecimento da privacidade como direito fundamental surgiu em resposta ao avanço tecnológico e às suas consequências sobre a liberdade individual. Após a Segunda Guerra Mundial, o continente vivenciou uma reconfiguração de valores jurídicos, tendo como foco a proteção das liberdades básicas. Esse cenário resultou na adoção da Convenção Europeia dos Direitos Humanos, em 1950, cujo artigo 8º estabeleceu o direito à vida privada e familiar, criando a base para regulamentações posteriores voltadas à proteção de dados pessoais (RODOTÁ, 2009).

O uso crescente de sistemas computacionais no armazenamento de informações pessoais, principalmente nos setores público e privado, gerou a necessidade de regulamentação específica. Em 1970, o estado de Hesse, na Alemanha, promulgou a primeira lei de proteção de dados do mundo, limitando o uso de sistemas eletrônicos para coletar, armazenar e processar dados. Esse marco inicial serviu de exemplo para outros países europeus, que começaram a adotar legislações similares para lidar com o aumento exponencial da circulação de informações pessoais (CASTELLS, 1999).

A década de 1980 marcou um momento decisivo na consolidação do instituto. Em 1981, o Conselho da Europa promulgou a Convenção 108, o primeiro tratado internacional juridicamente vinculante voltado exclusivamente à proteção de dados pessoais. Esse tratado foi pioneiro ao estabelecer princípios universais, como a necessidade de consentimento, a limitação de finalidade e o direito de acesso dos titulares às suas informações. A Convenção 108 não apenas influenciou a legislação interna dos Estados-membros, mas também serviu de referência para futuras iniciativas internacionais no tema (BIONI, 2019).

Além disso, a Convenção 108 teve um impacto direto na criação da Diretiva 95/46/CE da União Europeia, considerada um dos marcos mais importantes na história da proteção de dados. Como dito anteriormente, a diretiva padronizou as normas de tratamento de dados nos Estados-membros da União, promovendo uma abordagem uniforme para regulamentar o uso de informações pessoais. Ao exigir a criação de autoridades nacionais independentes para supervisionar a aplicação da lei, a Diretiva 95/46/CE garantiu maior transparência e responsabilização no tratamento de dados pessoais (DONEDA, 2019).

Os avanços tecnológicos que marcaram o início do século XXI, incluindo a **disseminação da internet e o surgimento de grandes plataformas digitais**, trouxeram desafios inéditos para o direito europeu. O volume de dados processados aumentou exponencialmente, e práticas como o uso de algoritmos para segmentação de consumidores e a coleta massiva de informações sem consentimento explícito destacaram as lacunas das regulamentações existentes.

A General Data Protection Regulation (GDPR) introduziu inovações significativas, como o "privacy by design" e o "privacy by default", que exigem a incorporação da proteção de dados desde a concepção de produtos e serviços. Além disso, regulamentou o direito ao esquecimento, permitindo que indivíduos solicitem a exclusão de suas informações em determinadas circunstâncias, um aspecto amplamente debatido e considerado essencial para resguardar a dignidade e a privacidade no ambiente digital (SARLET; SAAVEDRA, 2020).

Outro avanço trazido pela GDPR foi o conceito de **portabilidade de dados**[8], que fortalece a autonomia dos titulares ao permitir a transferência de suas informações entre plataformas de maneira segura e eficiente. Essa disposição não apenas amplia os direitos dos cidadãos europeus, mas também incentiva práticas mais transparentes e éticas por parte das empresas, estabelecendo um modelo que inspira legislações em outros países, como o Brasil, com a LGPD (BIONI, 2019).

[8] A portabilidade de dados é um direito garantido que permite ao titular dos dados solicitar a transferência de suas informações pessoais de uma organização para outra, sempre que tecnicamente viável e respeitadas as exigências legais. Esse direito visa garantir maior autonomia ao titular sobre seus dados e promover a competitividade entre empresas, incentivando práticas mais transparentes e eficientes no tratamento de informações pessoais.(comentários do autor)

Além disso, a expansão territorial da GDPR para além das fronteiras da União Europeia, ao exigir conformidade de empresas estrangeiras que tratam dados de cidadãos europeus, mostrou-se uma estratégia eficaz para estabelecer padrões globais de proteção de dados. Essa abordagem não apenas fortaleceu a proteção dos titulares na Europa, mas também impactou significativamente as práticas corporativas em todo o mundo, criando um ambiente mais seguro para o tratamento de informações (DONEDA, 2019).

A experiência europeia na proteção de dados é amplamente reconhecida como um **modelo de equilíbrio entre inovação tecnológica e segurança jurídica**. Diferentemente de outras regiões, onde a regulamentação muitas vezes é vista como um entrave ao progresso, o direito europeu considera a proteção de dados como uma base para fortalecer a confiança nas relações digitais e promover a competitividade econômica. Essa abordagem enfatiza que privacidade e inovação não são mutuamente excludentes, mas complementares.

A contribuição histórica da Europa para o desenvolvimento do instituto também está relacionada ao reconhecimento de que a proteção de dados é um elemento essencial para a **preservação da democracia**. Durante o período da Guerra Fria, práticas de vigilância em massa destacaram a vulnerabilidade dos cidadãos frente ao uso indiscriminado de informações pelo Estado. Esses precedentes reforçaram a importância de regulamentações que protejam a privacidade individual como um pilar das democracias contemporâneas (RODOTÁ, 2009).

A trajetória do instituto no direito europeu continua a influenciar diretamente outros ordenamentos jurídicos, incluindo o brasileiro. A LGPD, promulgada em 2018, adotou diversos princípios da GDPR, como a transparência, a finalidade e a responsabilização. Essa convergência demonstra como os padrões europeus têm servido de referência para a construção de marcos normativos em diferentes contextos culturais e econômicos (CANAAN, 2018).

Desse modo, a origem e o desenvolvimento do instituto na Europa não apenas destacam a importância de tratar a privacidade como um direito fundamental, mas também refletem a necessidade de um direito dinâmico, capaz de se adaptar às transformações tecnológicas e sociais. A experiência europeia demonstra que a regulamentação da proteção de dados é uma ferramenta indispensável para promover a dignidade humana, a segurança e a inovação de maneira equilibrada e sustentável.

1.2 BALANÇO DOS DADOS DA LGPD NO BRASIL

A implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil trouxe mudanças profundas para o ordenamento jurídico e para as **práticas empresariais e institucionais**. Desde sua entrada em vigor em setembro de 2020, a LGPD se destacou como um marco regulatório que busca equilibrar o uso econômico de dados pessoais com a proteção dos direitos fundamentais. O balanço desses primeiros anos de aplicação evidencia tanto avanços significativos quanto desafios estruturais que ainda precisam ser superados.

A criação da **Autoridade Nacional de Proteção de Dados (ANPD)** foi um passo crucial para a consolidação da LGPD. A ANPD assumiu a função de regulamentar e fiscalizar a aplicação da lei, além de orientar organizações públicas e privadas sobre a conformidade com seus dispositivos. Desde sua criação, a autoridade vem desempenhando um papel relevante no estabelecimento de diretrizes, como a definição de bases legais para o tratamento de dados e a delimitação de penalidades administrativas para infrações (BRASIL, 2018).

Cabe mencionar que a ANPD tem desempenhado um papel crucial na implementação e fiscalização da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. Entre suas principais realizações e implementações, destacam-se as regulamentações e normativas, como a aprovação de diversas resoluções que detalham aspectos específicos da LGPD. Um **exemplo é a Resolução CD/ANPD nº 19, de 23 de agosto de 2024**[9], que regulamenta a transferência internacional de dados e estabelece cláusulas-padrão contratuais. Além disso, a ANPD publicou guias orientativos, como o "Guia Orientativo sobre Agentes de Tratamento e Encarregado", que esclarece as funções de controlador, operador e encarregado.

No âmbito da fiscalização e aplicação de sanções, a ANPD iniciou processos administrativos para investigar possíveis infrações à LGPD. Em novembro de 2024, por exemplo, instaurou um processo contra o TikTok por tratamento irregular de dados de crianças e adolescentes.[10] A ANPD também aprovou o regulamento de dosimetria, que define critérios

[9] AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. *Resolução CD/ANPD nº 19, de 23 de agosto de 2024.* Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396. Acesso em: 27 out. 2024.

[10] AGÊNCIA BRASIL. *Governo processa TikTok por tratamento irregular de dados de crianças.* Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2024-11/governo-processa-tik-tok-por-tratamento-irregular-de-dados-de-criancas. Acesso em: 25 out. 2024.

para a aplicação de sanções administrativas, garantindo transparência e proporcionalidade.

A ANPD promoveu engajamento e participação social por meio de consultas e audiências públicas, com o objetivo de coletar contribuições da sociedade na elaboração de normativas, fomentando um ambiente regulatório participativo. Entre as iniciativas nessa área, destaca-se o lançamento de séries de publicações técnicas, como o "Radar Tecnológico", que aborda tecnologias emergentes e seu impacto na proteção de dados pessoais.

No planejamento estratégico, a ANPD estabeleceu agendas regulatórias bienais, definindo prioridades e cronogramas para a criação de regulamentações e ações estratégicas. No **planejamento 2024-2027**, foram definidos objetivos para ampliar a prevenção, detecção e repressão às infrações à LGPD, além de promover a cidadania e impulsionar a inovação na área de proteção de dados.

Essas iniciativas refletem o compromisso da ANPD em consolidar a cultura de proteção de dados no Brasil, assegurando os direitos dos titulares e orientando os agentes de tratamento na conformidade com a LGPD (GOVERNO FEDERAL, 2024).

O setor público também enfrenta dificuldades significativas. Embora a LGPD se aplique a órgãos governamentais, muitas instituições ainda não estão adequadamente estruturadas para cumprir suas exigências. A **falta de investimentos em tecnologia e treinamento de pessoal** é um obstáculo importante, que compromete a proteção de dados de milhões de brasileiros que utilizam serviços públicos (CORTÊS, 2020). Esse cenário contrasta com a abordagem de países como a Alemanha, onde a proteção de dados é uma prioridade institucional amplamente consolidada (RODOTÁ, 2009).

A aplicação de sanções pela ANPD é um aspecto que ainda está em fase de amadurecimento. Apesar de a LGPD prever multas e outras penalidades para infrações, o foco inicial da ANPD tem sido a educação e a conscientização, em vez da imposição de sanções severas. Essa abordagem pedagógica é compreensível no contexto de um marco regulatório recente, mas também levanta questionamentos sobre a eficácia da lei em coibir práticas abusivas (SARLET; SAAVEDRA, 2020).

O mercado de trabalho também foi impactado pela LGPD. A demanda por profissionais especializados em proteção de dados, como *Data Protection Officers (DPOs)*, aumentou significativamente, criando oportunidades, mas também evidenciando a escassez de mão de obra qualificada. Instituições de ensino superior e organizações profissionais têm respondido a essa demanda com a criação de cursos e certificações específicas, mas o déficit de profissionais ainda representa um gargalo (BIONI, 2019).

Outro ponto relevante é o impacto da LGPD sobre o **comércio eletrônico**. O setor foi um dos mais afetados pela regulamentação, dada a sua dependência de dados pessoais para personalização de ofertas e campanhas de marketing. Muitos e-commerces precisaram revisar suas políticas de privacidade e práticas de coleta de dados para garantir conformidade, o que resultou em custos adicionais, mas também em maior confiança por parte dos consumidores.

Além da personalização de ofertas e campanhas, o impacto da LGPD no e-commerce também pode ser observado na logística e na cadeia de suprimentos, especialmente no que tange ao armazenamento e compartilhamento de dados dos consumidores. De acordo com o estudo de Franco et al. (2021), transportadoras que operam no setor de e-commerce enfrentam o desafio de proteger dados sensíveis, como informações contidas em notas fiscais e endereços de entrega. A adequação à LGPD exige investimentos em tecnologia, treinamento de pessoal e revisão de processos para garantir a segurança e conformidade, sendo essa uma questão central para manter a confiança do consumidor e evitar sanções legais.

Ademais, a legislação também introduziu novos parâmetros para o tratamento de dados no transporte e entrega de mercadorias, como o uso responsável de dados sensíveis pelos motoristas e a rastreabilidade das informações durante todo o processo. Essas exigências têm sido encaradas como diferenciais competitivos para empresas que adotam boas práticas, promovendo maior segurança e satisfação do cliente (FRANCO et al., 2021). Por fim, a LGPD se consolida como um marco para fortalecer o ambiente digital no Brasil, incentivando práticas responsáveis em todas as etapas do ciclo comercial.

A legislação também trouxe desafios específicos para pequenas e médias empresas (PMEs), que muitas vezes não possuem os recursos necessários para implementar programas de conformidade. Iniciativas como a simplificação de normas para empresas de pequeno porte,

lideradas pela ANPD, são um esforço positivo para garantir que a LGPD seja acessível a todos os setores da economia. No entanto, a falta de apoio financeiro e técnico ainda é uma barreira para muitas PMEs (CARDOSO, 2020).

A influência da LGPD no comportamento dos titulares de dados é outro aspecto importante a ser destacado. Muitos brasileiros passaram a exercer ativamente seus direitos previstos na lei, como o direito de acesso, retificação e exclusão de dados. Esse engajamento é fundamental para a efetividade da LGPD, pois incentiva as organizações a adotarem práticas mais transparentes e responsáveis no tratamento de informações (MENDES, 2020).

A relação entre a LGPD e os valores constitucionais brasileiros também merece destaque. A proteção de dados pessoais está intimamente ligada à dignidade da pessoa humana, à liberdade e à privacidade, que são pilares do ordenamento jurídico brasileiro. Nesse sentido, a LGPD não apenas regula o tratamento de dados, mas também reforça a proteção de direitos fundamentais, promovendo um equilíbrio entre inovação tecnológica e segurança jurídica (SARLET; SAAVEDRA, 2020).

A análise do balanço da LGPD no Brasil evidencia que, embora avanços significativos tenham sido alcançados, **ainda há um longo caminho a percorrer**. A legislação é robusta em seus princípios e diretrizes, mas sua aplicação prática depende de fatores como o fortalecimento da ANPD, a capacitação de profissionais e a conscientização da sociedade. Esses elementos são indispensáveis para que a LGPD cumpra seu objetivo de proteger os dados pessoais dos brasileiros e promover a confiança no ambiente digital.

1.3 CONTEXTO NORMATIVO INTERNACIONAL E A ADEQUAÇÃO DA LEGISLAÇÃO BRASILEIRA AO CENÁRIO GLOBAL

O Brasil, com a publicação da Lei Geral de Proteção de Dados - LGPD em 14/8/18, deu um importante passo para fazer parte do contexto internacional de regulação da proteção de dados e privacidade, cujas regras estão sendo ditadas pelo modelo regulatório europeu - GDPR.

Neste *contexto internacional*, a privacidade é valor **ex ante**, a ser tratada como padrão

e princípio; o livre consentimento (qualificado ou adjetivado) do usuário titular dos dados pessoais é condição prévia para o processo de tratamento; o tratamento deve obedecer importantes princípios, como o da boa-fé, da finalidade, da adequação e da não-discriminação; o controle do usuário sobre toda a cadeia de tratamento deve ser garantido pelos agentes de tratamento; as autoridades independentes têm ampla atuação, preventiva e repressiva, com várias funções previstas na lei.

Essa sistemática legal internacional em que se insere a LGPD é voltada para **reduzir a assimetria da relação jurídica**, técnica e econômica do titular de dados com o agente de tratamento de dados. Neste aspecto, ela se assemelha a outras legislações que também enfrentam esse tipo desigual de relação, como o Código de Defesa do Consumidor (CDC) e a Consolidação das Leis do Trabalho (CLT).

Outra peculiaridade das legislações é a previsão de aplicação extraterritorial com a exigência de adequação de outros países, gerando um efeito cascata, em que fomenta a produção ou revisão de normas sobre privacidade em todo o mundo. Outrossim, uma empresa adequada à lei tende a exigir de outras empresas o mesmo padrão de segurança, como condição prévia para o compartilhamento de dados pessoais.

O maior e mais populoso país da América do Sul constroi a sua regulação de proteção de dados e privacidade visando alcançar o nível de adequação correspondente ao nível da Europa e de outros países que já estão mais avançados na discussão sobre o tema e já adequados às normas emanadas deste epicentro, como os nossos vizinhos fronteiriços, Uruguai e Argentina.

Ocorre que esta entrada não ocorreu da forma ideal. Logo de partida, a LGPD sofreu veto presidencial importante, que impediu a imediata instalação de uma Autoridade Nacional de Proteção de Dados - ANPD, responsável por uma série de funções fundamentais para a aplicação da **ratio legis**, como zelar pela proteção dos dados pessoais, editar políticas e procedimentos importantes, além de fiscalizar a aplicação da lei, entre outras funções.

Em um segundo momento, tal fato veio a ser parcialmente corrigido, com a edição da MP 869 de 27/12/18. Diz-se parcialmente por que a ANPD introduzida pela referida MP veio sem a autonomia e a independência que se esperava, em comparação à ANPD do PL 53/18.

Não é preciso ressaltar a importância da LGPD, diante da quantidade de dados que os cidadãos compartilham por meio do acesso à internet. O Brasil tinha, até o final de 2017, 74,9% dos domicílios com acesso à internet e 93,2% com a presença de celular. Além disso, o telefone celular é o principal equipamento utilizado para acessar a internet, com 97% dos usuários da rede, cerca de 122,5 milhões de pessoas. E o acesso aumenta em todas as faixas etárias, nas zonas urbana e rural.

Aliado a esses dados, temos o caráter expansionista da sistemática legal: o conceito de dados pessoais é toda informação relacionada a uma pessoa identificada ou identificável, isto é, mesmo que uma informação tenha sido anonimizada, caso não tenha sido da forma correta, ainda poderá ser considerada dado pessoal. Tratamento é toda operação possível e imaginável: é a coleta, a produção, a recepção, a classificação, a utilização, o acesso, a reprodução, a transmissão, a distribuição, até mesmo a eliminação, entre outros, conforme predito no inciso X do art. 5º da LGPD.

Assim, temos que a LGPD afetará a todos que, de alguma forma, compartilham dados pessoais e, por outro lado, também impactará todas as empresas que tratam (coletar já faz parte do tratamento) dados pessoais de brasileiros e estrangeiros que estão no Brasil, mesmo se a empresa estiver sediada fora do território nacional e que a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços, ou o próprio tratamento de indivíduos que estejam no Brasil, exceto as hipóteses do artigo 4º (uso para fins particulares e não econômicos, utilizados exclusivamente como objetivo jornalístico, artístico ou acadêmico; e ainda para fins de segurança pública, defesa nacional e segurança do Estado).

Como se vê, os desafios não são fáceis. Busca-se, na presente dissertação, tratar de alguns desses desafios, sem a mínima intenção de esgotar os temas ou mesmo a quantidade de desafios existentes.

2. FUNDAMENTOS JURÍDICOS DA PROTEÇÃO DE DADOS

A proteção de dados pessoais é um campo *interdisciplinar* que combina aspectos jurídicos, tecnológicos e sociais, sendo amplamente debatido em diferentes vertentes teóricas. No Brasil, esse debate tem ganhado relevância especialmente após a vigência da Lei Geral de

Proteção de Dados (LGPD), que consolidou conceitos fundamentais para o tratamento ético e seguro das informações pessoais. Embora a norma tenha um caráter essencialmente prático, seu embasamento teórico reflete a influência de diversas doutrinas nacionais e internacionais.

No campo jurídico, a proteção de dados é frequentemente associada ao conceito de **autodeterminação informativa**[11], que surgiu na Alemanha no julgamento do "Censo de 1983", que será abordada amplamente mais na frente. Esse princípio estabelece que cada indivíduo tem o direito de controlar suas próprias informações, determinando como elas podem ser utilizadas e por quem. Essa concepção foi amplamente defendida por doutrinadores como Stefano Rodotá, que destacou a importância da privacidade como elemento central para o livre desenvolvimento da personalidade (RODOTÁ, 2009).

Outra teoria amplamente debatida é a de que a proteção de dados transcende a esfera individual, sendo um bem coletivo essencial para o funcionamento das democracias. Joshua Fairfield e Christoph Engel, por exemplo, argumentam que a privacidade deve ser tratada como um "bem público", pois sua violação afeta não apenas os titulares dos dados, mas também a sociedade como um todo, ao comprometer valores como liberdade e igualdade (FAIRFIELD; ENGEL, 2015).

Na perspectiva filosófica, Hannah Arendt trouxe importantes contribuições ao debate ao distinguir o espaço público do privado. Embora sua obra não tenha sido dedicada diretamente à proteção de dados, seus conceitos ajudam a entender a relevância da privacidade como barreira contra o controle estatal e corporativo. Arendt argumenta que a invasão da esfera privada pelo poder público compromete a autonomia dos indivíduos e, consequentemente, a base de uma sociedade plural (ARENDT, 1958).

Por sua vez, doutrinadores como Ingo Wolfgang Sarlet enfatizam a conexão entre a proteção de dados e os direitos fundamentais consagrados na Constituição Federal de 1988. Para Sarlet, a proteção de dados deve ser entendida como uma extensão do direito à privacidade, previsto no artigo 5º, inciso X, da Constituição. Essa interpretação reforça o papel da LGPD

[11] A autodeterminação informativa é o direito do indivíduo de controlar seus próprios dados pessoais, incluindo a decisão sobre como, quando e por quem essas informações podem ser utilizadas. No contexto da LGPD, esse princípio é essencial para garantir a privacidade e a proteção contra usos indevidos, fortalecendo a autonomia e a dignidade do titular dos dados.

como instrumento de concretização da dignidade humana no contexto das relações digitais (SARLET; SAAVEDRA, 2020).

O conceito de "privacidade contextual", desenvolvido por Helen Nissenbaum, também tem grande relevância no debate sobre proteção de dados. Segundo a autora, a privacidade não deve ser vista como um direito absoluto, mas como um conjunto de normas que varia de acordo com o contexto em que os dados são coletados e utilizados. Essa teoria é especialmente aplicável no ambiente digital, onde as fronteiras entre público e privado são frequentemente indistintas (NISSENBAUM, 2009).

Outra abordagem importante é a de que a proteção de dados está intrinsecamente ligada à **liberdade de escolha**. Laura Schertel Mendes argumenta que a LGPD não apenas protege a privacidade, mas também promove a autodeterminação dos titulares ao garantir que eles tenham controle sobre suas informações. Essa perspectiva é fundamental em um contexto onde algoritmos e inteligência artificial moldam comportamentos e decisões de forma cada vez mais invasiva (MENDES, 2020).

Do ponto de vista técnico, o conceito de "privacy by design", introduzido por Ann Cavoukian, destaca a necessidade de incorporar mecanismos de proteção de dados desde a concepção de sistemas e processos. Essa abordagem foi incorporada pela GDPR e, subsequentemente, pela LGPD, sendo considerada um dos pilares para garantir a segurança das informações em ambientes digitais complexos (CAVOUKIAN, 2011).

Já na esfera econômica, Shoshana Zuboff contribuiu para o debate ao introduzir o conceito de "capitalismo de vigilância". Segundo Zuboff, a exploração de dados pessoais por grandes empresas tecnológicas não apenas compromete a privacidade, mas também cria uma forma de poder econômico, baseada na coleta e análise de informações para prever e influenciar comportamentos (ZUBOFF, 2015).

Outra teoria relevante é a de que a **proteção de dados deve ser vista como um direito transnacional**. Nelson Remolina Angarita argumenta que, em um mundo globalizado, as legislações nacionais não são suficientes para proteger os dados pessoais, sendo necessário um esforço conjunto para criar padrões internacionais que garantam a segurança e a privacidade em diferentes jurisdições (REMOLINA ANGARITA, 2012).

A discussão sobre proteção de dados também inclui perspectivas críticas, como as levantadas por Caitlin Mulholland. A autora destaca que a regulamentação do tratamento de dados muitas vezes falha em considerar as desigualdades estruturais existentes, especialmente em países como o Brasil, onde grande parte da população não tem acesso à educação digital. Essa desigualdade cria uma barreira para o exercício efetivo dos direitos previstos na LGPD, como o direito de acesso e correção de dados (MULHOLLAND, 2018).

Além disso, teorias de justiça social, como as de Amartya Sen, podem ser aplicadas ao debate sobre proteção de dados. Para Sen, a justiça está diretamente relacionada à capacidade dos indivíduos de exercer suas liberdades em igualdade de condições. No contexto da LGPD, isso significa garantir que todos os cidadãos tenham conhecimento e recursos para exercer seus direitos informativos, independentemente de sua classe social ou localização geográfica (SEN, 1999).

A análise dos conceitos e teorias sobre proteção de dados revela que o tema é complexo e multifacetado, envolvendo questões jurídicas, filosóficas, econômicas e técnicas. Essas diferentes abordagens são essenciais para compreender a importância da LGPD e seu papel na promoção de uma sociedade mais justa e equilibrada. Contudo, o sucesso da legislação depende de sua capacidade de dialogar com essas múltiplas perspectivas, adaptando-se às necessidades específicas de cada contexto.

2.1 AUTODETERMINAÇÃO INFORMATIVA E A PRIVACIDADE DA PESSOA

A autodeterminação informativa é um conceito que vai além do direito à privacidade, conferindo ao indivíduo o poder de controlar suas informações pessoais. Este conceito foi formalizado no direito alemão no histórico julgamento do Tribunal Constitucional Federal Alemão, em 1983, no caso Volkszählungsurteil (Julgamento do Censo). A decisão destacou que, sem controle sobre os próprios dados, o indivíduo estaria vulnerável à manipulação, comprometendo sua liberdade e dignidade, direitos fundamentais protegidos pelas democracias modernas (RODOTÁ, 2009).

No Brasil, a Lei Geral de Proteção de Dados (LGPD) consolidou a autodeterminação

informativa como um direito jurídico. A LGPD estabelece que o titular dos dados deve ter o controle sobre como suas informações são coletadas, armazenadas e utilizadas, alinhando-se aos padrões internacionais, como a General Data Protection Regulation (GDPR) da União Europeia. Essa legislação coloca o Brasil em uma posição de destaque no cenário global de proteção de dados, promovendo a segurança jurídica e o fortalecimento dos direitos fundamentais (BRASIL, 2018).

A *conexão* entre autodeterminação informativa e privacidade é evidente. Enquanto a privacidade se refere ao resguardo de aspectos da vida pessoal contra interferências externas, a autodeterminação informativa amplia essa proteção ao permitir que o indivíduo tenha poder decisório sobre o uso de seus dados. Laura Schertel Mendes argumenta que a autodeterminação informativa é uma *ferramenta de emancipação*, especialmente em um ambiente digital onde as informações circulam de forma intensa e muitas vezes incontrolável (MENDES, 2020).

A LGPD foi projetada para responder às demandas de um mundo cada vez mais digitalizado. No entanto, sua implementação enfrenta desafios significativos, principalmente em países como o Brasil, onde o desconhecimento dos direitos digitais é generalizado. Um estudo realizado pelo Reclame Aqui apontou que mais de 40% das empresas brasileiras não sabem o que é LGPD, o que demonstra a necessidade de maior conscientização e capacitação tanto para empresas quanto para indivíduos (CARDOSO, 2020).

Na teoria jurídica, a autodeterminação informativa é frequentemente analisada sob o **prisma da dignidade humana**, conforme estabelecido na Constituição Federal de 1988. Ricardo Villas Bôas Cueva ressalta que, ao regular o tratamento de dados pessoais, a LGPD concretiza princípios constitucionais como a liberdade, a privacidade e a igualdade, assegurando que a coleta e o uso de informações sejam feitos de forma ética e transparente (CUEVA, 2019, p. 2 e p. 83-96,).

A teoria de "privacidade contextual", proposta por Helen Nissenbaum, contribui para enriquecer o debate ao destacar que as expectativas de privacidade variam conforme o ambiente em que os dados são coletados e utilizados. Esse conceito é especialmente relevante em uma sociedade conectada, onde a linha entre público e privado é frequentemente tênue. Nissenbaum argumenta que a autodeterminação informativa deve levar em conta essas nuances contextuais para garantir uma proteção efetiva (NISSENBAUM, 2009).

Shoshana Zuboff, por sua vez, alerta que a falta de controle sobre os dados pode transformar os indivíduos em meros produtos de um *"capitalismo de vigilância"*. Nesse modelo econômico, empresas utilizam dados pessoais para prever e influenciar comportamentos, comprometendo a liberdade individual. Para Zuboff, a autodeterminação informativa é essencial para reequilibrar essa relação, devolvendo aos indivíduos o controle sobre suas informações (ZUBOFF, 2015).

No Brasil, a falta de **alfabetização digital** entre a população é um obstáculo importante para o exercício da autodeterminação informativa. A desigualdade de acesso à tecnologia e ao conhecimento sobre os direitos digitais dificulta que muitos cidadãos compreendam e exerçam os direitos previstos na LGPD. Essa realidade aponta para a necessidade de políticas públicas que promovam a inclusão digital e a educação em privacidade (CANAAN, 2018).

O conceito de "privacy by design", introduzido por Ann Cavoukian, também reforça a autodeterminação informativa. Esse princípio, que exige que a proteção de dados seja incorporada desde a concepção de produtos e serviços, foi adotado tanto pela GDPR quanto pela LGPD. Ao garantir que a privacidade seja uma preocupação central em todos os estágios do tratamento de dados, o "privacy by design" promove um ambiente mais seguro e alinhado às expectativas dos titulares.

Além do setor privado, o setor público também enfrenta desafios na implementação da autodeterminação informativa. Embora a LGPD se aplique a órgãos governamentais, muitas instituições públicas brasileiras ainda não possuem infraestrutura tecnológica e humana suficiente para garantir o tratamento adequado de dados pessoais. Isso compromete não apenas a privacidade dos cidadãos, mas também a confiança na administração pública (CORTÊS, 2020).

A autodeterminação informativa é uma ferramenta poderosa para combater práticas discriminatórias. Caitlin Mulholland argumenta que, ao garantir o controle sobre os dados, a LGPD oferece uma camada adicional de proteção contra o uso indevido de informações sensíveis, como raça, religião e orientação sexual. Essa proteção é especialmente importante em um país como o Brasil, onde desigualdades estruturais frequentemente resultam em discriminação digital (MULHOLLAND, 2018).

Daniel Solove, em sua obra sobre gestão de privacidade, alerta para o dilema do consentimento, que muitas vezes coloca os indivíduos em situações de escolha forçada. Solove defende que a autodeterminação informativa deve ser complementada por regulamentações robustas que imponham limites claros ao uso de dados, independentemente do consentimento do titular. Esse enfoque é essencial para proteger os indivíduos em um ambiente onde o desequilíbrio de poder entre empresas e consumidores é evidente (SOLOVE, 2012).

A relação entre autodeterminação informativa e segurança dos dados também é central. Marcus Magalhães destaca que a proteção efetiva de dados pessoais depende de sistemas robustos de segurança cibernética. Sem medidas adequadas, a autodeterminação informativa torna-se inviável, pois os titulares perdem a confiança na capacidade dos controladores de proteger suas informações (MAGALHÃES, 2024).

O avanço das tecnologias de **inteligência artificial (IA)** apresenta novos desafios para a *autodeterminação informativa*. Algoritmos cada vez mais sofisticados podem prever comportamentos e preferências com base em grandes volumes de dados, muitas vezes sem o conhecimento ou consentimento dos titulares. É fato que a regulamentação precisa evoluir para lidar com esses novos riscos, garantindo que a privacidade e a autonomia dos indivíduos sejam preservadas em um ambiente de inovação constante.

A autodeterminação informativa também tem uma **dimensão ética**, conforme argumentado por Carole Pateman. A autora ressalta que o controle sobre os dados pessoais é essencial para preservar a autonomia e a dignidade dos indivíduos em uma sociedade onde as fronteiras entre o público e o privado são cada vez mais fluidas. Essa abordagem destaca a necessidade de regulamentações que considerem os direitos dos indivíduos em sua totalidade, indo além de interesses econômicos ou políticos (PATEMAN, 2013).

No campo jurídico brasileiro, a autodeterminação informativa é cada vez mais reconhecida como um **direito fundamental**. Decisões do Superior Tribunal de Justiça (STJ) têm reforçado a importância desse princípio na interpretação da LGPD, destacando a necessidade de proteger os dados pessoais como parte integrante da dignidade da pessoa humana (CUEVA, 2019).

No que diz respeito a como o conceito de autodeterminação informativa protege a autonomia dos indivíduos, é estabelecido que o indivíduo é o principal responsável por decidir como seus dados serão tratados. Em um contexto em que informações pessoais são coletadas em larga escala por empresas e governos, a proteção da autonomia requer não apenas a garantia de privacidade, mas também o poder de escolha sobre o destino dos dados. Esse aspecto é destacado por Ingo Wolfgang Sarlet, que identifica a autodeterminação informativa como um elemento essencial para a realização dos direitos fundamentais em sociedades democráticas (SARLET; SAAVEDRA, 2020).

No Brasil, a Lei Geral de Proteção de Dados (LGPD) concretiza o conceito de autodeterminação informativa, ao estabelecer princípios como a transparência e a limitação de finalidade. A norma permite que os indivíduos exerçam maior controle sobre seus dados, fortalecendo sua posição frente aos controladores. De acordo com Laura Schertel Mendes, a LGPD não apenas regulamenta o tratamento de dados, mas também contribui para a construção de uma cidadania digital, onde a autonomia informativa é vista como um direito essencial (MENDES, 2020).

Mas qual a relação entre autodeterminação informativa e a autonomia dos indivíduos? É ainda mais relevante no contexto da economia digital. Shoshana Zuboff destaca que o capitalismo de vigilância compromete a autonomia dos indivíduos ao transformar dados pessoais em uma mercadoria, frequentemente sem o consentimento ou conhecimento dos titulares. Nesse cenário, a autodeterminação informativa atua como uma barreira contra práticas abusivas, permitindo que os indivíduos recuperem o controle sobre suas informações (ZUBOFF, 2015).

O direito à autodeterminação informativa também possui uma dimensão ética, que transcende a regulamentação jurídica. Carole Pateman argumenta que a autonomia dos indivíduos depende da capacidade de tomar decisões informadas, livres de coerção ou manipulação. No contexto da proteção de dados, isso significa garantir que os titulares tenham acesso a informações claras e compreensíveis sobre o tratamento de seus dados, conforme previsto pela LGPD (PATEMAN, 2013).

Além disso, a autodeterminação informativa é um elemento crucial para a proteção de grupos vulneráveis, que frequentemente enfrentam desigualdades no acesso à tecnologia e à

educação digital. Caitlin Mulholland enfatiza que a proteção dos dados sensíveis, como origem étnica ou religiosa, é essencial para promover a igualdade e a inclusão, fortalecendo a autonomia desses grupos frente a potenciais discriminações (MULHOLLAND, 2018).

Outro aspecto importante é a relação entre **autodeterminação informativa e inovação tecnológica.** Marcus Magalhães aponta que, embora a tecnologia ofereça novas ferramentas para ampliar a autonomia, ela também introduz riscos significativos, como o uso de algoritmos para influenciar decisões individuais. Nesse sentido, a regulamentação deve acompanhar o desenvolvimento tecnológico, garantindo que os direitos fundamentais sejam protegidos em todos os contextos (MAGALHÃES, 2024).

A LGPD também contribui para a autonomia dos indivíduos ao prever o direito de acesso e retificação, permitindo que os titulares verifiquem a exatidão de suas informações e corrijam eventuais inconsistências. Esse mecanismo é essencial para garantir que os dados sejam tratados de forma justa e transparente, fortalecendo a confiança nas relações entre titulares e controladores (BRASIL, 2018).

No campo jurídico, Ricardo Villas Bôas Cueva destacou que a proteção da autonomia informativa não pode ser dissociada da dignidade humana. Para o autor, o controle sobre os dados pessoais é uma manifestação concreta da dignidade, que é protegida pelo ordenamento jurídico brasileiro como um valor fundamental. Assim, a LGPD deve ser interpretada como uma ferramenta para garantir não apenas a privacidade, mas também a autonomia em um sentido mais amplo (CUEVA, 2019).

A perspectiva de Helen Nissenbaum sobre privacidade contextual também enriquece a discussão sobre a relação entre autodeterminação informativa e autonomia. A autora argumenta que as expectativas de privacidade variam conforme o contexto social, e que a proteção da autonomia requer uma abordagem adaptável, que leve em consideração as especificidades de cada situação. Esse conceito é especialmente relevante em um ambiente digital heterogêneo, onde as fronteiras entre público e privado são frequentemente borradas (NISSENBAUM, 2009).

O conceito de autodeterminação informativa também encontra aplicação prática no mercado de trabalho. Empresas frequentemente coletam dados de seus funcionários para

monitoramento e avaliação de desempenho, o que levanta questões éticas e jurídicas sobre os limites desse controle. A LGPD estabelece bases legais para o tratamento de dados no ambiente profissional, promovendo um equilíbrio entre os interesses empresariais e os direitos dos trabalhadores (MENDES, 2020).

A proteção da autonomia por meio da autodeterminação informativa também é relevante para a saúde pública, especialmente em contextos de pandemia. Bethânia de Araújo Almeida ressalta que o uso de dados para rastreamento de contato e monitoramento de saúde deve ser feito de maneira transparente, garantindo que os indivíduos tenham controle sobre suas informações e evitando o uso abusivo para fins discriminatórios (ALMEIDA et al., 2020).

No cenário global, a autodeterminação informativa tem sido discutida como um direito transnacional. Nelson Remolina Angarita argumenta que, em um mundo interconectado, a proteção de dados pessoais não pode ser limitada por fronteiras geográficas, exigindo uma abordagem colaborativa entre diferentes jurisdições. A LGPD, ao alinhar-se à GDPR, representa um passo importante nesse sentido, reforçando a autonomia dos indivíduos em um ambiente globalizado (REMOLINA ANGARITA, 2012).

Além disso, o fortalecimento da autonomia por meio da autodeterminação informativa **requer a aplicação efetiva das normas, incluindo a fiscalização rigorosa e a aplicação de sanções para descumprimento.** A Autoridade Nacional de Proteção de Dados (ANPD) desempenha um papel central nesse processo, ao estabelecer diretrizes e monitorar o cumprimento da LGPD, promovendo um ambiente de maior segurança jurídica (BRASIL, 2018).

Por mais que exista avanço a falta de clareza e uniformidade nas interpretações e aplicações práticas das normas previstas na LGPD merece destaque. Embora a lei estabeleça diretrizes abrangentes para a proteção de dados, muitos agentes públicos e privados enfrentam dificuldades em compreender suas obrigações e alinhar seus processos internos ao cumprimento integral da legislação. Essa incerteza normativa gera um ambiente de insegurança jurídica, onde a aplicação fragmentada e inconsistente das regras pode comprometer tanto a proteção dos direitos dos titulares quanto a competitividade das organizações em um cenário global.

Assim, há uma necessidade urgente de iniciativas educacionais e orientações claras por parte da ANPD, bem como de um esforço contínuo para simplificar e padronizar os

procedimentos de adequação à lei.

2.1.1 Proteção de dados como um direito fundamental

Vale mencionar que a rápida evolução tecnológica e a popularização da internet transformaram profundamente as dinâmicas sociais, econômicas e culturais, criando um ambiente digital que facilita o acesso à informação e promove a inclusão digital. Contudo, essa expansão também trouxe desafios significativos, como a massificação do uso da rede e o aumento das violações à privacidade. Nesse contexto, o direito à proteção dos dados pessoais emergiu como uma questão central, exigindo um equilíbrio entre o progresso tecnológico e a preservação dos direitos fundamentais dos indivíduos. No Brasil, a ausência de um marco regulatório robusto para o ciberespaço expõe lacunas que colocam em risco tanto a privacidade quanto o desenvolvimento econômico e cultural.

A proteção de dados pessoais se consolidou como um direito fundamental em diversos ordenamentos jurídicos, incluindo o Brasil. Esse reconhecimento reflete a crescente importância dos dados pessoais em uma sociedade marcada pela digitalização e pelo uso intensivo de informações para finalidades comerciais, políticas e sociais. A Constituição Federal de 1988 protege, em seu artigo 5º, incisos X e XII, a privacidade e a inviolabilidade das comunicações, fundamentos que servem de base para o entendimento da proteção de dados como uma garantia essencial (SARLET; SAAVEDRA, 2020).

O reconhecimento da proteção de dados como um direito fundamental ganhou força no cenário internacional, especialmente com a entrada em vigor da General Data Protection Regulation (GDPR) na União Europeia, como reiterado diversas vezes. A GDPR estabelece a proteção de dados como um direito fundamental, essencial para assegurar a dignidade e a liberdade dos indivíduos. Esse entendimento influenciou diretamente a Lei Geral de Proteção de Dados (LGPD) no Brasil, que, ao se alinhar a esses padrões, reforçou a proteção jurídica dos dados pessoais como um elemento central do Estado Democrático de Direito (BRASIL, 2018).

A necessidade de um marco regulatório específico para o ciberespaço brasileiro é evidenciada pelas contradições jurídicas e ausência de diretrizes claras, que geram insegurança tanto para os usuários quanto para as empresas. A adoção de ferramentas como a **Inspeção Profunda de Pacotes de Rede (DPI)**, por exemplo, expõe os dados pessoais a usos

indiscriminados, favorecendo práticas comerciais abusivas e ameaçando princípios fundamentais, como a neutralidade da rede. Essa falta de regulação adequada não apenas compromete a segurança dos usuários, mas também limita a atração de investimentos internacionais em tecnologia, enfraquecendo o posicionamento do Brasil no cenário global.

Diante desses desafios, o Marco Civil da Internet surge como um avanço importante, ao estabelecer princípios, direitos e deveres para o uso da rede no Brasil. Contudo, sua implementação plena exige amadurecimento normativo e maior articulação entre os diferentes agentes envolvidos. Além disso, a regulação deve respeitar as premissas originais da internet, garantindo liberdade, inclusão e diversidade. Apenas com a adoção de um marco regulatório abrangente, que concilie proteção de dados e inovação tecnológica, será possível construir um ambiente digital que assegure tanto os direitos fundamentais quanto o desenvolvimento sustentável no Brasil.

Ingo Wolfgang Sarlet destaca que a proteção de dados transcende a dimensão individual, assumindo uma relevância coletiva. Para Sarlet, a proteção de dados é um instrumento para a concretização da dignidade da pessoa humana e para o equilíbrio das relações de poder em sociedades contemporâneas. Essa visão é especialmente relevante em um ambiente digital onde dados são frequentemente utilizados para moldar comportamentos e influenciar decisões de forma opaca (SARLET, 2020).

O Supremo Tribunal Federal (STF) brasileiro reconheceu a proteção de dados como um direito fundamental no julgamento da **Ação Direta de Inconstitucionalidade 6387**[12], que tratou da criação da Autoridade Nacional de Proteção de Dados (ANPD). O STF afirmou que o tratamento adequado dos dados pessoais é uma condição indispensável para o exercício da cidadania e para a preservação da privacidade. Essa decisão consolidou a proteção de dados como uma prioridade constitucional no Brasil (STF, 2023).

[12] Cuida-se de pedido de medida cautelar em ação direta de inconstitucionalidade proposta pelo Conselho Federal da Ordem dos Advogados do Brasil – CFOAB contra o inteiro teor da Medida Provisória n. 954, de 17 de abril de 2020, que dispõe sobre "o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020"

O conceito de proteção de dados como direito fundamental também é explorado por Stefano Rodotà, que argumenta que a privacidade e o controle sobre os dados são essenciais para preservar a liberdade e a autonomia dos indivíduos em uma sociedade conectada. Para Rodotà, a proteção de dados não se limita à esfera privada, mas abrange também a relação dos indivíduos com o Estado e com as corporações, promovendo um equilíbrio de poder em contextos digitais (RODOTÀ, 2009).

Além disso, a proteção de dados como direito fundamental é um elemento central para a promoção da igualdade. Laura Schertel Mendes destaca que, em um país marcado por desigualdades estruturais como o Brasil, garantir a proteção de dados significa também proteger grupos vulneráveis contra discriminações baseadas em dados sensíveis. A LGPD, ao prever tratamentos diferenciados para dados sensíveis, reflete essa preocupação com a promoção de uma sociedade mais equitativa (MENDES, 2020).

A proteção de dados está profundamente relacionada ao direito à informação. Como destaca Nelson Remolina Angarita, em uma sociedade da informação, o controle sobre os dados é essencial para que os indivíduos participem de forma ativa e consciente nas decisões que impactam suas vidas. Dessa forma, a proteção de dados torna-se indispensável para a efetivação de outros direitos fundamentais, como a liberdade de expressão e o acesso à informação (REMOLINA ANGARITA, 2012).

Nesse contexto, tanto a proteção de dados pessoais quanto o direito à informação despontam como pilares essenciais para a construção de uma sociedade democrática. Previstos na Constituição Federal de 1988 e regulamentados pela Lei Geral de Proteção de Dados (LGPD) e pela Lei de Acesso à Informação (LAI), respectivamente, esses direitos promovem a redução das assimetrias informacionais entre o Estado e os cidadãos. Enquanto a LGPD assegura a proteção dos dados pessoais e a autodeterminação informativa, a LAI garante o acesso a informações públicas, fortalecendo a fiscalização e a participação cidadã no controle das políticas públicas.

Embora as duas legislações compartilhem objetivos complementares, tensões podem surgir em situações que envolvem informações públicas contendo dados pessoais. Nesses casos, é crucial interpretar a LGPD não como uma barreira, mas como uma ferramenta que regula o fluxo informacional de forma segura e responsável. A base legal prevista no artigo 7º, inciso II,

da LGPD possibilita o tratamento de dados pessoais para o cumprimento de obrigações legais, incluindo aquelas estabelecidas pela LAI. Assim, é possível disponibilizar informações públicas, desde que sejam observados os princípios de necessidade e finalidade, assegurando um equilíbrio entre transparência e proteção de dados.

A governança de dados desempenha um papel central na aplicação integrada dessas legislações. A LGPD exige que os órgãos públicos mantenham registros detalhados das atividades de tratamento de dados, facilitando a organização e a disponibilização das informações previstas na LAI. Essa interação é fortalecida pelo princípio da transparência ativa, que incentiva a divulgação proativa de informações de interesse coletivo, e pelo princípio da minimização, que limita a coleta e o compartilhamento de dados pessoais apenas ao necessário, promovendo um equilíbrio saudável entre proteção de dados e acesso à informação.

Nesse sentido, a complementaridade entre a LGPD e a LAI reforça a necessidade de interpretações que promovam a eficiência e a responsabilidade na administração pública. Em vez de se oporem, essas legislações se fortalecem mutuamente, garantindo um acesso à informação mais seguro e inclusivo. O principal desafio reside na aplicação prática, que demanda capacitação dos agentes públicos e diretrizes claras para evitar equívocos interpretativos. Assim, a interação entre proteção de dados e direito à informação consolida-se como um mecanismo indispensável para o fortalecimento da cidadania e da democracia no Brasil.

É importante destacar que o reconhecimento da proteção de dados como um direito fundamental também implica desafios significativos. Um dos principais é garantir a eficácia desse direito em um **ambiente de rápida evolução tecnológica**. Marcus Magalhães argumenta que a regulamentação deve ser suficientemente flexível para acompanhar as inovações, mas sem comprometer os princípios fundamentais que sustentam a proteção de dados. Esse equilíbrio é essencial para garantir que o direito à proteção de dados permaneça relevante e eficaz (MAGALHÃES, 2024).

Outro aspecto relevante é a relação entre a proteção de dados e a segurança jurídica. Caitlin Mulholland aponta que, ao estabelecer normas claras e aplicáveis, a LGPD promove um ambiente mais previsível e confiável tanto para indivíduos quanto para organizações. Isso é particularmente importante em um cenário globalizado, onde a circulação de dados transcende

fronteiras e exige cooperação internacional para garantir a proteção efetiva dos direitos dos titulares (MULHOLLAND, 2018).

Conforme argumentado por Shoshana Zuboff, o uso indevido de dados pessoais pode comprometer processos democráticos, como ***eleições***, ao permitir a **manipulação de informações** e comportamentos. Nesse sentido, a proteção de dados é essencial para preservar a integridade das instituições democráticas e garantir que os indivíduos possam tomar decisões informadas e autônomas (ZUBOFF, 2015).

No Brasil, a atuação da Autoridade Nacional de Proteção de Dados (ANPD) é um exemplo prático de como a proteção de dados pode ser operacionalizada como um direito fundamental. A ANPD tem o papel de regulamentar, fiscalizar e educar a sociedade sobre a importância desse direito, promovendo uma cultura de respeito à privacidade e ao controle informacional. A eficácia desse órgão é essencial para a implementação da LGPD e para a consolidação da proteção de dados como um direito fundamental no Brasil (BRASIL, 2018).

No entanto, para que a proteção de dados alcance sua plena efetividade, é necessário avançar na execução das normativas já existentes. Isso inclui o fortalecimento institucional da ANPD, com recursos adequados e maior autonomia, além da capacitação contínua dos agentes públicos e privados responsáveis pela aplicação da LGPD. A melhoria na execução também passa pela criação de diretrizes mais claras e acessíveis, que auxiliem organizações e cidadãos a compreenderem seus papéis e direitos no contexto da proteção de dados. Somente com uma atuação robusta e eficiente será possível transformar a LGPD em uma ferramenta prática de garantia dos direitos fundamentais, consolidando-a como um pilar indispensável para o desenvolvimento democrático e a inclusão digital no Brasil.

Ademais, a proteção de dados como direito fundamental tem uma dimensão internacional, que exige cooperação entre diferentes países para garantir padrões elevados de segurança e privacidade. A convergência normativa entre a LGPD e a GDPR é um exemplo de como diferentes jurisdições podem trabalhar juntas para proteger os direitos dos titulares em um ambiente globalizado. Essa abordagem colaborativa é essencial para enfrentar desafios como o fluxo transfronteiriço de dados e os riscos associados ao cibercrime (REMOLINA ANGARITA, 2012).

A efetividade da proteção de dados como direito fundamental depende também do engajamento da sociedade civil. Organizações não governamentais e movimentos sociais têm desempenhado um papel crucial ao pressionar governos e empresas para adotar práticas mais transparentes e responsáveis. Essa mobilização é essencial para garantir que a proteção de dados não seja apenas uma garantia formal, mas um direito efetivo que possa ser exercido por todos os cidadãos (CARDOSO, 2020).

Desse modo, a proteção de dados como um direito fundamental é um reflexo das transformações sociais e tecnológicas do século XXI. Em um mundo cada vez mais digitalizado, garantir o controle sobre os dados pessoais é uma condição indispensável para a dignidade, a liberdade e a igualdade. A LGPD, ao incorporar esses princípios, coloca o Brasil em uma posição de destaque no cenário global, promovendo uma sociedade mais justa e equilibrada.

Sobre o status atual da proteção de dados como direito fundamental no Brasil, o seu próprio reconhecimento, amplamente discutido anteriormente, reflete a maturidade legislativa e a adaptação às novas demandas sociais geradas pela digitalização das relações humanas. Com a Emenda Constitucional nº 115/2022, o Brasil formalizou o direito à proteção de dados pessoais como garantia constitucional, ao lado de direitos como privacidade e liberdade de expressão. Esse avanço posiciona o país entre as nações que tratam a proteção de dados como essencial para a preservação da dignidade humana.

Outrossim, a proteção de dados no Brasil possui um **caráter multidimensional**. Ela não apenas assegura a privacidade individual, mas também protege a integridade dos processos democráticos e a segurança econômica, como abordado. A relevância desse direito é destacada por doutrinadores como Laura Schertel Mendes, que afirma que a proteção de dados transcende o indivíduo, impactando diretamente a estabilidade social e política. No cenário atual, o uso indevido de dados pode desestabilizar eleições, moldar comportamentos e ampliar desigualdades sociais (MENDES, 2020).

Além da dimensão jurídica, a proteção de dados no Brasil está profundamente conectada à educação e à **conscientização digital**. Um dos desafios identificados por Caitlin Mulholland é a disparidade no conhecimento sobre direitos digitais entre diferentes regiões e classes sociais. Para que o status de direito fundamental seja efetivo, é imprescindível que a população

compreenda o valor e o alcance desse direito. Iniciativas educacionais, aliadas a campanhas públicas, são essenciais para consolidar a proteção de dados na prática cotidiana (MULHOLLAND, 2018).

Outro aspecto central no status atual da proteção de dados no Brasil é o impacto da regulamentação no **setor econômico**. Empresas têm se adaptado às exigências da LGPD, implementando políticas internas de compliance e contratando especialistas em proteção de dados. Embora muitos vejam essas medidas como um custo adicional, estudiosos como Bruno Bioni destacam que elas representam uma oportunidade de agregar valor às organizações, fortalecendo a confiança dos consumidores e garantindo competitividade no mercado global (BIONI, 2019).

A inclusão da proteção de dados no rol dos direitos fundamentais também promove maior alinhamento do Brasil com padrões internacionais, como o GDPR europeu. Esse alinhamento é estratégico, pois facilita acordos comerciais e o fluxo transfronteiriço de informações, ao mesmo tempo em que reforça a soberania nacional na regulamentação de questões digitais. Nelson Remolina Angarita ressalta que a convergência normativa é um passo importante para criar um sistema global de proteção de dados, que atenda às demandas de uma economia interconectada (REMOLINA ANGARITA, 2012).

Do ponto de vista institucional, o STF (**Ação Direta de Inconstitucionalidade 6387)** desempenhou um papel crucial na consolidação do status da proteção de dados como direito fundamental. A Corte reconheceu, em diversos julgamentos, que o tratamento de dados pessoais está intrinsecamente ligado à preservação da democracia e dos direitos humanos. A decisão que declarou a constitucionalidade da criação da ANPD foi um marco nesse sentido, destacando a importância de uma entidade reguladora especializada para garantir a efetividade da proteção de dados no país (STF, 2023). Todos os julgados relevantes serão analisados mais adiante.

Além disso, a proteção de dados no Brasil possui um **caráter integrador**, conectando-se a outros direitos fundamentais, como saúde e educação. No setor da saúde, por exemplo, a coleta e o processamento de dados sensíveis devem respeitar os princípios da LGPD, garantindo que essas informações sejam utilizadas exclusivamente para finalidades legítimas e em conformidade com a vontade do titular. Essa abordagem reforça a ideia de que a proteção de dados não é apenas um direito individual, mas também um mecanismo para assegurar justiça

social (ALMEIDA et al., 2020).

O status atual da proteção de dados no Brasil também se reflete em **desafios relacionados à fiscalização e à aplicação das sanções previstas na LGPD**. Embora a lei tenha estabelecido mecanismos para punir violações, ainda há **uma lacuna na efetividade dessas medidas**. Frederico Cortez argumenta que a ANPD precisa ampliar sua capacidade técnica e humana para lidar com o volume crescente de casos e garantir que os direitos dos cidadãos sejam devidamente protegidos (CORTÊS, 2020).

As lacunas na aplicação efetiva da LGPD representam um desafio significativo para a consolidação de uma cultura de proteção de dados no Brasil. A demora na implementação das sanções administrativas, que apenas começaram a vigorar em 2023, criou um vácuo normativo e temporal, permitindo que organizações públicas e privadas negligenciassem os parâmetros legais estabelecidos. Essa ausência de aplicabilidade imediata comprometeu o caráter preventivo da legislação e enfraqueceu o papel da Autoridade Nacional de Proteção de Dados (ANPD) como órgão fiscalizador.

Além disso, a atuação da ANPD tem enfrentado limitações **estruturais** que restringem sua capacidade de promover a conformidade com a LGPD. A insuficiência de recursos técnicos e financeiros prejudica a realização de auditorias abrangentes e dificulta a aplicação de sanções proporcionais às infrações cometidas. Embora a Resolução CD/ANPD nº 4/2023 tenha trazido maior clareza ao processo sancionatório, a fragilidade na execução prática das penalidades compromete a credibilidade do sistema e não incentiva as organizações a adotarem medidas de segurança robustas.

Outro aspecto preocupante refere-se à baixa frequência de sanções efetivamente aplicadas. Casos recentes envolvendo o vazamento de dados sensíveis por entidades públicas ilustram a incapacidade do sistema de coibir práticas inadequadas e de promover um ambiente seguro para o tratamento de informações pessoais. A ausência de políticas preventivas e de programas de governança de dados robustos contribui para a perpetuação de incidentes que afetam diretamente a privacidade dos titulares.

Portanto, o avanço na efetividade da LGPD exige a conjugação de esforços entre a ANPD, os agentes de tratamento de dados e os demais atores envolvidos. A capacitação

contínua, a implementação de relatórios de impacto e a manutenção de registros de operações de tratamento de dados são medidas indispensáveis para mitigar os riscos e assegurar a proteção dos direitos fundamentais. A superação das lacunas observadas depende, em grande parte, de uma atuação coordenada e estruturada que priorize a transparência e a responsabilidade no tratamento de dados pessoais.

Outro ponto importante é o papel das empresas de tecnologia no respeito aos direitos fundamentais de proteção de dados. Alguns autores destacam que as grandes plataformas digitais têm responsabilidade significativa nesse processo, devendo adotar práticas de transparência e accountability. A adesão dessas empresas às normas da LGPD é fundamental para consolidar o status desse direito no Brasil, especialmente considerando o impacto dessas corporações na vida cotidiana dos cidadãos

No âmbito acadêmico, a proteção de dados como direito fundamental tem fomentado debates sobre ética e governança digital. Stefano Rodotà destaca que a proteção de dados é uma ferramenta essencial para preservar a autonomia individual em um contexto de crescente vigilância e manipulação. No Brasil, esse debate ganha relevância à medida que se discute a regulamentação de tecnologias emergentes, como inteligência artificial e blockchain, que trazem novos desafios para a proteção de dados (RODOTÀ, 2009).

A evolução do status da proteção de dados no Brasil também **está associada ao fortalecimento do sistema judiciário como um todo**. Ricardo Villas Bôas Cueva argumenta que a interpretação da LGPD pelos tribunais é crucial para consolidar o entendimento desse direito como fundamental. Decisões que reforcem a importância da transparência e do consentimento, por exemplo, contribuem para a construção de uma cultura de respeito à privacidade e à proteção de dados (CUEVA, 2019).

No cenário internacional, o Brasil tem se destacado como um exemplo de como países em desenvolvimento podem avançar na proteção de dados. A harmonização da LGPD com normas internacionais demonstra o compromisso do país em liderar discussões globais sobre o tema, ao mesmo tempo em que protege os interesses nacionais. Essa abordagem reforça o status da proteção de dados como um direito fundamental e como um instrumento estratégico para a soberania digital (MAGALHÃES, 2024).

Diante dissp, o status atual da proteção de dados no Brasil é um reflexo de avanços legislativos, decisões judiciais e mudanças culturais. No entanto, para que esse direito se consolide plenamente, é necessário **continuar investindo em educação, fiscalização e inovação**. Apenas com uma abordagem integrada será possível garantir que a proteção de dados seja efetiva e acessível a todos os cidadãos, cumprindo sua função como pilar da dignidade humana e da democracia.

2.1.2 A proteção de dados e a dignidade da pessoa

A dignidade da pessoa humana é alçada, no Brasil, à condição de fundamento da República (art. 1º, III, CF/88), irradiando seus efeitos sobre todo o ordenamento jurídico e configurando-se como núcleo essencial dos direitos fundamentais. Em meio às transformações digitais do século XXI, a proteção de dados pessoais emerge como uma das expressões mais modernas desse princípio. Isso porque, em uma sociedade conectada, a exposição indevida de informações sensíveis pode causar estigmatização, discriminação e profunda violação da identidade individual (SARLET; SAAVEDRA, 2020, p. 36).

A Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD) — incorporou ao ordenamento jurídico um arcabouço normativo voltado para assegurar o tratamento ético, seguro e consentido dos dados pessoais. O artigo 2º da LGPD afirma explicitamente que o respeito à privacidade, à autodeterminação informativa, à liberdade de expressão e ao desenvolvimento da personalidade são fundamentos da proteção de dados no Brasil. Essa previsão legal reforça que a proteção de dados não é meramente uma questão técnica, mas essencialmente **ética e constitucional** (BRASIL, LGPD, art. 2º).

Como ressalta Caitlin Mulholland, o tratamento de dados pessoais sensíveis deve ser visto como um ponto de tensão entre liberdades individuais e interesses estatais ou empresariais. Conforme o pensamento da autora, pode-se extrair que a tutela de dados pessoais sensíveis deve ser considerada condição para o pleno exercício da cidadania, estando diretamente relacionada ao princípio da dignidade da pessoa humana (MULHOLLAND, 2018, p. 161).

A jurisprudência do Supremo Tribunal Federal tem reconhecido a relação direta entre

proteção de dados e dignidade. No julgamento da ADI 5545, o STF considerou inconstitucional a lei fluminense que previa a coleta compulsória de material genético de mães e recém-nascidos no momento do parto. Para a Corte, essa coleta configura violação ao direito à privacidade e à autodeterminação informativa, protegidos como desdobramentos da dignidade da pessoa humana (STF, ADI 5545, 2023).

Esse entendimento fortalece a ideia de que os dados pessoais não são meramente um ativo econômico, mas uma projeção existencial da pessoa. Como lembra Ingo Sarlet, o direito fundamental à proteção de dados possui "fundamentos jusfilosóficos que remetem à autodeterminação e ao livre desenvolvimento da personalidade" (SARLET; SAAVEDRA, 2020, p. 34). Inspirados nas teorias de Honneth, Hegel e Solove, os autores destacam que a tutela de dados é, em última análise, uma forma de reconhecimento jurídico e social da identidade dos sujeitos.

Sob essa perspectiva, o direito à proteção de dados pessoais no Brasil encontra fundamento jurídico sólido no princípio da dignidade da pessoa humana, considerado pilar estruturante do Estado Democrático de Direito consagrado pela Constituição de 1988. Segundo Janaina Muniz Lobato, esse princípio, além de representar a base axiológica do ordenamento, é o vetor que confere densidade normativa a diversos direitos fundamentais, entre eles o direito de personalidade. A autora destaca que a proteção de dados pessoais foi recentemente elevada ao patamar de direito fundamental, por meio da Emenda Constitucional n.º 115/2022, e deve ser compreendida como uma manifestação do direito à autodeterminação informativa e à privacidade (LOBATO, 2024).

Lobato salienta ainda que, ao lado de outros direitos da personalidade, como a intimidade, a imagem e a honra, o direito à proteção de dados constitui um instrumento essencial para o livre desenvolvimento da personalidade. Isso porque, em uma sociedade marcada pela hiperconectividade e pelo fluxo incessante de informações, o controle sobre os próprios dados passa a ser condição sine qua non para o exercício da liberdade individual e da autonomia pessoal. Assim, o tratamento indevido de dados compromete diretamente a dignidade da pessoa humana, ao expô-la a riscos de discriminação, estigmatização ou mesmo manipulação de sua identidade digital (LOBATO, 2024).

Importante destacar que, ao ser inserida no art. 5º da Constituição Federal, a proteção

de dados pessoais passa a gozar de proteção reforçada, inclusive contra emendas constitucionais que pretendam aboli-la, em razão da cláusula pétrea do §4º do art. 60 da CF[13]. Isso demonstra o reconhecimento do legislador constituinte derivado de que a proteção dos dados não é um direito acessório, mas uma garantia nuclear da dignidade da pessoa humana em sua dimensão contemporânea (LOBATO, 2024).

O reconhecimento jurídico do direito à proteção de dados como direito fundamental também é evidenciado no cenário internacional. O Regulamento Geral de Proteção de Dados da União Europeia (GDPR), em seu artigo 1º, reconhece expressamente que a proteção de dados é um direito fundamental dos cidadãos europeus. Esse paradigma tem influenciado a jurisprudência constitucional em países latino-americanos, como demonstra Nelson Remolina Angarita ao analisar decisões das Cortes Constitucionais da Colômbia, México e Argentina, que vinculam a proteção de dados ao núcleo essencial da dignidade (REMOLINA ANGARITA, 2018, p. 10).

No **plano filosófico**, a relação entre dados e dignidade humana exige atenção à "luta por reconhecimento" descrita por Axel Honneth. Segundo sua teoria, somente a partir da experiência de reconhecimento — inclusive no plano jurídico — é que os sujeitos podem desenvolver integralmente sua autonomia. A proteção dos dados pessoais, nesse contexto, opera como uma garantia de que a vida privada não será invadida de forma arbitrária, assegurando espaço de liberdade para que o sujeito se realize (HONNETH, 2010, p. 193).

Ademais, o tratamento ético dos dados é condição para a construção de confiança nas instituições, tanto públicas quanto privadas. Quando os dados são utilizados de forma ilícita ou discriminatória, há um esvaziamento da confiança social e uma ameaça à própria democracia. Nesse sentido, a jurisprudência internacional tem reconhecido que a proteção de dados é um pilar para o exercício de direitos como a liberdade de expressão, a igualdade e a não discriminação (REMOLINA ANGARITA, 2018, p. 14).

Sendo assim, o reconhecimento da proteção de dados como direito fundamental

[13] Art. 60. A Constituição poderá ser emendada mediante proposta:
(...)§ 4º Não será objeto de deliberação a proposta de emenda tendente a abolir:I - a forma federativa de Estado;II - o voto direto, secreto, universal e periódico;III - a separação dos Poderes;IV - os direitos e garantias individuais.

vinculado à dignidade da pessoa humana é essencial para a consolidação de um Estado Constitucional de Direito. A jurisprudência nacional e internacional, bem como a doutrina contemporânea, convergem na afirmação de que o controle sobre os dados pessoais não é apenas uma questão de segurança cibernética ou eficiência regulatória, mas uma exigência de justiça e respeito à condição humana (SARLET; SAAVEDRA, 2020, p. 41).

A questão da dignidade humana diante da violação de dados pessoais exige uma análise que ultrapasse o campo jurídico tradicional, adentrando o terreno da filosofia crítica do poder. Michel Foucault, em *Vigiar e Punir* (1975), oferece uma lente precisa para compreender como as tecnologias de vigilância e controle podem atingir profundamente a subjetividade e a integridade dos indivíduos. Em sua análise histórica da transformação do poder punitivo, Foucault demonstra que o poder disciplinar moderno deixou de se concentrar no corpo físico, passando a incidir diretamente sobre a alma, sobre a interioridade dos sujeitos — um deslocamento que guarda semelhanças com a forma como, hoje, o tratamento e a coleta indevida de dados pessoais impactam a autonomia e a identidade do indivíduo (FOUCAULT, 1975, p. 27-29).

Ao discutir o nascimento das prisões e das instituições modernas de controle, Foucault revela que o **corpo é politicamente investido**: ele é organizado, examinado, vigiado, categorizado. Essa racionalidade do poder, que opera por meio de dados, fichas, prontuários e registros, encontra seu equivalente contemporâneo nas bases de dados digitais que alimentam sistemas automatizados de perfilamento e vigilância. Assim como o corpo supliciado deixava marcas visíveis da punição nos séculos anteriores, o sujeito hoje pode ser simbolicamente marcado por algoritmos que o classificam, discriminam ou excluem silenciosamente — um processo menos visível, mas não menos violento (FOUCAULT, 1975, p. 31-34).

A violação de dados pessoais, nesse contexto, pode ser entendida como uma nova forma de suplício[14] invisível. Ela captura o indivíduo em sua vida cotidiana, muitas vezes sem o seu consentimento ou compreensão, submetendo-o a formas sutis de controle. A publicidade dirigida, a vigilância empresarial e estatal, as decisões automatizadas que afetam acesso ao crédito, trabalho ou serviços públicos, todos são mecanismos que, segundo a lógica

[14] dor ou sofrimento violento, físico, psicológico ou moral (p.ex., o que se inflige a alguém para lhe arrancar alguma revelação); tortura. (nota do autor).

foucaultiana, não visam punir abertamente, mas “corrigir”, “ajustar”, “governar” comportamentos sociais. Dessa maneira, o sujeito não é ferido no corpo, mas na sua autonomia, na sua liberdade de ser e decidir por si mesmo — o que compromete diretamente sua dignidade (FOUCAULT, 1975, p. 35-40).

Ao explorar a ideia de que o poder moderno atua principalmente por meio da vigilância — exemplificada pelo modelo do panóptico — Foucault explicita que o saber sobre os corpos e as almas é, na verdade, uma forma de poder sobre eles. No universo digital, os dados pessoais constituem o novo “saber” que permite controlar populações inteiras, não apenas individualmente, mas por meio de análises preditivas que moldam a política, o consumo e o comportamento coletivo. Isso gera uma nova forma de sujeição social: o cidadão é permanentemente observado, avaliado e ranqueado, frequentemente sem sequer perceber que está sob escrutínio — o que configura uma ameaça silenciosa à dignidade humana, pois reduz a pessoa a um conjunto de dados manipuláveis (FOUCAULT, 1975, p. 42-44).

Desse modo, inspirando-se em Foucault, é possível afirmar que a violação de dados pessoais constitui uma nova forma de violência simbólica, que embora não produza marcas físicas, opera sobre a estrutura mesma da identidade e da liberdade. O corpo disciplinado do século XIX é substituído pela alma governada por dados no século XXI. A proteção da dignidade da pessoa humana, nesse cenário, exige reconhecer que o tratamento ilícito, desproporcional ou discriminatório de dados é uma forma de dominação que fere o núcleo do sujeito. Assim, ao tratar a proteção de dados como um direito fundamental, o legislador constitucional brasileiro se alinha a essa exigência contemporânea de resistência à biopolítica da vigilância (FOUCAULT, 1975, p. 45-48).

3. PROTEÇÃO DE DADOS SOB A PERSPECTIVA CONSTITUCIONAL

Em um contexto marcado pela aceleração tecnológica, pela expansão dos fluxos informacionais e pelo uso intensivo de tecnologias digitais nas relações sociais, políticas e econômicas, o direito à proteção de dados se impõe como condição essencial para a preservação da dignidade da pessoa humana, núcleo axiológico da Constituição Federal de 1988. A informação, conforme assinala Manuel Castells, constitui a nova matéria-prima das relações de poder no século XXI, e o controle sobre os dados se traduz em controle sobre os indivíduos (CASTELLS, 1999).

A Constituição brasileira, ainda que concebida em um tempo pré-digital, oferece fundamentos normativos robustos para a tutela da privacidade, da intimidade, da honra e da imagem, todos previstos no art. 5º, incisos X e XII, e agora reforçados pela Emenda Constitucional nº 115/2022, que introduziu expressamente a proteção de dados pessoais como direito fundamental autônomo. A positivação desse direito reflete um movimento global de reconhecimento da centralidade da informação na vida contemporânea e responde à necessidade de limitar os riscos decorrentes da vigilância massiva, da monetização da privacidade e da manipulação algorítmica das condutas humanas.

A perspectiva constitucional da proteção de dados exige a leitura integrada do texto constitucional com os instrumentos normativos infraconstitucionais e internacionais. A LGPD — Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) — cumpre um papel central nesse panorama, funcionando como norma de concretização da Constituição, ao estabelecer princípios, fundamentos e regras para o tratamento adequado de dados pessoais. O art. 2º da LGPD afirma expressamente que a disciplina da proteção de dados deve observar, entre outros, o respeito à privacidade, à autodeterminação informativa, à liberdade e à dignidade da pessoa humana (BRASIL, LGPD, art. 2º).

Trata-se, portanto, de uma leitura constitucionalmente orientada da legislação ordinária, que articula os valores constitucionais com os parâmetros técnicos e jurídicos aplicáveis à realidade digital. Como destaca Caitlin Mulholland, o direito à proteção de dados não se resume à proteção da intimidade, mas envolve uma dimensão pública e política, relacionada à capacidade dos indivíduos de exercerem seus direitos em um ambiente digital seguro e livre de interferências indevidas (MULHOLLAND, 2018, p. 162).

O papel do Supremo Tribunal Federal nesse cenário é fundamental para consolidar a proteção de dados como direito fundamental. No **julgamento da ADI 6387**, a Corte reconheceu a inconstitucionalidade da Medida Provisória nº 954/2020, que previa o compartilhamento de dados pessoais de usuários de telecomunicações com o IBGE sem consentimento. O relator, Ministro Alexandre de Moraes, destacou que o uso de dados pessoais deve estar amparado por fundamentos legais, critérios de necessidade e proporcionalidade, e observância à finalidade específica, sob pena de violação da privacidade e da autodeterminação informativa (STF, ADI 6387).

Esse entendimento do STF revela a dimensão garantista da proteção de dados, reafirmando que sua violação configura agressão não apenas ao direito individual, mas também à ordem constitucional como um todo. A proteção de dados, nesse sentido, deve ser compreendida como um direito de resistência frente ao poder excessivo — seja estatal ou privado — sobre a intimidade, os hábitos, os comportamentos e as preferências dos indivíduos.

A doutrina contemporânea tem reforçado essa leitura. Sarlet e Saavedra argumentam que os direitos fundamentais à intimidade, à privacidade e à proteção de dados integram um "complexo de direitos de defesa" contra o Estado e contra os excessos de poder privado, em especial no contexto da sociedade digital (SARLET; SAAVEDRA, 2020, p. 39). Esses direitos são fundamentais para preservar a autodeterminação do sujeito e garantir a existência de uma esfera de reserva pessoal inviolável.

A Constituição de 1988, ao consagrar a dignidade da pessoa humana como fundamento do Estado, impõe ao legislador, ao administrador e ao julgador a tarefa de assegurar a integridade informacional do sujeito, como parte do seu direito de ser, agir e existir com liberdade. Esse é o núcleo do conceito de autodeterminação informativa, desenvolvido na Alemanha a partir do famoso caso do "Censo Federal", julgado pelo Tribunal Constitucional Federal em 1983, e que hoje influencia profundamente as discussões sobre privacidade e dados em nível global (MARTINS, 2008, p. 22).

No Brasil, essa doutrina começa a se firmar tanto no plano acadêmico quanto nas decisões judiciais. A autodeterminação informativa é entendida como o direito do indivíduo de decidir livremente sobre a coleta, uso, tratamento e compartilhamento de suas informações pessoais. Esse direito, como bem observa Mulholland, envolve não apenas a proteção contra a divulgação indesejada, mas o controle ativo sobre a trajetória dos próprios dados (MULHOLLAND, 2018, p. 165). Isso exige uma arquitetura jurídica capaz de garantir consentimento livre, informado, específico e revogável, como condição de validade do tratamento.

Do ponto de vista constitucional, a proteção de dados desafia a tradicional dicotomia entre esfera pública e privada. A Constituição deve ser compreendida como dotada de eficácia horizontal, aplicando-se às relações entre particulares, especialmente nas situações em que há assimetria informacional entre os titulares dos dados e os agentes de tratamento. A jurisprudência do STF já admite essa eficácia direta dos direitos fundamentais nas relações

privadas, como evidenciado em julgamentos sobre liberdade de expressão versus honra e imagem (BARROSO, 2007).

Essa compreensão tem impacto direto sobre os deveres das empresas e plataformas digitais que coletam, armazenam e processam grandes volumes de dados. O princípio da dignidade da pessoa humana impõe limites éticos e jurídicos à exploração econômica das informações pessoais, exigindo transparência, finalidade legítima, segurança e responsabilidade no uso dos dados. A proteção constitucional da personalidade, nesse contexto, deve prevalecer sobre interesses comerciais meramente lucrativos.

A Constituição, portanto, não é neutra diante do tratamento de dados: ela exige que o poder seja exercido com respeito aos direitos fundamentais, mesmo quando se manifesta em ambientes regulados pelo mercado. Como afirma Barroso, "os direitos da personalidade, entre os quais a proteção à privacidade, devem ser lidos à luz da Constituição, que lhes confere conteúdo, sentido e limites" (BARROSO, 2007, p. 19).

A constitucionalização da proteção de dados no Brasil também acarreta importantes consequências em termos de controle de constitucionalidade. Qualquer norma infraconstitucional — seja legal, infralegal ou contratual — que implique tratamento abusivo ou desproporcional de dados pessoais deverá ser invalidada, por incompatibilidade com os princípios constitucionais da dignidade da pessoa humana, da privacidade e da liberdade informacional. A Constituição, assim, atua como parâmetro de validade para todo o ordenamento, operando como limite e fundamento da atuação pública e privada em matéria de dados.

Essa diretriz interpretativa se fortalece diante da multiplicação de dispositivos digitais que operam com técnicas de vigilância, cruzamento de informações e decisões automatizadas. Como lembra Foucault, a vigilância moderna se caracteriza por ser difusa e contínua, alcançando os indivíduos não apenas em seus comportamentos públicos, mas em suas interioridades (FOUCAULT, 1975). Em um contexto como esse, a proteção constitucional de dados passa a ser também uma proteção contra o panoptismo digital[15] — ou seja, contra a

[15] [1] O conceito de panoptismo digital remete à ideia foucaultiana de vigilância constante, adaptada ao contexto das tecnologias digitais. Trata-se da internalização do controle por meio de dispositivos e plataformas que, ao captarem e analisarem dados constantemente, induzem comportamentos e moldam subjetividades. Nesse

redução do sujeito a objeto de controle permanente por parte do Estado e das corporações.

A Constituição impõe ainda uma dimensão proativa ao Estado: além de não violar a privacidade, deve adotar políticas públicas e marcos regulatórios voltados à proteção ativa de dados pessoais. Isso inclui a atuação da Autoridade Nacional de Proteção de Dados (ANPD), cuja função não é apenas regulatória e fiscalizatória, mas também pedagógica, promovendo a cultura da privacidade e orientando os agentes públicos e privados quanto às melhores práticas de governança informacional.

A criação da ANPD, como previsto no art. 55-A da LGPD, deve ser compreendida como uma concretização da cláusula do Estado Democrático de Direito, pois viabiliza o controle democrático sobre as estruturas técnicas de poder, permitindo ao cidadão exercer sua autonomia em ambiente digital com garantias mínimas de transparência e responsabilidade. A Constituição, ao reconhecer a proteção de dados como direito fundamental, impõe à ANPD um dever de tutela compatível com os parâmetros constitucionais, inclusive em relação à proteção de grupos vulneráveis, como crianças, adolescentes, idosos e pessoas com deficiência.

Importante observar que a proteção de dados também se conecta a outros princípios constitucionais estruturantes, como o da igualdade. O uso discriminatório de dados, seja em políticas públicas, seja em estratégias empresariais, pode reproduzir estigmas e desigualdades históricas. A Constituição não tolera a construção de perfis baseados em critérios étnico-raciais, religiosos, de gênero ou orientação sexual que limitem o acesso a bens, direitos ou oportunidades. Nesse sentido, a proteção de dados é também uma proteção contra a marginalização algorítmica e os chamados “preconceitos automatizados” (MULHOLLAND, 2018, p. 168).

A perspectiva constitucional exige, portanto, que todo tratamento de dados seja pautado pelos princípios da finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização, conforme expressamente estabelecido no art. 6º da LGPD. Esses princípios devem ser lidos à luz da Constituição, de modo a garantir que o tratamento de dados seja sempre orientado por finalidades legítimas e que respeitem a dignidade da pessoa humana.Nesse contexto, o princípio da proporcionalidade, já consagrado na

cenário, o usuário se comporta como se estivesse sempre sendo observado, ainda que não haja um vigilante visível. (nota do autor).

jurisprudência constitucional brasileira, assume papel fundamental na ponderação entre o interesse público ou privado no tratamento dos dados e os direitos fundamentais do titular.

A proporcionalidade atua como critério de controle de constitucionalidade e de conformidade de políticas públicas ou atos administrativos que envolvam coleta massiva de dados, especialmente em tempos de crise, como demonstrado nas ADIs que trataram da pandemia de COVID-19.

Exemplo paradigmático dessa aplicação foi o julgamento, já citado, da ADI 6586, que discutiu a constitucionalidade do compartilhamento de dados de saúde com órgãos federais. O STF reafirmou que, ainda em situações excepcionais, a utilização de dados deve respeitar os princípios constitucionais e que a emergência sanitária não suspende os direitos fundamentais. Essa decisão reitera que a proteção de dados, sob a ótica constitucional, não admite relativização arbitrária, mesmo em cenários de crise.

O debate sobre proteção de dados no Brasil, portanto, exige o abandono de uma leitura meramente legalista da LGPD e a adoção de uma hermenêutica constitucional comprometida com a centralidade da pessoa humana. Como destaca Barroso, os direitos fundamentais devem orientar a interpretação de todo o ordenamento, inclusive o civil, o penal e o administrativo, impondo a supremacia dos valores constitucionais nas relações jurídicas concretas (BARROSO, 2007, p. 23).

Além disso, a compreensão constitucional da proteção de dados implica reconhecer seu caráter intergeracional. A integridade informacional das crianças e adolescentes, por exemplo, deve ser resguardada com especial rigor, nos termos do art. 227 da Constituição. A jurisprudência brasileira e internacional tem afirmado a necessidade de consentimento parental e de tratamento compatível com o melhor interesse da criança, reconhecendo que a coleta precoce de dados pode ter efeitos permanentes sobre o desenvolvimento da personalidade.

No plano da **cidadania digital**, a proteção constitucional de dados reforça a necessidade de promover a literacia informacional, ou seja, a capacitação dos indivíduos para compreender, avaliar e tomar decisões sobre seus dados. A Constituição, ao assegurar o direito à educação e ao acesso à informação, impõe ao Estado o dever de desenvolver políticas públicas que permitam ao cidadão exercer seu direito à autodeterminação informativa de forma consciente e

ativa.

Diante disso, a proteção de dados como direito fundamental deve ser interpretada como um compromisso com a construção de uma sociedade democrática, plural e inclusiva. A Constituição de 1988, ao instituir o Estado Democrático de Direito, assume a dignidade da pessoa humana como valor fundante, e dela decorre a exigência de que toda regulação tecnológica seja orientada pelo respeito às liberdades fundamentais. A proteção de dados, nesse horizonte, não é um fim em si mesma, mas uma ferramenta de garantia da liberdade, da igualdade e da justiça social.

A análise da proteção de dados sob uma perspectiva constitucional não pode prescindir do exame comparado das experiências internacionais. O modelo europeu, em especial o consolidado pelo **Regulamento Geral sobre a Proteção de Dados (GDPR)** da União Europeia, é amplamente considerado paradigma normativo e institucional para outros ordenamentos. O GDPR, em seu artigo 1º, reconhece expressamente que o direito à proteção de dados pessoais é um direito fundamental e deve ser assegurado com base em princípios de legalidade, lealdade, transparência, limitação de finalidade, minimização e integridade dos dados.

Tal abordagem inspira diretamente a LGPD brasileira, mas também reforça a necessidade de uma interpretação constitucional que reconheça esse direito como pilar do modelo democrático europeu. Como destaca Caitlin Mulholland, o GDPR não apenas oferece diretrizes técnicas, mas carrega uma carga axiológica centrada no respeito à pessoa humana como sujeito de direitos, e não como mero objeto de análise estatística ou alvo de campanhas publicitárias (MULHOLLAND, 2018, p. 169).

A Corte Europeia de Direitos Humanos (CEDH) tem consolidado essa leitura em sua jurisprudência, afirmando reiteradamente que a privacidade e a proteção de dados estão no núcleo da dignidade humana e são indispensáveis ao desenvolvimento da autonomia individual. Em casos como **S. and Marper v. the United Kingdom** (2008), a CEDH estabeleceu que o armazenamento indiscriminado de dados genéticos por autoridades públicas viola o art. 8º da Convenção Europeia de Direitos Humanos, por não atender aos critérios de necessidade e proporcionalidade.

Esse entendimento contribui para fortalecer, no plano comparado, a ideia de que os direitos relacionados à informação pessoal devem ser protegidos contra abusos do Estado e das empresas. A jurisprudência europeia tem sido uma referência constante em julgados brasileiros, especialmente quando o STF precisa enfrentar temas ainda não completamente normatizados pelo legislador nacional.

No Brasil, um dos marcos dessa incorporação jurisprudencial foi o julgamento da ADI 6387, já mencionado, em que o STF adotou critérios de ponderação constitucionais semelhantes aos europeus, rejeitando a coleta indiscriminada de dados sob o pretexto de interesse estatístico. O relator, Ministro Alexandre de Moraes, fez referência expressa à autodeterminação informativa como direito fundamental, invocando inclusive precedentes do Tribunal Constitucional alemão.

Esse diálogo entre cortes constitucionais reforça a percepção de que a proteção de dados deve ser orientada por princípios universais de dignidade, liberdade e limitação do poder. Contudo, a transposição desses valores para o contexto brasileiro impõe desafios adicionais, especialmente quanto à eficácia horizontal dos direitos fundamentais nas relações privadas.

A Constituição brasileira, embora não tenha cláusula expressa de eficácia horizontal como a da Alemanha ou da África do Sul, já vem sendo interpretada pela doutrina e pela jurisprudência como aplicável às relações entre particulares sempre que estiverem em jogo direitos fundamentais. A partir da Teoria da Eficácia Direta dos Direitos Fundamentais, reconhecida por autores como Ingo Sarlet, é possível sustentar que empresas privadas têm deveres constitucionais na proteção de dados, independentemente de regulamentação infraconstitucional (SARLET; SAAVEDRA, 2020, p. 42).

Essa perspectiva amplia a responsabilidade dos entes privados, em especial de grandes plataformas digitais e prestadores de serviços, exigindo que suas práticas comerciais se adequem aos padrões constitucionais. O princípio da dignidade humana, nesse contexto, atua como limite material ao poder econômico, vedando condutas que submetam os titulares de dados a situações de risco, humilhação ou discriminação.

Outro ponto relevante é o dever de informação. A Constituição assegura, em seu art. 5º, XIV, o direito à informação e, no inciso XXXIII, o acesso a informações de interesse pessoal.

Esses dispositivos impõem obrigações positivas aos controladores de dados, que devem prestar informações claras, acessíveis e precisas sobre o tratamento de dados, inclusive nos casos de decisões automatizadas. Trata-se de uma projeção concreta do princípio democrático no ambiente digital, pois permite o exercício da cidadania em sua dimensão informacional.

Apesar dos avanços normativos, persistem dificuldades na implementação efetiva dos direitos constitucionais à proteção de dados. A cultura de vigilância, naturalizada por décadas de práticas abusivas, aliada à assimetria informacional entre titulares e controladores de dados, dificulta a materialização dos princípios constitucionais no cotidiano. Como lembra Barroso, o simples reconhecimento formal de um direito não garante sua eficácia social, sendo necessária uma atuação institucional coordenada e proativa (BARROSO, 2007, p. 27).

A atuação do Poder Judiciário é estratégica nesse sentido. **Cabe aos tribunais aplicar os princípios constitucionais da proteção de dados mesmo na ausência de legislação detalhada ou regulamentação específica, utilizando como guia os valores consagrados na Constituição e na LGPD.** A jurisprudência tem evoluído nesse sentido, como demonstram decisões que reconhecem o dano moral pela violação à privacidade e o dever de reparação nos casos de vazamento de dados sensíveis.

Além disso, a formação de uma jurisprudência constitucional sólida exige investimento em capacitação técnica de magistrados, promotores e defensores públicos, que nem sempre estão familiarizados com os desafios da proteção de dados. A atuação da ANPD pode colaborar nesse processo, mas é necessário que o sistema de Justiça internalize a cultura de proteção de dados como dimensão da jurisdição constitucional dos direitos fundamentais.

Por outro lado, a concretização da proteção constitucional de dados requer também a articulação com políticas públicas de inclusão digital e educação para a cidadania informacional. A Constituição de 1988 reconhece, em seus artigos 205 e 206, o direito à educação e à formação plena da pessoa, o que inclui a capacidade de compreender e exercer os próprios direitos em ambientes digitais. A proteção de dados, nesse sentido, não pode ser elitizada: deve alcançar todos os brasileiros, independentemente de sua renda, escolaridade ou localização geográfica.

Em sociedades desiguais como a brasileira, o risco de exclusão informacional e de

manipulação de dados é ainda maior. Por isso, a proteção constitucional de dados deve se articular com as diretrizes da justiça social, promovendo ações afirmativas e medidas compensatórias para garantir o exercício pleno do direito à autodeterminação informativa, em especial para os grupos historicamente marginalizados.

Essa perspectiva encontra respaldo nos objetivos fundamentais da República, previstos no art. 3º da Constituição, especialmente o de "construir uma sociedade livre, justa e solidária" e "promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação". A proteção de dados, quando constitucionalmente orientada, torna-se ferramenta para a efetivação desses objetivos, consolidando-se como parte integrante do projeto constitucional brasileiro.

O reconhecimento da proteção de dados como direito fundamental não apenas impõe limites ao poder do Estado, mas também redefine a própria arquitetura das liberdades civis na era digital. Como observa Ingo Sarlet, a proteção dos dados transcende o binômio público-privado e exige a criação de um espaço de imunidade informacional que resguarde a esfera íntima contra intervenções não justificadas (SARLET; SAAVEDRA, 2020, p. 33). Trata-se de reafirmar, à luz do constitucionalismo contemporâneo, a centralidade da pessoa humana em meio à lógica algorítmica que domina as estruturas decisórias atuais.

A presença de bancos de dados cada vez mais interligados e opacos transforma o modo como o poder é exercido. Essa nova forma de poder, como adverte Manuel Castells, opera de forma invisível, fluida e desmaterializada, sendo capaz de influenciar decisões políticas, comportamentos sociais e escolhas pessoais com base em análises de dados massivos (CASTELLS, 1999, p. 78). Nesse contexto, o controle dos fluxos informacionais torna-se uma nova forma de dominação, que precisa ser contida por garantias constitucionais firmes.

A Constituição deve, portanto, **assumir um papel regulador não apenas em relação ao que se pode fazer com os dados, mas em relação a quem os controla, com que finalidade e por quais meios**. Isso implica rever inclusive o princípio da neutralidade tecnológica: nem toda inovação digital pode ser aceita constitucionalmente se violar os valores fundantes do Estado Democrático de Direito. A jurisprudência constitucional precisa estar atenta à opacidade de certos algoritmos que, sob a aparência de neutralidade matemática, reproduzem padrões discriminatórios e reforçam estigmas sociais.

A decisão individualizada por meio de inteligência artificial, como em sistemas de crédito, triagem em políticas públicas ou controle de fronteiras, deve submeter-se a um escrutínio constitucional rigoroso. A LGPD já exige, em seu art. 20, o direito de revisão de decisões automatizadas. No entanto, é a Constituição que confere densidade a esse direito, exigindo que o tratamento de dados preserve a autonomia do sujeito e não reduza a pessoa a um número ou perfil estatístico.

Essa leitura é especialmente relevante se adotarmos, como lembra Caitlin Mulholland, a noção de que os dados pessoais compõem a "identidade informacional" do indivíduo — ou seja, uma projeção de sua personalidade no mundo digital (MULHOLLAND, 2018, p. 163). Assim, a tutela dos dados deve ser compreendida como tutela da subjetividade, da privacidade e da própria liberdade.

A eficácia constitucional da proteção de dados também implica o reconhecimento de um dever institucional de vigilância contínua. O Poder Legislativo deve fiscalizar o avanço tecnológico e sua compatibilidade com os direitos fundamentais. O Executivo, por sua vez, deve estruturar a ANPD como órgão técnico, independente e participativo. E o Judiciário precisa consolidar uma jurisprudência sensível às novas formas de violação de direitos que não se expressam apenas por atos explícitos, mas por arquiteturas silenciosas de exclusão, como o “data profiling” não consentido ou a extração de padrões comportamentais sem transparência.

A inserção da proteção de dados no art. 5º da Constituição, por meio da EC 115/2022, reforça a tese de que se trata de um direito fundamental de máxima densidade normativa. Isso significa que as restrições a esse direito só podem ocorrer por meio de lei, devem observar os princípios da proporcionalidade e da razoabilidade, e jamais podem afetar seu núcleo essencial. Essa estrutura protetiva está em sintonia com os parâmetros do **Tribunal Constitucional Federal Alemão**, cuja jurisprudência pioneira consolidou o direito à autodeterminação informativa como garantia contra o “cadastro total” do indivíduo pelo Estado (MARTINS, 2020, p. 91).

Por outro lado, a inserção constitucional do direito à proteção de dados também impõe uma nova racionalidade às políticas públicas. Programas sociais, iniciativas de segurança pública ou estratégias de saúde populacional devem ser desenhados com respeito aos princípios

constitucionais de finalidade e minimização de dados. O tratamento de dados, mesmo quando promovido pelo Estado, deve ser informado, legítimo, necessário e seguro — não se admite que a vulnerabilidade social sirva de pretexto para práticas de coleta de dados indiscriminadas.

Nesse ponto, torna-se relevante a construção de um controle de convencionalidade em matéria de dados, tendo como parâmetro a **Declaração Universal sobre Bioética e Direitos Humanos da UNESCO**, que estabelece que qualquer utilização de dados biométricos ou genéticos deve respeitar os princípios da dignidade, consentimento e integridade (UNESCO, 2005). A Constituição brasileira, ao integrar os tratados internacionais de direitos humanos, amplia o horizonte interpretativo da proteção de dados, permitindo a formação de uma jurisprudência mais sensível à complexidade do tema.

Outro elemento que deve ser enfrentado pela dogmática constitucional brasileira é a tensão entre liberdade de expressão e proteção de dados. A jurisprudência precisa distinguir a crítica legítima do uso abusivo de dados pessoais para linchamentos digitais, desinformação ou chantagens. O **STF já tem precedentes em que reconhece a prevalência da dignidade da pessoa humana sobre a liberdade de expressão em contextos de ofensa à intimidade e à vida privada, como se deu no julgamento da ADI 4815**, que tratou da divulgação de informações pessoais sensíveis em redes sociais.

A proteção de dados deve ser, portanto, entendida como parte do núcleo duro da Constituição, não sujeita a flexibilizações casuísticas. Em uma democracia pluralista, a identidade, a liberdade e a privacidade dos indivíduos são bens constitucionalmente protegidos que não podem ser reduzidos a ativos de mercado. A supremacia da Constituição impõe limites éticos e jurídicos às práticas digitais, transformando a proteção de dados em um novo campo de lutas constitucionais.

Finalmente, é preciso reconhecer que a consolidação da proteção de dados como direito fundamental exigirá o engajamento não apenas das instituições estatais, mas também da sociedade civil, das universidades, das organizações não governamentais e da imprensa. A Constituição não é um texto morto: ela exige interpretação viva e participativa, capaz de responder aos desafios tecnológicos com base em seus princípios fundantes.

A proteção de dados, sob a perspectiva constitucional, **é uma exigência de justiça,**

liberdade e igualdade na sociedade em rede. Ela expressa o compromisso do Estado brasileiro com a dignidade da pessoa humana em sua dimensão contemporânea e projeta o futuro da cidadania digital no século XXI.

3.1 A ATUAÇÃO DOS TRIBUNAIS SUPERIORES NA CONSOLIDAÇÃO DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS

A atuação dos Tribunais Superiores brasileiros tem sido determinante para a consolidação do direito à proteção de dados pessoais como um verdadeiro direito fundamental, dotado de eficácia normativa plena e exigibilidade imediata. O Supremo Tribunal Federal (STF), em especial, vem sendo protagonista na construção jurisprudencial do conteúdo, dos limites e da eficácia desse direito no Brasil, especialmente após o advento da Lei nº 13.709/2018 (LGPD) e da Emenda Constitucional nº 115/2022, que incluiu expressamente o direito à proteção de dados no rol dos direitos fundamentais.

A jurisprudência do STF, desde 2020, tem reiterado que a proteção de dados deve ser interpretada à luz da dignidade da pessoa humana e da autodeterminação informativa. O julgamento das **ADIs 6387, 6388, 6389, 6390 e 6393**, que discutiam o compartilhamento de dados telefônicos com o IBGE durante a pandemia, é paradigmático nesse sentido. Ali, a Corte afirmou, por maioria, que "a proteção de dados pessoais constitui direito fundamental autônomo, intimamente ligado à privacidade e ao livre desenvolvimento da personalidade" (STF, ADI 6387, voto do Min. Alexandre de Moraes, 2020).

Esse julgamento foi o primeiro a reconhecer expressamente a natureza fundamental do direito à proteção de dados, mesmo antes da promulgação da EC 115/2022. O STF adotou uma interpretação pró-eficácia dos direitos fundamentais, aplicando diretamente princípios constitucionais como o da proporcionalidade, finalidade, adequação e segurança, em conformidade com os arts. 1º, III, 5º, X e XII da CF/88, e com o art. 2º da LGPD.

Outro caso de significativa relevância foi o julgamento da **ADI 6561**, que tratava da criação, por lei estadual, de um cadastro de usuários de drogas no Estado do Tocantins. O STF declarou a norma inconstitucional, destacando a violação aos princípios da legalidade, da finalidade e da necessidade, além da ausência de salvaguardas adequadas quanto à guarda, segurança e uso dos dados pessoais. A Corte reforçou que "a criação de banco de dados

sensíveis sem fundamento constitucional e legal claro configura violação à autodeterminação informativa" (STF, ADI 6561, Rel. Min. Gilmar Mendes, 2020).

Esses entendimentos se aproximam da doutrina desenvolvida por Ingo Sarlet e Giovani Saavedra, segundo os quais o direito à proteção de dados deve ser compreendido como um "direito-ponte" entre a privacidade e a liberdade informacional, estando inserido no "núcleo duro" dos direitos fundamentais contemporâneos (SARLET; SAAVEDRA, 2020, p. 34).

A interpretação do STF também tem evoluído no que diz respeito ao compartilhamento de dados entre órgãos públicos. No julgamento da **ADI 6649 e ADPF 695**, a Corte estabeleceu critérios estritos para a constitucionalidade dessas práticas, afirmando que o compartilhamento de dados cadastrais entre entes públicos deve atender ao princípio da necessidade e ser limitado à mínima medida exigida para atingir a finalidade pública declarada, observando rigorosamente os protocolos de segurança e controle de acesso. A decisão reafirmou que "o simples fato de os dados serem públicos não autoriza sua circulação irrestrita entre entes administrativos, sob pena de violação à dignidade e ao livre desenvolvimento da personalidade" (STF, ADI 6649, voto do Min. Rosa Weber, 2022).

Em 2023, o STF voltou a se manifestar sobre a proteção de dados genéticos, julgando a **ADI 5545 (citada anteriormente)**, que impugnava a obrigatoriedade legal da coleta de material genético de mães e recém-nascidos no momento do parto, para formação de um banco genético estadual. A Corte considerou a prática inconstitucional, destacando que "dados genéticos, por sua natureza sensível, exigem protocolos rigorosos de segurança e não podem ser objeto de coleta compulsória sem consentimento e sem previsão legal clara e proporcional" (STF, ADI 5545, 2023). A decisão espelha a orientação da LGPD quanto à natureza sensível dos dados biométricos e genéticos (art. 5º, II), impondo padrões de governança de dados compatíveis com o modelo europeu (GDPR).

Na **ADC 51**, o STF analisou a possibilidade de autoridades brasileiras requisitarem dados diretamente de provedores de internet com sede no exterior. O Tribunal considerou que a interpretação conjunta do art. 11 do Marco Civil da Internet com o art. 18 da Convenção de Budapeste autoriza essa prática, desde que respeitados os direitos fundamentais dos titulares. Para a Corte, "a soberania digital brasileira deve ser compatibilizada com o respeito aos direitos fundamentais dos usuários, especialmente no que diz respeito à proteção de dados" (STF, ADC

51, voto do Min. Gilmar Mendes, 2023).

Essa compreensão se aproxima da ideia de soberania informacional, defendida por autores como Caitlin Mulholland, para quem o Estado deve garantir um ambiente digital regulado, ético e compatível com os princípios constitucionais, sob pena de esvaziamento do próprio projeto democrático (MULHOLLAND, 2018, p. 174).

A análise comparada demonstra que a jurisprudência brasileira tem avançado em consonância com as Cortes Constitucionais estrangeiras. O Tribunal Constitucional Federal Alemão, em decisão histórica de 1983, reconheceu que a autodeterminação informativa é um direito fundamental derivado do princípio da dignidade da pessoa humana e do livre desenvolvimento da personalidade, sendo vedada a formação de "perfil de cidadão" sem consentimento (MARTINS, 2020, p. 83).

Esse entendimento inspirou diretamente a formulação da LGPD e está sendo absorvido pela jurisprudência nacional, como se observa nos julgados que rechaçam práticas de coleta massiva e não consentida de dados. A construção do direito à proteção de dados como **"escudo informacional" contra práticas invasivas do poder público e do mercado revela a maturidade do constitucionalismo brasileiro** diante dos desafios da era digital.

A jurisprudência brasileira, ao reconhecer o direito à proteção de dados como cláusula pétrea, inverte a lógica do "vale-tudo informacional" e impõe limites substanciais à atuação do Estado e dos particulares. Trata-se de um movimento de contenção do poder informacional, a partir da Constituição, que reafirma o compromisso do país com o modelo democrático e inclusivo de proteção de direitos.

O STF, portanto, caminha no sentido de formar um "bloco de constitucionalidade informacional", reunindo o texto constitucional, a LGPD, os tratados internacionais e os princípios estruturantes da dignidade, da liberdade e da igualdade. Essa jurisprudência de proteção integral dos dados reflete um amadurecimento do controle de constitucionalidade sobre práticas digitais e posiciona o Brasil em diálogo com experiências avançadas como a do Tribunal de Justiça da União Europeia.

No entanto, a jurisprudência ainda precisa enfrentar com mais contundência questões

estruturais, como a regulação de algoritmos, o uso de inteligência artificial em decisões públicas e privadas e a responsabilização objetiva em grandes vazamentos de dados. O STJ e o STF ainda oscilam quanto à inversão do ônus da prova e à extensão do dano presumido em casos de violação à LGPD.

Ainda assim, o caminho percorrido é relevante. O controle judicial da proteção de dados já constitui um novo campo de constitucionalização das relações sociais e de humanização das tecnologias. A postura dos Tribunais Superiores brasileiros revela que, no constitucionalismo digital, a privacidade não é apenas uma questão individual, mas um valor público a ser resguardado institucionalmente.

A consolidação dessa linha jurisprudencial exige coerência, previsibilidade e atualização contínua por parte das Cortes. A proteção de dados como direito fundamental impõe ao Poder Judiciário o papel de guardião da identidade digital dos cidadãos, reafirmando que a Constituição de 1988 continua viva e apta a responder aos desafios da era dos dados.

4. DIREITO INTERNACIONAL - COMO O GDPR EUROPEU INFLUENCIA A INTERPRETAÇÃO DA LGPD NO BRASIL?

A Lei Geral de Proteção de Dados Pessoais (LGPD), ao ser aprovada no Brasil, não surgiu em um vácuo normativo. Ela foi claramente inspirada pelo Regulamento Geral de Proteção de Dados da União Europeia (GDPR), refletindo uma tendência global de reconhecimento do valor dos dados pessoais como direito fundamental. A estrutura principiológica, os fundamentos e até mesmo a nomenclatura adotada na LGPD demonstram uma replicação adaptada dos parâmetros europeus. Como observado pelos pensamentos do autor Renan Gadoni Canaan, o legislador brasileiro optou por seguir uma lógica convergente com o GDPR, buscando garantir segurança jurídica e estímulo à inovação tecnológica (CANAAN, 2022, p. 5).

A **aproximação normativa entre a LGPD e o GDPR** também se manifesta na estrutura de governança de dados. Ambas as normas instituem figuras similares, como o controlador, o operador e o encarregado pelo tratamento de dados (data protection officer – DPO). Essa semelhança estrutural visa facilitar o alinhamento regulatório entre países, essencial em tempos de globalização digital, em que dados circulam com facilidade entre

fronteiras (MAGALHÃES, 2021, p. 12).

Contudo, embora o Brasil tenha adotado esse modelo europeu, há diferenças marcantes no desenho institucional. Enquanto a GDPR conta com autoridades de proteção de dados independentes em cada Estado-membro da União Europeia, coordenadas pelo European Data Protection Board (EDPB), no Brasil a Autoridade Nacional de Proteção de Dados (ANPD) foi criada inicialmente como órgão vinculado à Presidência da República, o que gerou críticas quanto à sua autonomia decisória (RODOTÀ, 2009, p. 31).

Do ponto de vista jurisprudencial, a Corte de Justiça da União Europeia (CJUE) possui precedentes robustos que consolidam a proteção de dados como direito fundamental. Um dos mais importantes foi o caso *Google Spain SL v. Agencia Española de Protección de Datos* (C-131/12), em que a Corte reconheceu o direito ao esquecimento, afirmando que os cidadãos podem requerer a remoção de informações irrelevantes ou desatualizadas dos resultados de buscadores. No Brasil, o STF ainda não consolidou um entendimento uniforme sobre esse tema, o que demonstra uma lacuna interpretativa a ser preenchida.

A influência da GDPR também se reflete na formulação dos princípios da LGPD, como o da finalidade, da adequação, da necessidade, da livre acesso, da segurança e da não discriminação (art. 6º da LGPD), que se espelham diretamente no artigo 5º do GDPR. Essa convergência fortalece o argumento de que a LGPD não é uma norma isolada, mas sim parte de uma tendência transnacional de harmonização de direitos fundamentais na era digital.

Sob uma perspectiva funcionalista, a GDPR estabelece mecanismos mais robustos para o exercício de direitos dos titulares de dados, como o direito à portabilidade, à limitação do tratamento, à oposição e à revisão de decisões automatizadas. A LGPD incorporou essas prerrogativas, mas com escopo ligeiramente mais restrito, e com baixa incidência prática até o momento nos tribunais e na atuação da ANPD (CANAAN, 2022, p. 8).

A legislação americana, por sua vez, apresenta um modelo fragmentado, setorial e menos protetivo. A proteção de dados nos Estados Unidos é regulada por normas específicas para setores como saúde (HIPAA), finanças (GLBA) e crianças (COPPA), sem um estatuto federal unificado equivalente ao GDPR. Esse modelo dificulta a conformidade internacional e afasta os Estados Unidos da lógica dos direitos fundamentais observada na GDPR e, por

reflexo, na LGPD brasileira (MAGALHÃES, 2021, p. 17).

Mesmo com essas diferenças estruturais, é possível observar que algumas cortes americanas vêm reconhecendo, ainda que de forma incipiente, a violação de dados como uma violação à privacidade individual protegida pela Quarta Emenda. A jurisprudência norte-americana, entretanto, tende a ser mais permissiva com práticas empresariais de coleta massiva de dados, especialmente quando consentidas por contratos de adesão – o que seria inadmissível à luz do GDPR (NISSENBAUM, 2009, p. 89).

Outro ponto relevante de comparação refere-se ao papel do consentimento. No modelo europeu, o consentimento deve ser livre, informado, inequívoco e específico, com possibilidade de revogação. A LGPD adota a mesma lógica, mas admite hipóteses de tratamento sem consentimento, como o cumprimento de obrigação legal, interesse legítimo e execução de políticas públicas. Essa ampliação de bases legais gera debates sobre os limites da autodeterminação informativa no contexto brasileiro (REMOLINA ANGARITA, 2018, p. 7)

No que se refere à responsabilização por danos, o GDPR adota um modelo de responsabilidade objetiva, prevendo multas que podem alcançar até 4% do faturamento global anual da empresa. A LGPD também prevê sanções semelhantes, mas até o momento a aplicação prática dessas penalidades ainda está em fase inicial, com poucos precedentes e baixa atuação sancionatória da ANPD.

A doutrina de Stefano Rodotà, um dos principais arquitetos intelectuais da GDPR, contribui para o entendimento filosófico dessa regulação. Para ele, "a proteção de dados é a nova fronteira dos direitos fundamentais, pois representa a defesa do sujeito contra a mercantilização da identidade" (RODOTÀ, 2009, p. 19). Essa compreensão tem sido progressivamente incorporada no Brasil por autores como Sarlet e Mulholland, que identificam na proteção de dados uma condição de possibilidade da dignidade humana em ambientes digitais (SARLET; SAAVEDRA, 2020, p. 34; MULHOLLAND, 2018, p. 161).

Além disso, os mecanismos de accountability previstos na GDPR, como o registro das operações de tratamento, o relatório de impacto à proteção de dados (DPIA) e a nomeação de DPOs, também foram transplantados para a LGPD, embora sem o mesmo grau de obrigatoriedade e sofisticação. A LGPD, por exemplo, não exige relatório de impacto em todos

os casos, o que pode enfraquecer a prevenção de danos em ambientes de alto risco (CANAAN, 2022, p. 11).

Do ponto de vista dos fluxos internacionais de dados, o GDPR estabelece critérios rigorosos para a transferência internacional de dados, exigindo garantias adequadas de proteção no país de destino. A LGPD adotou os mesmos critérios no art. 33, mas carece de uma lista oficial de países considerados adequados pela ANPD, dificultando o comércio internacional de dados entre empresas brasileiras e estrangeiras.

A jurisprudência comparada também evidencia a diferença na efetividade da proteção. Enquanto o **Tribunal de Justiça da União Europeia** já declarou inválidas cláusulas contratuais padrão e tratados de transferência de dados (como no caso "Schrems II", C-311/18), o Brasil ainda não desenvolveu jurisprudência consolidada sobre transferência internacional de dados, permanecendo dependente de regulação futura da ANPD.

Finalmente, é importante destacar que a inspiração no GDPR não se deu apenas no plano normativo, mas também discursivo. A linguagem dos direitos fundamentais, do risco, da autodeterminação informativa e da prevenção permeia os debates legislativos e judiciais brasileiros, demonstrando um fenômeno de constitucionalização transnacional dos direitos digitais, conforme já apontado por Remolina Angarita (2018, p. 11).

4.1 SIMILARIDADES E DISCREPÂNCIAS ENTRE A PROTEÇÃO DE DADOS NO BRASIL E NO EXTERIOR

A proteção de dados pessoais, enquanto manifestação contemporânea dos direitos fundamentais, apresenta diferentes delineamentos e níveis de efetividade a depender do ordenamento jurídico em que se insere. Ao analisar comparativamente a legislação brasileira, especialmente a Lei Geral de Proteção de Dados Pessoais (LGPD), e os regimes de proteção de dados adotados no exterior — com destaque para a Europa e os Estados Unidos —, é possível identificar um conjunto de similaridades estruturais, mas também divergências marcantes quanto à aplicação prática, à interpretação judicial e à cultura de proteção da privacidade.

No que tange às similaridades, o ponto de convergência mais evidente é o reconhecimento do valor intrínseco dos dados pessoais como projeção da personalidade

humana. Tanto a LGPD quanto o *General Data Protection Regulation* (GDPR) europeu estabelecem expressamente que o tratamento de dados deve respeitar a dignidade da pessoa humana, o que insere a proteção de dados no núcleo dos direitos da personalidade. No caso europeu, essa diretriz é reforçada pelo artigo 8º da *Carta dos Direitos Fundamentais da União Europeia*, que institui o direito à proteção de dados como autônomo e distinto do direito à privacidade, já assegurado pelo artigo 7º. No Brasil, esse reconhecimento foi positivado com a promulgação da Emenda Constitucional nº 115/2022, que conferiu à proteção de dados pessoais status de direito fundamental, com eficácia plena e imediata.

Além disso, as legislações brasileira e europeia compartilham um arcabouço principiológico semelhante, fundado em valores como a finalidade, a adequação, a necessidade, a transparência, a segurança e a não discriminação. Esses princípios não apenas norteiam a interpretação das normas, mas também orientam a formulação de políticas públicas e condutas empresariais no tratamento de dados. Essa convergência evidencia a influência do modelo europeu na elaboração da LGPD, cuja vocação internacionalista buscou harmonizar o ordenamento brasileiro aos padrões globais de proteção de dados, garantindo maior previsibilidade jurídica e facilitando o trânsito internacional de informações (MAGALHÃES, 2021, p. 22).

Contudo, a análise comparativa revela importantes discrepâncias, especialmente no que se refere à efetividade normativa e à maturidade institucional. O GDPR apresenta um sistema de enforcement altamente robusto, com autoridades de supervisão independentes e dotadas de amplos poderes investigatórios e sancionatórios, como a *Commission Nationale de l'Informatique et des Libertés* (CNIL), na França, e o *Information Commissioner's Office* (ICO), no Reino Unido. No Brasil, embora a Autoridade Nacional de Proteção de Dados (ANPD) tenha sido criada com funções semelhantes, sua atuação ainda é embrionária, carecendo de independência financeira e administrativa consolidada. Essa fragilidade compromete a capacidade da ANPD de exercer plenamente seu papel fiscalizador e pedagógico, o que pode reduzir a eficácia prática da LGPD (CANAAN, 2022, p. 14).

Outro elemento que distingue os sistemas é a adoção e aplicação de instrumentos preventivos, como os *Data Protection Impact Assessments* (DPIAs) e o modelo de *privacy by design*. Tais mecanismos estão bem consolidados no contexto europeu, sendo obrigatórios em determinados tratamentos de alto risco. No Brasil, embora a LGPD preveja tais instrumentos,

sua implementação tem sido restrita, muitas vezes limitada a grandes empresas com capacidade técnica e financeira para realizar esse tipo de análise. Pequenas e médias empresas, que compõem a maior parte do tecido empresarial brasileiro, enfrentam dificuldades operacionais e econômicas para atender a esses requisitos, o que contribui para um abismo entre a letra da lei e sua aplicabilidade concreta (GARCEL; MORO, 2022, p. 5).

A forma de tratamento dos dados sensíveis também evidencia divergências substanciais. Enquanto o GDPR detalha de forma exaustiva as hipóteses legais de tratamento e exige avaliação de risco rigorosa para proteção adicional desses dados — como os relativos à saúde, à orientação sexual, à religião ou à origem étnica —, a LGPD remete muitos aspectos à regulamentação infralegal a ser elaborada pela ANPD. A ausência de diretrizes claras e específicas, portanto, gera insegurança jurídica e lacunas interpretativas que dificultam o cumprimento rigoroso da norma (RODOTÀ, 2009, p. 35).

O sistema sancionatório europeu também é mais rigoroso. O GDPR estabelece multas que podem alcançar até 20 milhões de euros ou 4% do faturamento global da empresa infratora, o que já resultou em sanções expressivas, como no caso da Google, multada em 50 milhões de euros pela CNIL em 2019. No Brasil, embora a LGPD preveja sanções administrativas, sua aplicação ainda é tímida, e não há precedentes com impacto comparável. A atuação da ANPD, nesse ponto, tem sido mais orientadora do que punitiva, o que pode comprometer o caráter dissuasório das sanções previstas.

Na esfera judicial, o contraste é ainda mais acentuado. O Tribunal de Justiça da União Europeia (TJUE) tem desempenhado papel central na consolidação do direito à proteção de dados, como demonstra a emblemática decisão “Schrems II”, que invalidou o acordo de transferência de dados entre União Europeia e Estados Unidos por ausência de garantias suficientes de proteção. O Brasil, por sua vez, ainda carece de uma jurisprudência consolidada sobre o tema, embora decisões como as proferidas na ADI 6387 e ADI 5545 pelo Supremo Tribunal Federal sinalizem um caminho promissor no reconhecimento da proteção de dados como direito fundamental vinculado à dignidade da pessoa humana.

Nos Estados Unidos, a lógica jurídica se orienta por uma abordagem contratual e setorial. Não há uma legislação federal única de proteção de dados, mas sim um mosaico normativo que abrange setores específicos, como o setor financeiro (Gramm-Leach-Bliley Act),

a saúde (HIPAA) e a educação (FERPA). Além disso, o direito à privacidade nos EUA é derivado da Quarta Emenda da Constituição, sendo aplicado sobretudo em contextos de buscas e apreensões ilegais. O modelo americano privilegia a autorregulação das empresas, e a responsabilização só costuma ocorrer mediante comprovação de dano concreto, o que limita o alcance da proteção preventiva (NISSENBAUM, 2009, p. 113).

Essa disparidade reflete uma diferença filosófica profunda. Enquanto o modelo europeu e, por extensão, o brasileiro, concebem a proteção de dados como uma questão de ordem pública, ligada à autodeterminação informativa e à dignidade da pessoa humana, o modelo norte-americano a trata como um bem negociável, sujeito às regras do mercado e à livre iniciativa. A adoção da responsabilidade objetiva na LGPD, mesmo sem exigência de dano material para a reparação, alinha o Brasil à lógica da precaução do GDPR, distanciando-o da tradição estadunidense (REMOLINA ANGARITA, 2018, p. 15).

A transferência internacional de dados é outro ponto de divergência. A GDPR exige que a Comissão Europeia reconheça a "adequação" do país destinatário ou que sejam adotadas cláusulas contratuais específicas e instrumentos jurídicos vinculantes. O Brasil ainda não possui uma lista oficial de países com nível adequado de proteção, o que gera insegurança para empresas brasileiras que atuam no comércio internacional. A indefinição da ANPD quanto aos critérios de adequação tem sido um entrave prático significativo (MAGALHÃES, 2021, p. 26).

Cultural e institucionalmente, a Europa possui uma longa tradição de proteção de direitos fundamentais, o que favorece a internalização da cultura da privacidade por parte da sociedade civil, das instituições públicas e das empresas. No Brasil, a proteção de dados ainda é um campo em construção, carente de maior engajamento educacional, normativo e corporativo. O nível de literacia digital da população brasileira é baixo, e muitas organizações tratam a LGPD como um fardo burocrático, e não como instrumento de fortalecimento da cidadania digital (CANAAN, 2022, p. 10).

Essa diferença de mentalidade é reforçada pela matriz jusfilosófica de cada sistema. A Europa é profundamente influenciada pelo pensamento de Kant, Hegel e Habermas, para quem a autonomia do sujeito é indissociável de sua capacidade de controlar suas informações. No Brasil, embora esse debate seja incipiente, autores como Ingo Sarlet, Giovani Saavedra, Caitlin Mulholland e Danilo Doneda vêm construindo uma doutrina sólida que insere a proteção de

dados no rol dos direitos da personalidade, ampliando o seu alcance teórico e prático (SARLET; SAAVEDRA, 2020, p. 34; MULHOLLAND, 2018, p. 161).

Portanto, embora haja pontos de contato relevantes entre os sistemas brasileiro, europeu e norte-americano de proteção de dados, as discrepâncias institucionais, culturais e filosóficas ainda são profundas. Para que o Brasil avance na consolidação de um regime de proteção de dados efetivo e compatível com os padrões internacionais, será necessário um esforço conjunto de desenvolvimento institucional, sensibilização da sociedade civil, qualificação técnica e fortalecimento da atuação da ANPD, além de um engajamento sério do Poder Judiciário na construção de uma jurisprudência protetiva e orientada por valores constitucionais.

5. A DIMENSÃO PATRIMONIAL E NÃO PATRIMONIAL DA PROTEÇÃO DE DADOS E A RESPONSABILIDADE CIVIL

5.1 SOBRE AS MULTAS DECORRENTES DA VIOLAÇÃO DE DADOS

O valor econômico dos dados pessoais transformou-se em uma realidade incontornável no cenário jurídico e mercadológico contemporâneo. O tratamento indevido de tais informações não apenas implica riscos à privacidade individual, mas também representa danos com consequências patrimoniais e extrapatrimoniais. A Lei Geral de Proteção de Dados (LGPD), ao prever sanções pecuniárias de até R$ 50 milhões por infração, conforme o artigo 52, revela uma tentativa de dar concretude à proteção legal em um ambiente em que os dados pessoais se tornaram moeda de troca em plataformas digitais e estratégias empresariais (COTS; OLIVEIRA, 2019).

Essas sanções administrativas, entretanto, não são meramente simbólicas. A primeira multa aplicada pela Autoridade Nacional de Proteção de Dados (ANPD), no caso da empresa *Telekall Infoservice*, evidenciou que mesmo pequenas empresas podem ser alvo de fiscalização rigorosa. A empresa foi multada por oferecer bancos de dados contendo contatos de mais de 130 milhões de usuários de WhatsApp para fins eleitorais, violando os artigos 7º e 41 da LGPD, além do artigo 5º do Regulamento de Fiscalização da ANPD. A sanção totalizou R$ 14.400,00, considerando o porte da empresa (SANTOS; SOUZA, 2025).

Mais que o montante financeiro, essa decisão possui valor pedagógico e reafirma a

centralidade da proteção de dados como bem jurídico relevante. Segundo Santos e Souza, "a aplicação da sanção representa a consolidação da LGPD como mecanismo efetivo de responsabilização, mesmo diante de condutas aparentemente triviais do ponto de vista comercial" (SANTOS; SOUZA, 2025, p. 17).

Contudo, a responsabilização civil ainda enfrenta obstáculos interpretativos no Judiciário. Conforme Cots e Oliveira (2019), o modelo de responsabilidade objetiva previsto na LGPD (art. 42) exige que se prove o dano, o nexo causal e a conduta lesiva, o que por vezes limita a eficácia protetiva da norma. Em complemento, Schreiber (2014) adverte que o dano extrapatrimonial causado por vazamento de dados deve ser analisado à luz da dignidade da pessoa humana e do direito à autodeterminação informativa.

A dualidade entre dano patrimonial e não patrimonial é evidenciada em julgados que envolvem, por exemplo, o uso não autorizado de dados para fins comerciais. Quando um titular tem seus dados vazados e passa a receber ligações indevidas ou tem seu nome vinculado a práticas comerciais com as quais não consentiu, há, segundo entendimento doutrinário, tanto a violação a um direito de personalidade quanto um prejuízo econômico direto (Junior; Ricardo, 2019).

Desse modo, ao avaliar se as multas previstas na LGPD são suficientes para garantir a proteção de dados pessoais, deve-se considerar que elas funcionam como mecanismos dissuasórios e corretivos. No entanto, sua efetividade depende da robustez institucional da ANPD, da transparência na aplicação das penalidades e da articulação com o Judiciário para a reparação civil do dano.

A discussão sobre o valor econômico dos dados, assim, não pode se limitar ao impacto financeiro das sanções. Como bem ressaltam Cots e Oliveira (2019), é preciso observar também os aspectos estruturais que envolvem a governança da informação, a arquitetura das plataformas digitais e o papel da LGPD na construção de um ecossistema de confiança.

A proteção de dados pessoais não se limita à esfera técnica ou regulatória, tampouco se restringe ao campo da segurança da informação. Na verdade, trata-se de um direito de personalidade com desdobramentos que tocam diretamente valores constitucionais — como a dignidade humana, a privacidade e a autodeterminação informativa — e que comporta tanto

implicações de ordem patrimonial quanto não patrimonial (Capanema, 2020).

No plano patrimonial, os dados tornaram-se ativos valiosos para o mercado digital, sendo utilizados como matéria-prima para estratégias de marketing, personalização de serviços, desenvolvimento de produtos e precificação dinâmica. Essa lógica insere os dados no contexto da chamada "economia da informação", em que eles adquirem valor econômico mensurável. Como destacam Bruno Bioni e Daniel Dias, a estrutura da LGPD adotou um regime de responsabilidade civil subjetiva, mas com critérios objetivos de aferição da violação de deveres, de modo a facilitar o acesso à reparação e a evitar a desconsideração do dano patrimonial sofrido em razão da exploração indevida dos dados (BIONI; DIAS, 2020).

Entretanto, não se pode negligenciar a dimensão não patrimonial que acompanha os danos decorrentes da violação de dados pessoais. O uso não autorizado de informações íntimas pode gerar sofrimento psíquico, humilhação, exposição indevida, bem como comprometer relações familiares, laborais e sociais. Como observa Walter Aranha Capanema, os efeitos do não atendimento às normas da LGPD repercutem em ações de responsabilidade civil justamente por causarem abalos que superam o plano econômico e adentram na violação à personalidade e à integridade moral do titular dos dados (Capanema, 2020, p. 164).

Nessa perspectiva, a própria configuração dos danos à luz da LGPD exige um olhar bifocal, que compreenda a multiplicidade dos efeitos do tratamento indevido. Isso é reforçado pela doutrina ao afirmar que os dados são expressão da identidade do sujeito, e sua violação pode significar tanto perda patrimonial quanto diluição de atributos existenciais que compõem sua pessoa, como a honra, o nome, a reputação e o livre desenvolvimento da personalidade (BIONI; DIAS, 2020).

Ademais, o art. 52 da LGPD prevê que, além das sanções administrativas, como advertências e multas, deve haver reparação integral dos danos causados, o que inclui os danos materiais e morais. Essa previsão vincula-se à ideia de que a responsabilização não pode se esgotar na compensação pecuniária, mas deve abarcar também a reconstituição simbólica da dignidade violada e a garantia de não repetição da conduta ilícita. Nessa linha, autores como Danilo Doneda sustentam que a proteção de dados exige um novo olhar sobre os institutos clássicos da responsabilidade civil, ampliando o seu escopo para além do critério puramente pecuniário (Doneda, 2018).

Ainda que seja possível quantificar, por exemplo, a perda de oportunidades decorrente de um vazamento de dados financeiros, o verdadeiro prejuízo pode estar na perda da confiança institucional, na percepção de vulnerabilidade digital e no medo constante da exposição. Esses aspectos não são menos danosos apenas porque são imateriais; ao contrário, muitas vezes sua repercussão subjetiva é mais perene e destrutiva que os prejuízos mensuráveis.

Em síntese, a dualidade entre os conteúdos patrimonial e não patrimonial no campo da proteção de dados deve ser compreendida como complementar e não excludente. A violação de dados pode comprometer não apenas os bens materiais do indivíduo, mas também sua liberdade, autonomia, imagem e projeto de vida — valores protegidos pela Constituição e pela própria ratio da LGPD. Portanto, o ordenamento jurídico precisa tratar esses dois aspectos com igual seriedade, sem relegar a dimensão existencial a uma categoria secundária da tutela civil.

A transformação digital que marcou as últimas décadas converteu os dados pessoais em ativos estratégicos no novo modelo econômico global. Essa virada paradigmática insere os dados no centro da atividade econômica, tornando-os comparáveis a recursos naturais essenciais como o petróleo. É a chamada “data-driven economy”, em que o valor das empresas é medido, em grande parte, por sua capacidade de extrair, analisar e monetizar informações pessoais (Zuboff, 2015).

Essa lógica de valorização dos dados se consolida com a expansão dos algoritmos e das plataformas digitais, que utilizam essas informações para direcionamento de publicidade, modelagem de perfis de consumo e predição comportamental. Segundo Magalhães (2020), a personalização dos serviços oferecidos por empresas de tecnologia e o crescimento de setores como o marketing digital e o e-commerce demonstram que os dados passaram a desempenhar papel central na dinâmica de mercado, sendo cotados e comercializados como ativos intangíveis de alto valor.

A literatura aponta que a coleta e o tratamento massivo de dados permitiram o surgimento de um novo modelo de acumulação capitalista, que Shoshana Zuboff batizou de “capitalismo de vigilância”. Nesse contexto, o comportamento humano é transformado em matéria-prima gratuita para processos comerciais secretos, nos quais empresas controlam, preveem e influenciam condutas futuras em benefício próprio (Zuboff, 2015). Trata-se de uma

exploração econômica que opera não apenas sobre a informação, mas sobre a própria liberdade dos indivíduos.

Autores como Stefano Rodotà já advertiam, antes mesmo da expansão total das redes digitais, que os dados pessoais deixavam de ser simples registros administrativos e passavam a constituir o núcleo de uma nova cidadania, cuja integridade deveria ser protegida com o mesmo rigor dispensado aos direitos fundamentais tradicionais (Rodotà, 2009). A lógica da monetização dos dados, contudo, tensiona essa proteção, transformando o sujeito de direitos em objeto de análise mercadológica.

No Brasil, o fenômeno da "dataficação" da vida social ganha contornos próprios a partir da inserção da LGPD no ordenamento jurídico. A lei impõe restrições à coleta desmedida de dados e prevê sanções significativas em caso de tratamento irregular, evidenciando que, mesmo como ativos de mercado, os dados não podem ser dissociados de seu titular, pois permanecem juridicamente vinculados à pessoa a quem dizem respeito (Capanema, 2020).

O mercado de dados é, de fato, uma das esferas mais lucrativas da economia contemporânea. Como apontado em estudo da Ambra University, empresas de tecnologia como Facebook, Google e Amazon construíram seus impérios baseando-se quase exclusivamente na exploração de dados pessoais, cuja coleta massiva permite lucrar com anúncios hiper personalizados e negociação de perfis comportamentais (Magalhães, 2020). A rentabilidade dessa lógica impulsionou a criação de startups especializadas na compra e venda de informações pessoais, muitas vezes em mercados informais e sem regulação adequada.

Esse cenário reforça a ideia de que os dados se tornaram ativos comerciais com valor mensurável, integrando o patrimônio informacional das empresas e exigindo controle e responsabilidade quanto ao seu uso. O valor econômico dos dados também pode ser percebido nos casos de fusões e aquisições empresariais, nas quais a base de dados dos consumidores é considerada um dos **ativos mais relevantes da transação** (Moro; Garcel, 2021). O caso emblemático da compra do WhatsApp pelo Facebook, por exemplo, envolveu não apenas a tecnologia da plataforma, mas o acesso à rede de contatos e aos dados dos usuários.

Além disso, a jurisprudência brasileira já começou a reconhecer essa dimensão econômica dos dados. A decisão da ANPD de aplicar multa por infração à LGPD reforça a

importância da informação como bem juridicamente tutelado, cuja exploração indevida gera responsabilidade civil e administrativa (ANPD, 2023). O caráter pedagógico e repressivo das multas evidencia que a proteção de dados não se limita à moralidade institucional, mas abrange valores econômicos substanciais.

Neste viés, o valor econômico dos dados pessoais no ambiente digital é incontestável. Eles não apenas influenciam decisões de consumo e estratégias empresariais, como também passaram a integrar o núcleo patrimonial das corporações. Essa realidade exige do Direito uma resposta regulatória firme, que reconheça o potencial danoso do uso abusivo desses dados e assegure, em paralelo, a sua proteção como extensão da personalidade e projeção econômica do indivíduo na sociedade da informação.

5.1 CONSEQUÊNCIAS CONCRETAS QUANTO À VIOLAÇÃO DE DADOS DA PESSOA

A violação de dados pessoais pode causar danos que extrapolam a dimensão econômica, atingindo diretamente esferas sensíveis da existência humana, como a dignidade, a intimidade e a identidade dos indivíduos. A doutrina contemporânea reconhece que os efeitos da exposição indevida de informações pessoais são muitas vezes irreversíveis, comprometendo a confiança social, a segurança individual e a autodeterminação informativa do titular (Moro; Garcel, 2021).

Em termos concretos, os danos decorrentes de vazamentos de dados podem se manifestar sob múltiplas formas: constrangimento público, discriminação em processos seletivos ou financeiros, exposição de dados sensíveis que revelam aspectos de saúde, orientação sexual ou convicções políticas, além de prejuízos psicológicos e morais relacionados ao sentimento de insegurança e perda de controle sobre a própria identidade digital (Silva, 2021).

No **plano prático**, o vazamento de dados também pode resultar em fraudes bancárias, clonagens de identidade, uso indevido de informações para fins de chantagem, estelionato e outras práticas criminosas. Como observado pela pesquisadora Gisele Truzzi, o ambiente digital aumentou exponencialmente a capacidade de alcance e dano das ações ilegais com dados pessoais, tornando indispensável a responsabilização civil e administrativa dos agentes que descumprem os deveres legais (Truzzi, 2020).

Tais consequências tornam-se ainda mais graves quando envolvem dados pessoais sensíveis. A divulgação indevida desses dados pode acarretar **discriminação direta, perda de oportunidades profissionais e sociais, além de comprometer a reputação e integridade moral da pessoa atingida**.

É relevante destacar que o dano decorrente da violação de dados pode ser também difuso ou coletivo. Quando milhares de titulares têm suas informações comprometidas por uma única falha de segurança, os efeitos são massivos e impactam a coletividade. Nesses casos, o Ministério Público e entidades civis podem atuar judicialmente, como já observado em diversas ações coletivas ajuizadas com base na LGPD e no Código de Defesa do Consumidor (Melo, 2021).

Além disso, a confiança dos usuários nas instituições responsáveis pelo tratamento de dados é fortemente abalada diante de uma violação. Como destaca Marcos Magalhães, a credibilidade das organizações passa a ser medida não apenas pela qualidade de seus produtos ou serviços, mas também pela capacidade de proteger os dados que lhes são confiados (Magalhães, 2020). A perda de reputação institucional pode ter reflexos econômicos significativos, incluindo queda de receitas, evasão de clientes e desvalorização da marca no mercado

A partir de 2022, com a efetiva atuação fiscalizadora da Autoridade Nacional de Proteção de Dados (ANPD), os impactos concretos da violação de dados se tornaram ainda mais tangíveis. A aplicação da primeira multa com base na LGPD — contra uma pequena empresa que não possuía política de privacidade adequada — demonstrou que, mesmo em escala reduzida, as consequências jurídicas são relevantes (ANPD, 2022). A sanção teve efeitos pedagógicos e serviu como alerta para o mercado quanto à necessidade de conformidade com os princípios da legislação.

Nesse sentido, a violação de dados também pode comprometer o exercício de direitos fundamentais, como o direito ao voto livre e informado, à liberdade de expressão e à igualdade de oportunidades. Casos como o escândalo da Cambridge Analytica, no qual dados de milhões de usuários do Facebook foram utilizados para manipulação de campanhas políticas, demonstram como o mau uso de dados pessoais ameaça os pilares da democracia contemporânea (Zuboff, 2015).

Diante desse panorama, torna-se **inquestionável que as consequências da violação de dados vão muito além do universo técnico.** Elas envolvem sofrimento humano, abalo à integridade pessoal e institucional, e distorção do equilíbrio democrático. Proteger os dados pessoais, portanto, é também proteger as condições mínimas de convivência social justa, segura e inclusiva — uma exigência ética e constitucional que se impõe ao Estado e ao mercado na sociedade da informação.

A imposição de multas administrativas é, por definição, um dos mecanismos mais visíveis do aparato sancionador da LGPD. Contudo, a verdadeira indagação que deve mover o pesquisador do Direito é se essas sanções pecuniárias, por si só, são aptas a modificar estruturas de comportamento institucional e promover a efetiva tutela dos direitos fundamentais à privacidade e à autodeterminação informativa. Em outros termos: a aplicação de multas garante proteção substancial, ou serve apenas como alívio simbólico e episódico para uma demanda crescente por justiça informacional?

Há uma tendência preocupante no sistema brasileiro: a de tratar a multa como o centro do regime sancionador da LGPD, ao invés de compreendê-la como parte de um ecossistema regulatório mais complexo, que inclui medidas reparatórias, educativas, preventivas e estruturantes. Ao analisar esse modelo, Rocha e Barros (2022) observam que as primeiras sanções aplicadas pela ANPD, por mais que tenham sido simbólicas, recaíram sobre pequenas empresas e geraram pouca ou nenhuma dissuasão estrutural junto aos grandes agentes econômicos, justamente os que concentram a maior quantidade de dados e operam sob modelos intensamente extrativistas.

A resposta institucional brasileira, nesse aspecto, ainda padece de uma lógica de enforcement reativa e fragmentada. A LGPD, ao prever um teto de R$ 50 milhões por infração (art. 52, II), aparentemente importou o modelo europeu do GDPR, mas sem dotar a ANPD dos instrumentos investigativos, orçamentários e operacionais adequados para implementar um modelo de regulação responsiva ou punitiva robusta. Como pontua Costa (2022, p. 113), há um risco real de que as multas se tornem, na prática, meras externalidades negativas do modelo de negócio das grandes plataformas, e não um fator real de transformação.

Esse argumento encontra eco no pensamento de Shoshana Zuboff, ao descrever o

modelo de negócios das big techs como “capitalismo de vigilância” — uma lógica na qual o custo eventual de multas é absorvido como parte do orçamento, sem qualquer impacto real sobre a engrenagem central da captura e monetização de dados (Zuboff, 2015, p. 77). Nesse sentido, a multa não representa ruptura, mas sim assimilação da ilegalidade ao modelo de lucro. A questão se agrava quando se constata que os mecanismos judiciais de responsabilização civil ainda enfrentam obstáculos, como a dificuldade de comprovação de danos, a hipossuficiência técnica dos consumidores e o alto custo processual de litígios envolvendo dados pessoais.

No plano teórico, Tomasevicius Filho (2022, p. 111) alerta para a necessidade de compreender a multa não como fim em si mesma, mas como parte de um sistema regulatório que produza efeitos pedagógicos, estruturais e simbólicos. Isso implica combinar sanção com orientação, punição com incentivo à adoção de boas práticas e responsabilização com políticas públicas de transparência e educação digital.

A crítica, portanto, não é à existência da multa — que é necessária —, mas à sua insuficiência como eixo único de enforcement. Em um sistema marcado por assimetria informacional e desequilíbrio entre titulares e controladores, a sanção pecuniária precisa estar acompanhada de outras formas de controle e responsabilização. Souza (2021, p. 61) é direto ao afirmar que "a multa administrativa não garante, por si, qualquer reparação às vítimas", apontando a urgente necessidade de integração entre esfera administrativa, civil e, em certos casos, penal.

É nesse ponto que o Brasil parece ainda imaturo institucionalmente. A ANPD não possui, até o presente momento, um programa articulado de cooperação com o Ministério Público, o Poder Judiciário e os órgãos de defesa do consumidor, como o Procon. A fragmentação do enforcement compromete a ideia de proteção integral e efetiva. Além disso, como alerta Canaan (2022, p. 107), a baixa densidade regulatória da ANPD no que tange à avaliação de impacto regulatório, à fixação de parâmetros claros de cálculo das multas e à publicização das decisões administrativas impede que o sistema se torne previsível, transparente e, sobretudo, confiável.

Outro ponto crítico reside no fato de que a multa administrativa não opera sobre a subjetividade das organizações, ou seja, não promove cultura de proteção. O que faz isso são mecanismos internos como governança de dados, compliance, adoção de práticas de “privacy

by design” e, especialmente, uma cultura corporativa que trate dados como valor público e não como recurso explorável. Silveira (2022, p. 99) ressalta que as multas, por mais elevadas que sejam, não têm o poder de transformar estruturas internas sem um processo contínuo e coerente de autorregulação e controle social.

Deve-se considerar a fragilidade dos mecanismos de reparação. No modelo atual, a vítima de vazamento ou uso indevido de dados enfrenta um duplo desafio: de um lado, a invisibilidade do dano (muitas vezes difuso, coletivo ou não imediatamente quantificável); de outro, a opacidade do sistema de responsabilização. É uma “dupla invisibilidade”: do dano e da reparação. Nesse sentido, os autores do estudo "Responsabilidade civil pela violação de dados" argumentam que apenas a criação de uma jurisprudência sólida, combinada com regulação proativa e pressão social, pode reequilibrar as forças em jogo (Santos; Oliveira, 2022).

Desse modo, as multas, embora necessárias e expressivas, são absolutamente insuficientes para assegurar a efetividade da proteção de dados no Brasil. Elas devem ser compreendidas como um dos muitos instrumentos de uma política pública mais ampla, que envolva educação, controle social, responsabilização múltipla e, sobretudo, transformação estrutural da lógica do uso de dados. Sem isso, o sistema de proteção de dados corre o risco de se tornar, como diria Zuboff, apenas um verniz de legalidade sobre um modelo de exploração que continua intacto (Zuboff, 2015, p. 79).

5.2 A PROTEÇÃO DE DADOS PESSOAIS COMO EXPRESSÃO DOS DIREITOS DA PERSONALIDADE

A consolidação dos direitos da personalidade no ordenamento jurídico brasileiro não pode ser compreendida sem a análise dos marcos históricos que influenciaram a evolução dos direitos humanos no plano internacional. Desde o século XVII, movimentos sociais e políticos foram essenciais para a formação de garantias fundamentais que hoje integram as constituições modernas. O *Bill of Rights* de 1689, por exemplo, já antecipava liberdades civis como o direito à liberdade, à igualdade, à petição e à proibição de penas cruéis (GUERRA, 2015). Posteriormente, a Declaração de Independência dos Estados Unidos, em 1776, afirmou o princípio da soberania popular e influenciou diretamente a Declaração dos Direitos do Homem e do Cidadão, de 1789, fruto da Revolução Francesa, que encerrou o sistema de privilégios feudais e introduziu ideais de igualdade e cidadania (HOBSBAWM, 2014).

Esses documentos foram fundamentais para o reconhecimento de direitos inatos à pessoa humana, inaugurando o que Ramos (2020) classifica como a primeira dimensão dos direitos humanos — aqueles relacionados às liberdades civis e políticas. Com o tempo, surgiram novas dimensões: a segunda, com os direitos sociais; a terceira, voltada à solidariedade e à coletividade (como o direito ao meio ambiente); e até mesmo propostas de quarta e quinta dimensões, que abrangem temas como bioética, democracia participativa e o direito à paz (RAMOS, 2020).

Após os horrores da Segunda Guerra Mundial, a criação da ONU e a promulgação da Declaração Universal dos Direitos Humanos em 1948 representaram um novo marco na proteção da dignidade humana, influenciando diretamente o texto da Constituição Federal de 1988, considerada uma "Constituição Cidadã" por privilegiar os direitos fundamentais da pessoa (MENDES; BRANCO, 2018). A CRFB/88 incorporou direitos como a vida, liberdade, igualdade, intimidade e honra, presentes no artigo 5º, e que integram o conceito de direitos da personalidade. O Código Civil de 2002, em harmonia com a Constituição, dedicou um capítulo exclusivo a esses direitos, reconhecendo-os como inerentes, inalienáveis, imprescritíveis, vitalícios e absolutos (GAGLIANO; PAMPLONA FILHO, 2022).

No mundo contemporâneo, marcado pelo avanço tecnológico e pela circulação massiva de informações, os dados pessoais passaram a compor uma nova camada da personalidade humana. Nesse cenário, a Emenda Constitucional nº 115/2022 incluiu, expressamente, o direito à proteção dos dados pessoais no rol de direitos fundamentais, ampliando o alcance das garantias constitucionais frente à era digital (BRASIL, 2022). Como consequência, a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) surgiu para regulamentar o tratamento de dados pessoais e assegurar o livre desenvolvimento da personalidade, a privacidade e a liberdade individual. Inspirada no Regulamento Geral de Proteção de Dados Europeu (GDPR), a LGPD estruturou princípios como finalidade, necessidade, transparência e segurança, e criou mecanismos de fiscalização por meio da Autoridade Nacional de Proteção de Dados (ANPD), conferindo ao Brasil um sistema jurídico mais sólido e moderno de proteção da personalidade (PINHEIRO, 2020; MARTINS; LONGHI, 2020).

Dessa forma, a trajetória dos direitos da personalidade revela-se como um processo histórico contínuo, com raízes nas lutas por liberdade e igualdade, mas que se reinventa para

enfrentar os desafios contemporâneos da era digital. Proteger tais direitos é garantir que a dignidade humana, fundamento do Estado Democrático de Direito, não se perca frente às transformações sociais e tecnológicas.

CONSIDERAÇÕES FINAIS

É fato que a Lei Geral de Proteção de Dados Pessoais (LGPD) representa um marco jurídico de grande relevância para a consolidação de direitos fundamentais no Brasil, especialmente diante dos desafios impostos pela economia digital e pelo avanço das tecnologias de vigilância. No entanto, **a análise detalhada da doutrina, jurisprudência e do contexto normativo internacional revelou que a eficácia jurídica da LGPD ainda se encontra em construção**, exigindo um esforço conjunto entre o Estado, as empresas e a sociedade civil.

A investigação evidenciou que os dados pessoais adquiriram valor econômico considerável no ambiente digital contemporâneo, sendo tratados como ativos intangíveis de alto valor estratégico. Essa transformação impõe novos deveres aos agentes de tratamento, sobretudo no que tange à responsabilidade civil decorrente de incidentes de segurança e uso indevido das informações. Verificou-se, à luz da literatura especializada, que a simples previsão de sanções e multas, embora relevante, não é suficiente para garantir a efetividade da proteção de dados pessoais, sendo necessário um modelo robusto de governança e accountability, que valorize a prevenção e a cultura da privacidade (Bioni, 2019; Doneda, 2021).

Além disso, constatou-se que o modelo brasileiro, inspirado na General Data Protection Regulation (GDPR) europeia, reflete uma tentativa de inserção do país no cenário global de proteção de dados, mas ainda carrega desafios normativos, técnicos e institucionais, como a assimetria na aplicação da lei, a baixa conscientização dos titulares e a fragilidade estrutural da ANPD frente à complexidade das demandas contemporâneas (Canaan, 2018; Remolina Angarita, 2012).

A análise crítica da jurisprudência do STF e STJ indicou avanços relevantes, especialmente no reconhecimento da proteção de dados como um desdobramento do direito à privacidade e da dignidade da pessoa humana. No entanto, ainda se observa uma timidez institucional na consolidação de uma jurisprudência mais estável e coerente, capaz de oferecer previsibilidade jurídica e segurança ao titular dos dados. Em muitas situações, as Cortes

Superiores têm adotado uma postura reativa e casuística, o que dificulta a consolidação de parâmetros interpretativos sólidos e alinhados à proteção substancial dos direitos informacionais.

No **plano comparado,** a pesquisa destacou que o Brasil ainda precisa avançar na harmonização normativa com padrões internacionais mais exigentes, especialmente no que se refere à efetiva implementação dos princípios da autodeterminação informativa, finalidade, necessidade e não discriminação. A experiência europeia demonstra que o reconhecimento formal dos direitos dos titulares deve ser acompanhado de estruturas institucionais fortes, fiscalização efetiva e participação social, sob pena de esvaziamento normativo e vulnerabilização dos cidadãos frente à lógica predatória do capitalismo de vigilância (Zuboff, 2015; Rodotà, 2009).

As análises realizadas ao longo dos capítulos também permitiram evidenciar que a proteção de dados, além de constituir um direito fundamental de primeira grandeza, possui uma função instrumental para a promoção da cidadania digital e da inclusão social. Em um país marcado por profundas desigualdades estruturais, garantir a proteção de dados significa também democratizar o acesso à informação, fortalecer a autonomia dos indivíduos e prevenir formas contemporâneas de discriminação e exclusão baseadas em perfis algorítmicos e sistemas automatizados de decisão (Mendes, 2020; Mulholland, 2018).

Neste sentido, a pesquisa reafirma que a LGPD, mais do que um conjunto de regras, deve ser compreendida como uma ferramenta normativa de transformação social, capaz de resguardar os direitos fundamentais em um ambiente tecnológico cada vez mais intrusivo e assimétrico. A efetivação desse ideal exige uma leitura constitucionalizada da LGPD, em sintonia com os valores da dignidade da pessoa humana, da igualdade substancial e da liberdade informacional, de modo a garantir não apenas a conformidade formal, mas a concretização substancial dos direitos dos titulares.

A consolidação de um regime de proteção de dados eficaz no Brasil dependerá, portanto, da maturação institucional da ANPD, da qualificação do debate judicial sobre o tema, da capacitação técnica dos operadores do direito e do engajamento ativo da sociedade civil na defesa de seus direitos informacionais. Só assim será possível **construir um ambiente digital que não apenas respeite os direitos fundamentais, mas que os coloque no centro das decisões políticas, jurídicas e econômicas de uma sociedade verdadeiramente democrática**

e inclusiva.

REFERÊNCIAS

ALMEIDA, B. de A. et al. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. *Ciência & Saúde Coletiva*, Rio de Janeiro, v. 25, p. 2487-2492, 2020.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo; DIAS, 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*, v. 9, n. 3, 2020. Disponível em: https://civilistica.com/responsabilidade-civil-lgpd-e-cdc/. Acesso em: 31 mar. 2025.

BIONI, Bruno Ricardo et al. Xeque-mate: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI/USP, 2015. p. 692-708.

BRASIL. Código Civil. Lei nº 10.406, de 10 de janeiro de 2002. Diário Oficial da União, Brasília, DF, 11 jan. 2002.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 29 maio 2025.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Diário Oficial da União, Brasília, DF, 11 fev. 2022.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. *Diário Oficial da União: seção 1*, p. 1, 15 ago. 2018.

BRASIL. Supremo Tribunal Federal. *Ação Declaratória de Constitucionalidade n. 51*, Relator: Min. Gilmar Mendes, Brasília, DF, 24 fev. 2023. Disponível em: http://www.stf.jus.br. Acesso em: 31 mar. 2025.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade n. 4815*, Relator: Min. Gilmar Mendes, Brasília, DF, 15 jun. 2022. Disponível em: http://www.stf.jus.br. Acesso em: 31 mar. 2025.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade n. 5545*, Relator: Min. Ricardo Lewandowski, Brasília, DF, 10 abr. 2023. Disponível em: http://www.stf.jus.br. Acesso em: 7 out. 2024.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade n. 6387*, Relator: Min. Alexandre de Moraes, Brasília, DF, 7 maio 2020. Disponível em: http://www.stf.jus.br. Acesso em: 31 mar. 2025.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade n. 6561*, Relator: Min. Gilmar Mendes, Brasília, DF, 17 set. 2020. Disponível em: http://www.stf.jus.br. Acesso em: 31 mar. 2025.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade n. 6586*, Relator: Min. Rosa Weber, Brasília, DF, 7 out. 2020. Disponível em: http://www.stf.jus.br. Acesso em: 31 mar. 2025.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade n. 6649*, Relator: Min. Rosa Weber, Brasília, DF, 7 abr. 2022. Disponível em: http://www.stf.jus.br. Acesso em: 31 mar. 2025.

BRASIL. Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental n. 695*, Relator: Min. Rosa Weber, Brasília, DF, 7 abr. 2022. Disponível em: http://www.stf.jus.br. Acesso em: 31 mar. 2025.

CANAAN, Renan Gadoni. Estímulo à inovação através de regulamentações para a proteção de dados pessoais: o impacto da replicação da GDPR na LGPD. [S.l.: s.n.], [s.d.].

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. [S.l.: s.n.], [2020?]. Disponível em: https://www.waltercapanema.com.br. Acesso em: 31 mar. 2025.

CARDOSO, Ana Paula. Pesquisa: 41,6% das empresas não sabem o que é LGPD. *Blog Reclame Aqui*. Disponível em: https://blog.reclameaqui.com.br/pesquisa-416-empresas-naosabem-que-e-lgpd/. Acesso em: 21 ago. 2020.

CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 1999.

CORTEZ, Frederico. O setor público está preparado para LGPD? *Focus.jor*, 2020. Disponível em: https://focuspoder.com.br/o-setor-publico-esta-preparado-para-lgpd-por-frederico-cortez/. Acesso em: 21 ago. 2020.

CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. v. 2, p. 83-96.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. Um código para a proteção de dados pessoais na Itália. *Revista Trimestral de Direito Civil*, Rio de Janeiro, v. 16, p. 117, 2003.

FAIRFIELD, J. A. T.; ENGEL, C. Privacy as a public good. *Duke Law Journal*, [S.l.], v. 65, p. 385, 2015.

FOUCAULT, Michel. *Vigiar e punir: nascimento da prisão*. 27. ed. Petrópolis: Vozes, 2021.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. v. 1, p. 23-52.

FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo. *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. Novo Curso de Direito Civil: parte geral. 21. ed. Salvador: JusPodivm, 2022.

GARCEL, Adriane; MORO, Sergio Fernando. Data Protection Law and its Interactions With The Anti-Money Laundering Law. In: *VII Simpósio Internacional de Direito Consinter / Universidad de Computense de Madrid*, 17 a 19 nov. 2020. *Revista Internacional CONSINTER de Direito*. Disponível em: https://revistaconsinter.com/. Acesso em: 31 mar. 2025.

GUERRA, Sidney. Curso de direitos humanos. 4. ed. Rio de Janeiro: Forense, 2015.

HOBSBAWM, Eric. A era das revoluções: 1789-1848. 26. ed. São Paulo: Paz e Terra, 2014.

LOBATO, Janaina Muniz. O princípio da dignidade da pessoa humana e o direito fundamental à proteção de dados pessoais no Brasil. *Revista FT, Ciências Humanas*, v. 29, ed. 140, nov. 2024. Disponível em: https://revistaft.com.br/o-principio-da-dignidade-da-pessoa-humana-e-o-direito-fundamental-a-protecao-de-dados-pessoais-no-brasil/. Acesso em: 30 mar. 2025. DOI: 10.69849/revistaft/cl10202411042126.

MARTINS, Leonardo de Faria Beraldo; LONGHI, Fernando. Lei geral de proteção de dados comentada. São Paulo: Revista dos Tribunais, 2020.

MAGALHÃES, Marcus. *Proteção de dados: estudo comparado de normas nacionais*. Orlando: Ambra University, 2024. Disponível em: https://orcid.org/0000-0002-9366-9007. Acesso em: 10 out. 2024.

MARTINS, Leonardo. *Tribunal Constitucional Federal Alemão: decisões anotadas sobre direitos fundamentais. Volume 1: dignidade humana. Livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física e igualdade*. São Paulo: Konrad-Adenauer Stiftung – KAS, 2016.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de direito constitucional. 13. ed. São Paulo: Saraiva, 2018.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2020.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. *Revista de Direito do Consumidor*, v. 120, p. 555-587, 2018.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, v. 19, n. 3, p. 159-180, 2018.

NISSENBAUM, H. *Privacy in context: Technology, policy and the integrity of social life*. Stanford, CA: Stanford University Press, 2009.

PATEMAN, Carole. Críticas feministas à dicotomia público privado. In: MIGUEL, Luis Felipe; BIROLI, Flávia (Org.). *Teoria política feminista: textos centrais*. Niterói: Eduff, 2013. p. 55-80.

PINHEIRO, Daniel. Proteção de dados pessoais: comentários à LGPD. Belo Horizonte: Fórum, 2020.

RAMOS, André de Carvalho. Curso de direitos humanos. 8. ed. São Paulo: Saraiva, 2020.

REMOLINA ANGARITA, N. Aproximación constitucional de la protección de datos personales en Latinoamérica. *Revista Internacional de Protección de Datos Personales*, [S.l.], v. 1, p. 1-13, 2012.

RODOTÀ, S. Data protection as a fundamental right. In: GUTWIRTH, S. et al. (ed.). *Reinventing data protection?*. Dordrecht: Springer Netherlands, 2009. p. 77-82.

SARLET, Ingo Wolfgang; SAAVEDRA, Giovani Agostini. Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à proteção de dados pessoais. *Revista Direito Público*, 2020.

SOLOVE, D. J. Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, [S.l.], v. 126, p. 1880, 2012.

ZUBOFF, S. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, [S.l.], v. 30, n. 1, p. 75-89, 2015.

GLOSSÁRIO

ADC – Ação Declaratória de Constitucionalidade: instrumento jurídico utilizado para declarar a conformidade de uma norma com a Constituição Federal.

ADI – Ação Direta de Inconstitucionalidade: mecanismo jurídico que visa declarar a inconstitucionalidade de uma norma perante a Constituição.

ANPD – Autoridade Nacional de Proteção de Dados: entidade da administração pública federal responsável por fiscalizar e implementar a LGPD no Brasil.

Anonimização – Processo pelo qual os dados perdem a possibilidade de associação, direta ou indireta, a um indivíduo, não sendo considerados dados pessoais.

Autodeterminação informativa – Direito do indivíduo de controlar as informações que lhe dizem respeito, inclusive quanto à coleta, uso e compartilhamento de seus dados pessoais.

Big Data – Grandes volumes de dados, estruturados ou não, que exigem técnicas específicas para análise, processamento e extração de valor.

Blockchain – Estrutura tecnológica descentralizada que armazena dados em blocos encadeados de forma criptografada e imutável.

Compliance digital – Conjunto de práticas e políticas adotadas por organizações para garantir a conformidade com leis e normas relacionadas à tecnologia e proteção de dados.

Consentimento – Manifestação livre, informada e inequívoca do titular dos dados, autorizando o tratamento de suas informações pessoais.

Cookie – Arquivo criado por sites e armazenado no navegador do usuário, utilizado para coletar dados sobre navegação.

Crowdsourcing – Estratégia de colaboração coletiva por meio da internet, para a obtenção de serviços, ideias ou conteúdos.

Data breach – Violação de dados: incidente de segurança que resulta na divulgação, acesso não autorizado ou perda de dados pessoais.

Dado pessoal – Qualquer informação relacionada a pessoa natural identificada ou identificável.

Dado sensível – Categoria especial de dado pessoal, relacionada à origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, dados genéticos ou biométricos.

Data Protection Officer (DPO) – Encarregado de proteção de dados: profissional responsável por atuar como canal de comunicação entre o controlador, os titulares e a ANPD.

GDPR – *General Data Protection Regulation*: regulamento europeu de proteção de dados que inspirou a LGPD brasileira.

Governança de dados – Conjunto de processos, políticas e estruturas que visam garantir a qualidade, segurança, privacidade e o uso ético dos dados em uma organização.

IoT (Internet of Things) – Internet das Coisas: conceito que descreve a conexão de objetos físicos à internet para coleta e troca de dados.

LGPD – Lei Geral de Proteção de Dados Pessoais: Lei n. 13.709/2018, que regulamenta o tratamento de dados pessoais no Brasil.

Machine learning – Aprendizado de máquina: técnica de inteligência artificial que permite a sistemas aprenderem automaticamente a partir de dados.

Minimização de dados – Princípio segundo o qual apenas os dados estritamente necessários para a finalidade pretendida devem ser coletados e tratados.

Privacy by design – Conceito segundo o qual a privacidade deve ser incorporada desde a concepção de um produto, serviço ou sistema.

Privacidade – Direito fundamental à proteção da vida privada e das informações pessoais de um indivíduo.

Profiling – Técnica de análise de dados usada para prever comportamentos, preferências ou características de indivíduos com base em dados pessoais.

STF – Supremo Tribunal Federal: órgão máximo do Poder Judiciário brasileiro, responsável por julgar questões constitucionais.

Tratamento de dados – Toda operação realizada com dados pessoais, incluindo coleta, produção, recepção, classificação, utilização, acesso, reprodução, armazenamento, eliminação, entre outras.