Cognitio Juris
ISSN 2236-3009

A PROTEÇÃO DA PRIVACIDADE DIGITAL: DESAFIOS DA COMERCIALIZAÇÃO DE DADOS PESSOAIS E A ATUAÇÃO DA LGPD EM UM CONTEXTO GLOBAL

DIGITAL PRIVACY PROTECTION: CHALLENGES OF THE COMMERCIALIZATION OF PERSONAL DATA AND THE EFFECT OF THE LGPD IN A GLOBAL CONTEXT

Artigo submetido em 08 de junho de 2025
Artigo aprovado em 10 de junho de 2025
Artigo publicado em 10 de junho de 2025

Cognitio Juris
Volume 15 – Número 58 – 2025
ISSN 2236-3009

.

Autor(es):
Daniel Rodrigues Martins [1]
Jefferson Franco Silva [2]

.

RESUMO: Este estudo tem como objetivo analisar os desafios e implicações relacionados à privacidade de dados pessoais na era digital, com ênfase na comercialização de informações no ciberespaço. A partir de uma abordagem teórica e legislativa, são discutidos os impactos

da coleta massiva de dados por plataformas digitais, o papel da Lei Geral de Proteção de Dados (LGPD) no Brasil e suas semelhanças com o Regulamento Geral de Proteção de Dados (GDPR) europeu. Observa-se que o direito à privacidade enfrenta ameaças significativas diante da lógica econômica que transforma dados em mercadoria, exigindo regulamentações rigorosas e ações educativas voltadas à conscientização da sociedade. O estudo evidencia a necessidade de uma postura crítica e ética da crescente digitalização das relações sociais, destacando a importância de garantir a autodeterminação informacional dos indivíduos como um direito fundamental. Conclui-se que, embora os avanços legais sejam relevantes, sua efetividade depende da articulação entre políticas públicas, fiscalização eficiente e engajamento da sociedade civil.

Palavras-chave: Ciberespaço; Plataformas Digitais; Regulamentações.

ABSTRACT: This study aims to analyze the challenges and implications related to personal data privacy in the digital age, with an emphasis on the commercialization of information in cyberspace. From a theoretical and legislative approach, the impacts of the mass collection of data by digital platforms, the role of the General Data Protection Law (LGPD) in Brazil and its similarities with the European General Data Protection Regulation (GDPR) are discussed. It is observed that the right to privacy faces significant threats in the face of the economic logic that transforms data into a commodity, requiring strict regulations and educational actions aimed at raising awareness in society. The study highlights the need for a critical and ethical stance towards the increasing digitalization of social relations, highlighting the importance of guaranteeing the informational self-determination of individuals as a fundamental right. It is concluded that, although legal advances are relevant, their effectiveness depends on the articulation between public policies, efficient monitoring and civil society engagement.

KEYWORDS: Cyberspace; Digital Platforms; Regulations.

1 INTRODUÇÃO

Na contemporaneidade, violação à privacidade digital tornou-se um obstáculo a ser superado diante da rápida expansão da tecnologia da informação e da crescente coleta e comercialização de dados pessoais.

Essa problemática exige uma perspectiva abrangente para que se possa compreender a complexidade do ambiente digital e as consequências da exposição de informações sensíveis. Cabe ressaltar que a prática disseminada de coleta e tratamento de dados, muitas vezes realizada sem a devida transparência e consentimento explícito dos titulares, constitui um verdadeiro impasse a ser resolvido na defesa dos direitos individuais.

Como a privacidade é um direito fundamental, torna-se essencial que se implemente uma postura combativa para enfrentar as ameaças que emergem no cenário digital. Nessa perspectiva, a regulamentação legal assume papel crucial ao assegurar que empresas e instituições tratem os dados pessoais com responsabilidade, respeitando os princípios de segurança e confidencialidade.

Cumpre acrescentar que a Lei Geral de Proteção de Dados (LGPD), no Brasil, exerce uma função essencial ao criar um ordenamento regulatório que visa resguardar os direitos dos titulares, promovendo uma vivência formativa tanto para organizações quanto para usuários quanto ao uso ético e legal dos dados.

Ademais, as legislações internacionais, em especial o General Data Protection Regulation (GDPR) da União Europeia, têm exercido grande influência e atuam como referência para o desenvolvimento de marcos regulatórios globais. Tal legislação estabelece um alicerce que serve de modelo para diversos países, oferecendo um fundamento sólido com o objetivo de elaborar políticas públicas que visam intensificar a garantia da privacidade e consolidar a segurança dos dados no contexto globalizado.

Sob esse prisma, analisar o impacto dessas legislações torna-se uma questão substancial e relevante, dada à interconexão dos sistemas e a circulação internacional de informações

pessoais.

Diante do disso, a presente pesquisa busca responder à seguinte problemática: quais desafios à privacidade digital emergem da comercialização de dados pessoais e de que maneira a legislação brasileira, em especial a LGPD, contribui para reduzir esses riscos e proteger os direitos dos titulares?

Dessa maneira, o objetivo deste trabalho é analisar os principais desafios decorrentes da comercialização de dados pessoais no ambiente digital, destacando o papel da LGPD e das legislações internacionais na mitigação dos riscos e na proteção efetiva dos direitos dos titulares.

Para tanto, será adotado um método de análise bibliográfica e documental que contempla os aspectos legais, técnicos e sociais envolvidos, buscando oferecer uma visão ampla do tema e subsidiar o debate sobre estratégias que possibilitem um equilíbrio entre inovação tecnológica e respeito à privacidade.

2 A PRIVACIDADE NA SOCIEDADE DIGITAL E O PAPEL DA LEGISLAÇÃO

O cenário atual da privacidade na era digital enfrenta desafios trazidos pela expansão da tecnologia e pela crescente recolhimento de informações pessoais, justamente pelo fato de os riscos inerentes a essa realidade, como o uso indevido, vazamentos e manipulações, evidenciarem a complexidade e a gravidade dessas questões para a segurança e autonomia dos indivíduos.

Em face disso, análise sobre os principais perigos enfrentados, como a violação de dados, o roubo de identidade e a exploração comercial, bem como a adequada discussão acerca do papel das normas regulatórias na proteção dos direitos dos titulares de dados são primordiais.

Assim, este tópico enfatiza a importância da responsabilidade compartilhada entre Estado,

empresas e sociedade para garantir a efetividade das ações voltadas à proteção e à consolidação de uma cultura de privacidade e segurança no meio digital

2.1 RISCOS À PRIVACIDADE DIGITAL E O PAPEL DA LGPD NA PROTEÇÃO DOS DADOS PESSOAIS

A privacidade digital configure-se como uma das principais preocupações da sociedade contemporânea, sobretudo em razão da constante digitalização dos processos e da prática disseminada da coleta, processamento e comercialização de dados pessoais.

Sob esse prisma, o avanço tecnológico proporcionou uma enorme expansão da coleta de informações, que, na maioria das vezes, ocorre sem o devido consentimento ou transparência por parte dos titulares, representando um obstáculo a ser superado na proteção dos direitos individuais.

Cumpre salientar que esse cenário impõe uma gama de vulnerabilidades quanto à integridade de dados pessoais sigilosos, tais como o uso indevido, vazamentos, fraudes e até mesmo manipulações direcionadas, características inerentes ao que Zuboff (2019) denomina de capitalismo de vigilância, no qual dados pessoais são explorados como commodities no mercado digital.

De acordo com Castells (2003), a sociedade em rede instaurou um novo paradigma social, no qual a circulação de informações é contínua e instantânea, implicando uma dificuldade considerável em controlar o fluxo e o uso desses dados pessoais.

Outrossim, Solove (2004) destaca que a privacidade na era digital não se limita apenas ao sigilo das informações, mas envolve também o direito ao controle e à autodeterminação informacional, princípios fundamentais que estão ameaçados diante do comércio indiscriminado de dados. Isso revela uma questão complexa que exige atenção especial, pois a coleta sem critérios claros resulta em vulnerabilidades para os titulares, comprometendo

sua liberdade e autonomia.

No cenário jurídico brasileiro, a entrada em vigor da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), representa um marco regulatório crucial para enfrentar esses desafios.

Conforme Costa e Mello (2021), a LGPD exerce uma função primordial ao estabelecer regras claras para o processamento de informações pessoais, definindo direitos e deveres para controladores, operadores e titulares.

A legislação brasileira cumpre um papel de certificar que os dados sejam coletados, armazenados e utilizados de forma responsável, transparente e segura, minimizando os riscos associados à comercialização indiscriminada desses dados (MOLINARIO; RUARO, 2019). Ademais, a LGPD está alinhada com regulamentações internacionais, como o GDPR europeu, o que proporciona uma estrutura compatível com padrões globais de proteção.

Vale destacar que, entre os principais riscos associados à comercialização de dados pessoais estão a exposição indevida de informações, a discriminação, a perda de privacidade, além do potencial uso para fins fraudulentos e manipulação social (MARTINEZ *et al*., 2019).

Essa prática representa um desafio de elevada magnitude, uma vez que, frequentemente, os usuários desconhecem a extensão e as consequências da captura e utilização das suas informações, principalmente em ambientes digitais e redes sociais, onde a mineração de dados é uma atividade rotineira (GROPP; MOTTA, 2020; GOMES, 2024).

Sob esse enfoque, a LGPD desenvolve uma atividade regulatória que visa resguardar a proteção dos dados pessoais e os direitos constitucionais dos cidadãos, impondo a necessidade do consentimento explícito e informando sobre o motivo e o controle sobre as informações pessoais.

Conforme Carvalho e Pedrini (2019), a lei também institui mecanismos de fiscalização e

sanções que contribuem para uma postura combativa contra práticas abusivas, incentivando a responsabilidade corporativa e o respeito à privacidade como um direito constitucional. Dessa forma, a aplicação da LGPD contribui para o desenvolvimento de uma cultura voltada à proteção e à segurança da informação., promovendo um ambiente digital mais confiável.

Além disso, é pertinente observar que o marco legal brasileiro atua como agente na consolidação da proteção da privacidade, estimulando a adoção de medidas técnicas e administrativas adequadas para garantir a segurança dos dados (FINKELSTEIN; FINKELSTEIN, 2019). Essas medidas são fundamentais para viabilizar a transparência e a responsabilidade no uso de dados pessoais, atendendo às demandas da sociedade e do mercado, que cada vez mais dependem da tecnologia para suas atividades cotidianas.

Por conseguinte, pode-se inferir que, apesar dos avanços legislativos, a proteção da privacidade digital ainda constitui uma problemática a ser tratada de forma contínua, pois os desafios tecnológicos e a complexidade do mercado de dados pessoais exigem atualizações constantes e aprimoramento dos mecanismos legais.

Sob esse prisma, a análise crítica da LGPD e sua aplicação prática se tornam indispensáveis para garantir que os direitos dos titulares sejam efetivamente salvaguardados frente às novas formas de exploração de informações no espaço digital

2.2 PRINCIPAIS RISCOS À PRIVACIDADE DIGITAL

A privacidade digital enfrenta riscos crescentes diante da expansão da coleta e comercialização de dados pessoais, muitas vezes sem o consentimento adequado dos titulares. Conforme destaca Castells (2003), a sociedade em rede intensificou a circulação de informações pessoais, criando vulnerabilidades que ameaçam o direito fundamental à privacidade. Essa exposição, amplificada pelas tecnologias digitais, gera uma série de riscos que afetam diretamente a segurança e autonomia dos indivíduos.

Um dos riscos mais significativos é a violação de privacidade, que ocorre quando informações pessoais são utilizadas sem autorização explícita ou para fins diversos daqueles originalmente consentidos. Essa conduta viola fundamentos essenciais do direito à privacidade, previsto tanto na Constituição Federal de 1988 (art. 5º, incisos X e XII) quanto no artigo 7º da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), que estabelece a necessidade de consentimento livre, informado e inequívoco para o processamento de informações pessoais (CARVALHO; PEDRINI, 2019; COELHO, 2023).

Segundo Martínez, Damasceno e Macedo (2019), a ausência de transparência e a comercialização de dados ampliam o risco de uso indevido dessas informações, colocando em xeque a confiança do usuário nas plataformas digitais.

Outro risco expressivo é o roubo de identidade, fenômeno que tem se intensificado com o vazamento e comercialização ilícita de dados pessoais. De acordo com Solove (2004), o uso indevido desses dados pode resultar em fraudes financeiras, abertura de contas bancárias fraudulentas e outras práticas criminosas que comprometem a integridade financeira e moral das vítimas.

Dados da Autoridade Nacional de Proteção de Dados (ANPD) indicam que, em 2023, cerca de 40% das denúncias recebidas estavam relacionadas à exposição indevida e uso ilícito de informações pessoais, evidenciando a gravidade dessa ameaça.

Além disso, destaca-se a exploração comercial com o uso de anúncios direcionados e da discriminação algorítmica. Zuboff (2019) conceitua esse fenômeno como “capitalismo de vigilância”, em que empresas capturam e monetizam informações pessoais para manipular comportamentos e influenciar decisões de consumo.

Essa prática compromete a autonomia do indivíduo, que é submetido a estratégias de mercado muitas vezes opacas e predatórias. Costa e Mello (2021) ressaltam que a LGPD introduziu medidas para limitar esses abusos, exigindo maior transparência e

responsabilização das instituições no uso e controle de informações pessoais, alinhando-se às normas europeias do GDPR.

Esses riscos, amplamente documentados na literatura, revelam a urgência de um marco regulatório eficaz para a proteção da privacidade digital. Como aponta Boff e Fortes (2014), a privacidade deve ser interpretada como um direito fundamental no ciberespaço, essencial para a preservação da dignidade humana e a garantia da cidadania digital.

A LGPD representa um avanço significativo nesse sentido, ao estabelecer princípios e obrigações claras para a gestão de dados, promovendo maior controle aos titulares e restringindo práticas abusivas (FINKELSTEIN; FINKELSTEIN, 2019).

Assim, é importante reconhecer que a preservação da intimidade no ambiente digital não é apenas uma questão legal, mas também social e ética. Molinaro e Ruaro (2019) alertam que a “negociação” e o “fim da privacidade” tornam-se problemas estruturais da sociedade contemporânea, exigindo conscientização e responsabilização conjunta entre usuários, empresas e Estado.

Dessa forma, a tutela das informações pessoais deve ser uma prioridade para assegurar um ambiente digital mais seguro, transparente e democrático.

2.3 A LGPD COMO INSTRUMENTO DE PROTEÇÃO

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) constitui um conjunto de normas regulatórias fundamental para a proteção da privacidade digital no Brasil. Inspirada na *General Data Protection Regulation* (GDPR) da União Europeia, a LGPD estabelece diretrizes claras e robustas para a administração de dados pessoais, enfatizando princípios como transparência, segurança, finalidade e consentimento livre, informado e inequívoco, conforme preconizado no artigo 6º da lei (COSTA; MELLO, 2021).

A legislação brasileira busca diminuir os riscos à privacidade digital por meio de mecanismos

essenciais, entre os quais destacam-se (i) o consentimento informado, (ii) os direitos dos titulares e (iii) a responsabilização e sanções.

O consentimento informado dispõe que a gestão de dados pessoais depende do autorização clara do titular, salvo nas exceções legais previstas no artigo 7º da LGPD, garantindo que o titular tenha gerenciamento do uso das suas informações.

O instrumento dos direitos dos titulares fomenta que a LGPD assegure aos cidadãos Direitos fundamentais, tais como o acesso simplificado aos dados, a retificação, a eliminação e a portabilidade das informações, promovendo o fortalecimento da autonomia e do controle individual sobre os dados pessoais. (CARVALHO; PEDRINI, 2019).

E a responsabilização e sanções impõem às empresas e às organizações que violarem as disposições da LGPD sujeição à penalidades severas, incluindo multas que podem chegar a 2% do faturamento anual, limitadas a R$ 50 milhões por infração, conforme previsto no artigo 52, promovendo maior rigor na proteção dos dados (FINKELSTEIN; FINKELSTEIN, 2019).

Embora a LGPD e a GDPR compartilhem fundamentos e objetivos semelhantes, como a centralidade do quanto ao consentimento e à proteção dos direitos dos titulares, há diferenças significativas entre as duas normas.

A GDPR, por exemplo, apresenta uma regulamentação mais detalhada acerca do processamento de dados sensíveis e do papel das Autoridades de Proteção de Dados, promovendo uma estrutura administrativa mais rígida (COSTA; MELLO, 2021).

Em contrapartida, a LGPD adota uma abordagem flexível, possibilitando adaptações conforme as particularidades do contexto brasileiro, especialmente em setores emergentes da economia digital.

A efetiva preservação da privacidade digital demanda uma responsabilidade compartilhada entre governos, empresas e sociedade civil. Enquanto o poder público detém o papel de

implementar e fiscalizar o cumprimento da legislação, cabe às organizações privadas a adoção de práticas éticas e investimentos contínuos em segurança da informação para prevenir abusos e vazamentos.

Segundo Solove (2004), a segurança dos direitos pessoais deve transcender a mera conformidade legal, configurando-se como uma prática essencial visando assegurar a confiança no ambiente virtual.

Dessa forma, a LGPD vai além de um mero conjunto de normas jurídicas, mas funciona como um instrumento para fomentar uma cultura de proteção de dados no Brasil. A conscientização dos titulares e a postura proativa das empresas são indispensáveis para enfrentar os desafios relacionados à comercialização irregular e ao uso indevido de dados pessoais.

Em conclusão, apesar de a venda e o compartilhamento de dados pessoais ainda representarem desafios significativos à privacidade digital, a LGPD oferece um arcabouço normativo robusto e moderno para mitigar tais riscos. Contudo, sua eficácia depende diretamente da fiscalização rigorosa, do comprometimento corporativo e do engajamento social (BOFF; FORTES, 2014).

Ademais, a harmonização entre a LGPD e a GDPR reforça a importância de normativas internacionais alinhadas para garantir a proteção dos direitos fundamentais à privacidade em um mundo cada vez mais interconectado (REIS; NAVES, 2020).

3 O PAPEL DAS LEGISLAÇÕES INTERNACIONAIS NA PROTEÇÃO DA PRIVACIDADE DIGITAL

A harmonização das legislações internacionais de proteção de dados pessoais diante da globalização digital demonstra a necessidade de regulamentações eficazes devido à coleta, armazenamento e comercialização transfronteiriça dessas informações.

Nessa perspectiva, o papel central das normas constantes da *General Data Protection Regulation* (GDPR) da União Europeia serviu de influência na formulação de outras legislações, como a Lei Geral de Proteção de Dados (LGPD) no Brasil.

As convergências entre essas legislações, precisamente suas relevâncias para mitigar riscos à privacidade digital, ainda que existam diferenças normativas, são de importância salutar à cooperação internacional para enfrentar os desafios complexos do mercado global de dados, que é caracterizado por uma dinâmica acelerada e constante inovação tecnológica.

3.1 A GDPR E SUA INFLUÊNCIA NA LGPD

A *General Data ProtectionRegulation* (GDPR), em vigor desde 2018, constitui um referencial normativo internacional na proteção de dados pessoais, estabelecendo um padrão global para a privacidade digital (CASTELLS, 2003).

Surgiu como resposta às crescentes preocupações sobre o uso indiscriminado e abusivo de informações no âmbito de um contexto digital globalizado, buscando garantir que os indivíduos tenham maior controle sobre suas informações pessoais e maior transparência das empresas no tratamento desses dados (SOLOVE, 2004; ZUBOFF, 2019).

Uma das características fundamentais da GDPR é sua aplicação extraterritorial, o que significa que qualquer organização, independentemente de sua localização, que trate dados de cidadãos da União Europeia deve cumprir suas normas (art. 3º) (COSTA; MELLO, 2021). Isso provocou um impacto global imediato, pois muitas empresas fora da UE tiveram que ajustar suas práticas para continuar acessando o mercado europeu.

Outro ponto de destaque da GDPR são as multas rigorosas aplicadas em caso de descumprimento, que podem chegar a 20 milhões de euros ou 4% do faturamento global da empresa (art. 83), incentivando as organizações a adotarem uma postura proativa em relação à proteção de dados (MOLINARO; RUARO, 2019).

Além disso, a GDPR introduziu conceitos como “proteção por design” e “proteção por padrão” (art. 25), que exigem a incorporação da segurança e da privacidade desde a concepção de sistemas, produtos e serviços, assegurando que a proteção de dados não seja um aspecto posterior ou acessório (FINKELSTEIN; FINKELSTEIN, 2019).

Inspirada pela GDPR, a Lei Geral de Proteção de Dados (LGPD) do Brasil, sancionada em 2018, adotou muitos desses princípios, mas com adaptações específicas para o contexto nacional. Uma dessas adaptações é a consideração do impacto socioeconômico do Brasil, especialmente em relação à desigualdade digital e à capacidade das micro e pequenas empresas de se adequarem às exigências regulatórias.

Para isso, a LGPD prevê tratamento diferenciado e simplificado para essas organizações (art. 55-J), permitindo que o arcabouço regulatório seja rigoroso, porém factível para um mercado diversificado (COELHO, 2023).

Outro elemento fundamental da LGPD é a criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão regulador responsável por fiscalizar a aplicação da lei, orientar as empresas e promover a educação em proteção de dados no país (art. 55-A).

Apesar de ainda estar em processo de consolidação estrutural, a ANPD representa um avanço importante na governança da privacidade no Brasil, criando um canal institucionalizado para a supervisão e aplicação das normas, algo até então inexistente (CARVALHO; PEDRINI, 2019).

Sobretudo, a LGPD concedeu um prazo mais dilatado para que as organizações brasileiras se adaptassem às suas normas, considerando os desafios específicos do país, como o acesso desigual à tecnologia, a baixa maturidade digital de diversos setores e a necessidade de conscientização da população sobre seus direitos digitais (BOFF; FORTES, 2014).

Essa flexibilização temporal visa garantir uma transição mais suave, evitando impactos

econômicos negativos e facilitando a adequação técnica e operacional das empresas.

Apesar dessas adaptações, o alinhamento da LGPD com a GDPR demonstra a importância da harmonização internacional das legislações de proteção de dados, especialmente diante do fluxo global de informações que ultrapassa fronteiras e envolve múltiplos agentes econômicos.

Essa convergência normativa não só protege os direitos dos titulares de dados, mas também fortalece a posição do Brasil no mercado internacional, assegurando que as empresas brasileiras possam operar com conformidade e competitividade perante parceiros e clientes estrangeiros (MATOS, 2005).

Entretanto, desafios persistem, porquanto a efetividade da LGPD depende não só da existência da lei e da ANPD, mas também da capacitação das empresas para implementar medidas técnicas e administrativas adequadas, da fiscalização rigorosa para punir infrações e da conscientização dos titulares sobre seus direitos (SILVEIRA, 2024).

Só assim será possível construir um ambiente digital mais seguro, transparente e respeitoso à privacidade, fundamental para a confiança e o desenvolvimento sustentável da economia digital no Brasil (REIS; NAVES, 2020).

3.2 A CONVERGÊNCIA INTERNACIONAL NA PROTEÇÃO DE DADOS

A intensificação da digitalização das relações sociais, econômicas e políticas impôs novos desafios à garantia da privacidade e à gestão de dados pessoais. Em resposta a esse cenário, emergem legislações como a General Data Protection Regulation (GDPR), da União Europeia, e a Lei Geral de Proteção de Dados (LGPD), do Brasil, que buscam garantir maior controle dos cidadãos sobre suas informações pessoais.

Ambas as normas representam um esforço relevante de regulamentação da privacidade em meio à expansão do uso de tecnologias de rastreamento, coleta e processamento de dados.

Contudo, a harmonização global ainda enfrenta importantes entraves de ordem normativa, cultural e institucional.

A GDPR, em vigor desde 2018, consolidou-se como um marco regulatório internacional por estabelecer princípios robustos de proteção de dados, com destaque para a responsabilização das empresas, a transparência no tratamento das informações e a consagração de direitos específicos aos titulares dos dados.

A sua aplicação extraterritorial (art. 3º), bem como as severas sanções previstas em caso de descumprimento (art. 83), obrigaram empresas de todo o mundo a reverem suas políticas de privacidade, promovendo uma mudança de paradigma no modo como os dados são tratados no ambiente digital (COSTA; MELLO, 2021).

Inspirando-se nesse modelo, o Brasil sancionou a LGPD em 2018, adotando muitos dos princípios da GDPR, mas também os adaptando à sua realidade socioeconômica.

Entre as principais adaptações, destaca-se a criação da Autoridade Nacional de Proteção de Dados (ANPD), encarregada de fiscalizar e orientar a aplicação da lei, bem como o tratamento diferenciado concedido à micro e pequenas empresas (art. 55-J).

A LGPD também estabeleceu obrigações como o consentimento expresso para tratamento de dados, a necessidade de justificar a finalidade do uso das informações e a possibilidade de revogação do consentimento pelo titular (CARVALHO; PEDRINI, 2019).

Entretanto, apesar dessas semelhanças normativas, ainda existem desafios significativos à harmonização global. A fragmentação normativa entre países cria obstáculos operacionais para empresas multinacionais, que precisam se adequar a exigências específicas de cada jurisdição.

Conforme observam Martínez, Damasceno e Macedo (2019), essa diversidade legal demanda altos custos de *compliance* e dificulta a uniformidade de práticas internacionais de proteção

de dados. Além disso, a fiscalização em países em desenvolvimento, como o Brasil, ainda é incipiente, o que reduz a efetividade da legislação. A ANPD, embora importante, ainda carece de estrutura consolidada e autonomia plena para exercer sua função de forma eficaz (BOFF; FORTES, 2014).

Outro fator que agrava essa complexidade é a divergência cultural e política na compreensão da privacidade. Enquanto em países europeus a proteção de dados é vista como um direito fundamental inviolável, em outras regiões, como os Estados Unidos, prevalece uma visão mais voltada à regulação pelo mercado.

No Brasil, ainda se verifica um processo em construção sobre a valorização da privacidade como direito essencial, o que impacta diretamente na implementação e fiscalização da LGPD (SILVEIRA, 2024).

Nesse contexto, como destacam Costa e Mello (2021), “a proteção de dados pessoais é um desafio transnacional, que exige um equilíbrio entre regulamentações locais e a necessidade de uma governança global robusta”.

Para enfrentar esses obstáculos, torna-se necessária a articulação de esforços multilaterais por meio de acordos internacionais, fóruns regulatórios e políticas de interoperabilidade entre legislações. Essas iniciativas não apenas facilitam a conformidade regulatória, mas também promovem a construção de um ambiente digital seguro e colaborativo, no qual a proteção dos dados seja respeitada independentemente da jurisdição.

O fortalecimento da cooperação entre autoridades de proteção de dados também contribui para a uniformização de práticas, compartilhamento de boas experiências e maior efetividade no combate a abusos.

Todavia, a convergência normativa entre GDPR e LGPD tem gerado impactos positivos significativos. Ao alinhar-se com os padrões europeus, o Brasil reforça sua credibilidade no

cenário internacional, estabelecendo-se como um parceiro confiável para negócios digitais e atraindo investimentos. Essa harmonização não apenas eleva o nível de proteção dos dados, mas também favorece o comércio internacional, a transferência de tecnologia e o desenvolvimento de soluções inovadoras baseadas em princípios éticos e sustentáveis (FINKELSTEIN; FINKELSTEIN, 2019).

Entretanto, essa convergência também impõe novas responsabilidades às empresas e ao Estado. As organizações precisam investir em infraestrutura, políticas internas de governança de dados e capacitação de suas equipes, ao mesmo tempo em que o poder público deve garantir a efetiva aplicação das normas e a proteção dos direitos dos titulares.

Como enfatiza Zuboff (2019), “em uma economia digital guiada pelo poder de dados, a transparência e a responsabilidade corporativa são pré-requisitos indispensáveis para preservar a confiança pública”.

Dessa forma, constata-se que a harmonização legislativa na proteção de dados pessoais é um processo complexo, que exige mais do que a replicação de normas internacionais.

Requer, sobretudo, uma articulação entre instituições sólidas, cultura de privacidade, cooperação transnacional e participação ativa dos cidadãos. É importante que empresas e indivíduos compreendam que o tratamento adequado dos dados é não apenas uma obrigação legal, mas um pilar ético de respeito à dignidade humana.

Ao integrar-se aos princípios globais de proteção de dados, o Brasil não apenas assegura os direitos de seus cidadãos, mas também contribui para a construção de um ecossistema digital mais justo, transparente e seguro em escala global.

4 CONCLUSÃO

A análise realizada ao longo deste estudo evidencia a crescente complexidade que envolve a proteção da privacidade na era digital, especialmente diante do avanço tecnológico e da

monetização dos dados pessoais.

A sociedade conectada tornou os dados um ativo importante, levando empresas e plataformas digitais a desenvolverem modelos de negócio centrados na coleta, tratamento e comercialização dessas informações. Nesse contexto, a privacidade deixa de ser apenas uma questão individual e passa a representar um desafio coletivo que demanda regulamentações eficazes, fiscalização ativa e conscientização da população.

A LGPD, em diálogo com a GDPR europeia, surge como um marco importante para garantir direitos e responsabilizar os agentes que manipulam dados pessoais. Contudo, apesar dos avanços legais, ainda se observa a existência de lacunas na efetividade da proteção, especialmente no que se refere à educação digital da população e à capacidade do Estado em aplicar sanções às empresas infratoras.

A democratização das redes sociais e a exposição excessiva de informações sensíveis agravam essa problemática, exigindo uma postura combativa e vigilante por parte de todos os atores envolvidos.

Diante disso, é relevante fortalecer a cultura da privacidade por meio de políticas públicas, estratégias educativas e desenvolvimento de tecnologias que assegurem a autodeterminação informacional do cidadão.

A proteção dos dados pessoais não deve ser tratada como um obstáculo a ser superado pelas empresas, mas como um valor inegociável em uma sociedade que pretende ser mais democrática.

Assim, o compromisso com a ética digital e com os direitos fundamentais deve orientar a construção de um ambiente virtual mais seguro e respeitoso para todos.

REFERÊNCIAS

BOFF, Salete Oro; FORTES, Vinícius Borges. **A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental:** perspectivas de construção de um marco regulatório para o Brasil*. Sequência (Florianópolis),* v. 35, n. 68, p. 109–128, 2014. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2013v35n68p109. Acesso em: 27 maio 2025.

CARVALHO, Gisele Primo; PEDRINI, Tainá Fernanda. Direito à privacidade na lei geral de proteção de dados pessoais. ***Revista da ESMESC,*** v. 26, n. 32, p. 363–382, 2019.

CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 2003.

COELHO, Karolainy Vitória Ferreira. **A tutela constitucional à privacidade frente à Lei Geral de Proteção de Dados:** o impacto do uso indevido e da comercialização de dados pessoais na democratização das redes sociais. 2023.

COSTA, Eduardo; MELLO, Marina. LGPD e GDPR: semelhanças e diferenças. ***Revista Brasileira de Direito Digital,*** 2021.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e lei geral de proteção de dados pessoais. ***Revista de Direito Brasileira,*** v. 23, n. 9, p. 284–301, 2019.

GOMES, Giara Maria. **A coleta de dados pessoais pelas redes sociais digitais com impactos sobre a privacidade.** 2024.

GROPP, Maria Eduarda; MOTTA, Jefferson Holliver. **A mineração de dados e os direitos de personalidade dos consumidores:** análise da privacidade na era digital. *Governança e Direitos Fundamentais, p. 65.*

MARTÍNEZ, Gabriel Francisco Cevallos; DAMASCENO, HandhersonLeyltton Costa; MACEDO, Társio Roberto Lopes. Privacidade e redes digitais: a comercialização de dados no

ciberespaço. ***Revista e-Curriculum,*** v. 17, n. 3, p. 1393–1398, 2019. Disponível em: https://revistas.pucsp.br/curriculum/article/view/36859. Acesso em: 27 maio 2025.

MATOS, Tiago Farina. Comércio de dados pessoais, privacidade e Internet. ***Revista de Doutrina da 4ª Região,*** v. 18, n. 7, 2005.

MOLINARO, Carlos Alberto; RUARO, Regina Linden. **Fim da privacidade:** divulgação e negociação de dados pessoais. *EconomicAnalysisof Law Review,* v. 10, n. 3, 2019. Disponível em: https://portalrevistas.ucb.br/index.php/EALR/article/view/10456. Acesso em: 27 maio 2025.

REIS, Émilien Vilas Boas; NAVES, Bruno Torquato de Oliveira. **O meio ambiente digital e o direito à privacidade diante do Big Data.***Veredas do Direito,* v. 17, n. 37, p. 145–167, 2020. Disponível em: https://revista.domhelder.edu.br/index.php/veredas/article/view/1795. Acesso em: 27 maio 2025.

SILVEIRA, João Victor Pires. **Tutela jurídica dos dados pessoais:** sob o contexto da sociedade digital. 2024.

SILVEIRA, Sergio Amadeu *et al.* A privacidade e o mercado de dados pessoais. ***Liinc em Revista,*** v. 12, n. 2, 2016. Disponível em: https://www.revista.ibict.br/liinc/article/view/3719. Acesso em: 23 maio 2025.

SOLOVE, Daniel J. ***The digital person:****technologyandprivacy in theinformation age.* New York: NYU Press, 2004.

ZUBOFF, Shoshana. ***The age ofsurveillancecapitalism:*** *thefight for a human future atthe new frontierofpower*. New York: PublicAffairs, 2019.

[1] Graduando em Direito pela Faculdade Serra do Carmo – FASEC. E-mail: martins.daniel334@gmail.com.

[2] Professor na Faculdade Serra do Carmo – Fasec, da disciplina de Direito Tributário, Direito Administrativo e Prática Real e Simulada V, no curso de Bacharelado em Direito. Especialista em Direito Processual Civil, graduado em Direito pela Universidade Federal do Tocantins UFT/Palmas/TO. Servidor Público Federal da Seção Judiciária do Estado do Tocantins – Justiça Federal da 1ª Região. E-mail: jefferson.franco.silva@gmail.com.