Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v12i4.25623

PROTEÇÃO DE DADOS PESSOAIS NA ERA DIGITAL: UM ESTUDO COMPARATIVO ENTRE A LGPD BRASILEIRA E O GDPR EUROPEU

PERSONAL DATA PROTECTION IN THE DIGITAL AGE: A COMPARATIVE STUDY BETWEEN BRAZIL'S LGPD AND THE EUROPEAN GDPR

Gabriel Penna Firme de Melo[1]

RESUMO: O presente trabalho analisa como e em que medida as normas estabelecidas pela Lei Geral de Proteção de Dados (LGPD) no Brasil e pelo Regulamento Geral de Proteção de Dados (GDPR) na União Europeia efetivamente asseguram a proteção dos titulares de dados pessoais, avaliando também os custos de adequação e os obstáculos de *enforcement* em um cenário de "capitalismo de vigilância". O foco recai sobre a análise comparativa das bases legais, direitos dos titulares, obrigações das organizações e sanções previstas nos dois diplomas, bem como sobre as particularidades do contexto brasileiro frente à maturidade regulatória europeia. A pesquisa, de abordagem qualitativa e baseada em revisão bibliográfica e documental, demonstra que o GDPR se encontra em estágio mais consolidado de aplicação e fiscalização, ao passo que a LGPD ainda enfrenta desafios no fortalecimento institucional da Autoridade Nacional de Proteção de Dados (ANPD) e na difusão de uma cultura de *compliance*. Aponta-se, ainda, para a importância de harmonização normativa e de incentivos à inovação responsável, a fim de garantir a proteção efetiva de dados pessoais sem inviabilizar o desenvolvimento tecnológico. As conclusões reafirmam a necessidade de regulamentações complementares, fiscalização consistente e práticas organizacionais de governança de dados robustas, indicando caminhos para superar as limitações atuais e acompanhar a evolução contínua das tecnologias digitais.

Palavras-chave: LGPD. GDPR. Capitalismo de Vigilância. ANPD. Proteção Efetiva de Dados Pessoais. Governança de Dados.

ABSTRACT: This paper analyzes how - and to what extent - Brazil's General Data Protection Law (LGPD) and the European Union's General Data Protection Regulation (GDPR) safeguard personal data subjects. It assesses compliance costs and enforcement barriers within the landscape of "surveillance capitalism", comparing the statutes' legal bases, data-subject rights, organizational obligations, and sanctions. A qualitative methodology grounded in bibliographic and documentary review reveals that the GDPR benefits from greater regulatory maturity and consistent oversight, whereas the LGPD still contends with institutional strengthening of Brazil's National Data Protection Authority (ANPD) and the spread of a robust compliance culture. The study underscores the need for normative harmonization and incentives for responsible innovation to achieve effective personal data protection without hindering technological development. It concludes that supplementary regulations, sustained enforcement, and strong data-governance practices are essential to overcome current limitations and keep pace with evolving digital technologies.

Keywords: LGPD. GDPR. Surveillance Capitalism. ANPD. Effective Personal Data Protection. Data Governance.

[1]Mestre em Estudos Jurídicos com Ênfase em Direito Internacional, MUST University (EUA).

1 INTRODUÇÃO

A proteção de dados pessoais passou a ocupar posição estruturante no âmbito das relações jurídicas próprias da sociedade marcada pela ubiquidade tecnológica. Os dados passaram a integrar o núcleo operacional de modelos econômicos baseados em rastreamento sistemático, categorização comportamental e projeções estatísticas. As relações entre pessoas, organizações empresariais e instituições estatais reorganizaram-se em torno de circuitos informacionais de elevada densidade, cuja administração exige balizas normativas capazes de delimitar encargos, conferir previsibilidade às práticas de tratamento e assegurar a integridade dos direitos fundamentais.

No direito brasileiro, a salvaguarda de dados pessoais permaneceu, durante extenso período, dispersa em diplomas setoriais e em cláusulas gerais de tutela da personalidade. A edição da Lei nº 13.709/2018 instituiu regime jurídico de feição sistemática, fixando princípios orientadores, reconhecendo prerrogativas aos titulares e atribuindo deveres específicos aos agentes de tratamento, além de assimilar referências internacionais de governança e instituir instâncias voltadas à fiscalização e à responsabilização.

A presença de disciplina normativa abrangente não conduz, por si, à efetivação integral das garantias previstas. A realização concreta da LGPD mostra-se condicionada por fatores institucionais, econômicos e culturais que incidem sobre sua implementação, entre os quais figuram a capacidade regulatória do Estado, o grau de internalização organizacional de práticas de governança informacional e os dispêndios inerentes aos processos de adequação. A análise comparativa entre o regime europeu e a disciplina brasileira evidencia proximidades estruturais, ao lado de diferenças relevantes relacionadas ao detalhamento das obrigações, à intensidade dos mecanismos de supervisão e ao grau de sedimentação das práticas de conformidade.

A presente pesquisa desenvolve um exame comparativo entre a LGPD e o GDPR, contemplando princípios orientadores, direitos assegurados aos titulares, deveres atribuídos aos agentes de tratamento e modelos institucionais de supervisão. Busca-se aferir o desempenho desses regimes na salvaguarda das informações pessoais e identificar obstáculos observados na implementação brasileira, com atenção aos impactos econômicos e institucionais sobre organizações, aos custos de conformidade e às estratégias adotadas no ambiente concorrencial.

2 A PRIVACIDADE COMO DIREITO FUNDAMENTAL

A análise comparativa entre a LGPD e o GDPR pressupõe o exame das matrizes históricas e conceituais que informam a construção jurídica da privacidade e, posteriormente, da proteção de dados pessoais. No cenário internacional, instrumentos como a Convenção Europeia de Direitos Humanos (1950) e a Convenção 108 do Conselho da Europa (1981) contribuíram decisivamente para o reconhecimento da privacidade como direito humano dotado de densidade normativa própria. No direito brasileiro, a Constituição Federal de 1988, ao assegurar a inviolabilidade da intimidade e da vida privada, e o Marco Civil da Internet (Lei nº 12.965/2014), ao estabelecer parâmetros para o uso da rede, fornecem o substrato jurídico que sustenta a Lei Geral de Proteção de Dados, cuja conformação revela nítida aproximação com o modelo europeu (Lugati; Almeida, 2020).

A evolução da proteção de dados pessoais evidencia um alargamento progressivo de sua significação jurídica. A privacidade, inicialmente concebida como esfera de resguardo contra ingerências externas, passa a incorporar a ideia de domínio sobre os próprios fluxos informacionais, traduzida na noção de autodeterminação informativa (Doneda, 2019). Tal desenvolvimento acompanha a consolidação de práticas econômicas fundadas na exploração sistemática de dados, fenômeno designado como "capitalismo de vigilância", marcado pela coleta extensiva de informações orientada a finalidades preditivas e comerciais (Zuboff, 2021). Nesse horizonte histórico-normativo inscrevem-se o GDPR (2016) e a LGPD (2018), diplomas que afirmam a proteção jurídica da privacidade e ampliam o espectro de controle individual sobre os dados pessoais (Neves, 2021).

Na tentativa de equilibrar inovação tecnológica, circulação informacional e tutela de direitos fundamentais, o GDPR tornou-se referência regulatória global, influenciando legislações subsequentes, entre elas a LGPD (Magalhães, 2021; Fernandes; Nuzzi, 2022). Todavia, o cenário internacional não é homogêneo. Modelos como o *California Consumer Privacy Act* e a legislação chinesa apresentam diferenças relevantes quanto ao escopo, aos mecanismos de *enforcement* e ao papel estatal. Essa diversidade regulatória impõe desafios à harmonização normativa e às organizações que operam em múltiplas jurisdições, motivando instrumentos como Cláusulas Contratuais Padrão e acordos de adequação, ainda insuficientes para uma uniformização plena (Neves, 2022).

No direito europeu, a proteção de dados pessoais possui posição jurídica autonomamente afirmada, expressa na Carta dos Direitos Fundamentais da União Europeia (União Europeia,

2012, art. 8º). Tal consagração encontra correspondência em estruturas regulatórias estáveis, cuja atuação coordenada densifica a eficácia prática do direito reconhecido (Neves, 2021; Lorenzon, 2021). No Brasil, a Constituição de 1988 já assegurava a inviolabilidade da intimidade e da vida privada (Brasil, 1988, art. 5º, X), porém a identificação explícita da proteção de dados como direito fundamental apenas se formalizou com a Emenda Constitucional nº 115/2022, que a inseriu de modo expresso no sistema constitucional, em harmonia com orientação jurisprudencial gradualmente afirmada pelo Supremo Tribunal Federal (Bioni; Martins, 2022; Supremo Tribunal Federal, 2022).

Constata-se convergência entre Brasil e União Europeia quanto ao reconhecimento da proteção de dados como dimensão inerente à dignidade, à liberdade e ao desenvolvimento da pessoa. O sistema europeu opera com aparato regulatório consolidado, ao passo que o ordenamento brasileiro atravessa fase de institucionalização progressiva, tendo incorporado formalmente a proteção de dados ao catálogo de direitos fundamentais, embora ainda se depare com obstáculos atinentes à plena eficácia normativa.

2.1 Teorias e discussões contemporâneas (capitalismo de vigilância, *big data*, IA)

A formulação do denominado "capitalismo de vigilância" (Zuboff, 2021) evidencia a centralidade econômica adquirida pela coleta e pela análise massiva de dados, cuja exploração se converte em fonte de lucros expressivos, ao mesmo tempo em que projeta tensões sobre a esfera da privacidade e sobre a autonomia individual. A disseminação de algoritmos de IA e de instrumentos de *big data* amplia a capacidade de antecipação de condutas e intensifica a possibilidade de interferências indevidas, inclusive sob a forma de manipulação e discriminação informacional (Fornasier; Knebel, 2021). Conforme Almeida e Soares (2022), modelos empresariais estruturados pela mercantilização de dados reclamam tratamento regulatório atento às particularidades de mercados globalizados.

Fornasier e Knebel (2021) registram, em estudos recentes, a consolidação de arranjos econômicos nos quais a vigilância sistemática assume estatuto de base operacional de poder e de rentabilidade. Tal configuração adquire maior densidade com a incorporação de algoritmos de inteligência artificial e de ferramentas de big data, aptas a reconhecer padrões comportamentais e a projetar preferências de consumo ou formas de interação social.

Além disso, essa dinâmica tecnológica impõe uma tensão entre o impulso inovador e a necessidade de proteção dos direitos fundamentais. O modelo de capitalismo de vigilância

evidencia como a comercialização dos dados pode levar à exploração e à perda de controle dos indivíduos sobre suas informações pessoais, o que exige uma resposta normativa robusta. Por exemplo, Zuboff (2021) argumenta que o uso indiscriminado dos dados transforma informações pessoais em *commodities* e cria condições para a manipulação comportamental e erosão da autonomia individual.

Por outro lado, o uso responsável de IA e *big data* pode impulsionar avanços tecnológicos e otimizar processos. Masseno *et al.* (2020) enfatizam a importância de medidas de segurança robustas para mitigar violações em um cenário de rápida evolução tecnológica. Nessa mesma linha, Chou *et al.* (2024) propõem *frameworks* como a ISO 27701 para padronizar práticas de privacidade, servindo de guia para organizações que buscam adequar-se tanto às exigências do GDPR quanto da LGPD.

Assim, as teorias contemporâneas evidenciam uma tensão central: de um lado, há o imperativo de tutelar a privacidade e garantir direitos fundamentais, enquanto, de outro, existe a necessidade de promover a inovação e o crescimento econômico em um ambiente de fluxos de dados intensos. A LGPD e o GDPR representam tentativas de equilibrar esses interesses, mas enfrentam desafios de implementação, *enforcement* e adaptação cultural que demandam análises contínuas e abordagens regulatórias articuladas entre países.

2.2 Análise Econômica do Direito como ferramenta para avaliar a regulação de proteção de dados

Para além da leitura dogmática e da análise de princípios, a avaliação da eficácia da LGPD e do GDPR adquire maior densidade quando observada sob a lente da Análise Econômica do Direito (AED), perspectiva que investiga os efeitos econômicos e sociais decorrentes da aplicação dessas legislações e examina de que modo organizações administram os dispêndios de adequação normativa em relação às exigências de competitividade no ambiente digital (Feiler *et al.*, 2024).

Conforme assinalam Feiler *et al.* (2024), essa perspectiva destaca a necessidade de ponderação entre os custos de conformidade e os ganhos associados à proteção de direitos, à segurança jurídica e à confiança institucional. A implementação da LGPD e do GDPR impõe encargos significativos às organizações, e a transposição irrefletida de modelos normativos estrangeiros, desatenta às especificidades do contexto brasileiro, pode acarretar restrições indesejadas à inovação (Canaan, 2022).

A AED também analisa os incentivos gerados pela regulação. Obrigações de transparência, segurança e governança, bem como sanções e fiscalização previstas na LGPD e no GDPR, buscam induzir práticas de tratamento de dados seguras e éticas. A efetividade desses mecanismos depende da consistência do *enforcement*, como o realizado pela ANPD no Brasil, ainda em consolidação, permitindo avaliar se sanções e fiscalização realmente promovem conformidade (Magalhães, 2021).

3 INFLUÊNCIA EUROPEIA NA LEGISLAÇÃO BRASILEIRA

A elaboração da Lei Geral de Proteção de Dados (LGPD) revela uma forte influência das normativas europeias, em especial do Regulamento Geral de Proteção de Dados (GDPR). Essa influência manifesta-se na reprodução de dispositivos legais e princípios e também na forma como se estimula ou se restringe a inovação no país. Conforme argumenta Canaan (2021), a importação "acrítica" do modelo europeu para o contexto brasileiro traz benefícios e desafios, ampliando simultaneamente o leque de direitos dos titulares de dados e o ambiente de competitividade, gerando insegurança jurídica que pode inibir a inovação local.

Segundo Derbli (2019), a LGPD representa uma tradução do GDPR para o contexto brasileiro. Contudo, há diferenças, como a criação do Encarregado de Proteção de Dados (EPD) em vez do DPO europeu e sanções menos rigorosas (Magalhães, 2021), refletindo adaptações locais, embora persistam riscos de inconsistências normativas.

A replicação do GDPR na LGPD reflete a hegemonia eurocêntrica sobre países do Terceiro Mundo. Canaan (2021) aponta que essa transposição não é neutra, incorporando valores europeus, como portabilidade e *privacy by design*, muitas vezes sem adaptação local. A influência combina emulação - o modelo europeu como referência - e coerção indireta, como o *Brussels effect*, que condiciona o acesso ao mercado internacional ao cumprimento das normas da UE.

Todavia, esse transplante jurídico não se resume a meras cópias normativas. Derbli (2019) salienta que a LGPD, apesar de inspirada no GDPR, adapta certos pontos para o contexto brasileiro, a exemplo das sanções e da disciplina do encarregado de dados. Ademais, a LGPD introduz bases legais adicionais para tratamento, voltadas à execução de políticas públicas e à proteção da saúde, o que indica um ajuste à realidade nacional (Almeida; Soares, 2022).

A incorporação dos direitos e princípios do GDPR na LGPD trouxe avanços ao ambiente digital brasileiro. O estímulo à competitividade e à inovação é um exemplo, pois

dispositivos como o direito à portabilidade e ao esquecimento permitem aos titulares contestar monopólios de dados, criando espaço para que empreendedores desenvolvam novas soluções tecnológicas e ampliem a concorrência no mercado (Canaan, 2021). Essa abertura favorece diferenciação empresarial e, teoricamente, incentiva inovações compatíveis com as exigências regulatórias, conforme a "Porter Hypothesis" (Porter; van der Linde, 1995).

Também há de se considerar os desafios gerados aos monopólios de dados. Ao conferir aos indivíduos o poder de contestar grandes concentrações de dados, a legislação contribui para reduzir barreiras à entrada de novas empresas, o que pode favorecer o surgimento de startups e de tecnologias disruptivas. Concomitantemente, como demonstrado no estudo de Canaan (2022), o fortalecimento dos direitos dos titulares estimula modelos de negócio que se baseiam no uso responsável dos dados, reforçando a confiança dos consumidores na economia digital.

Há também o desestímulo ao desenvolvimento de soluções locais. A adoção do princípio de *privacy by design* sem a exigência de se considerar o "estado da arte" local pode levar os empresários a optarem por soluções já consolidadas no mercado internacional, em vez de desenvolverem tecnologias próprias que atendam às demandas específicas do Brasil (Canaan, 2021). Essa situação favorece, assim, as empresas europeias e amplia o fosso tecnológico entre as regiões, resultando na importação de pacotes prontos de *compliance* que não necessariamente dialogam com o contexto brasileiro (Magalhães, 2021).

Conclui-se que a influência do modelo europeu foi decisiva para a consolidação da proteção de dados no Brasil, ao oferecer parâmetros normativos consistentes e ampliar padrões de governança informacional. Contudo, a incorporação desse referencial exige adaptação às condições institucionais, econômicas e socioculturais brasileiras, sob pena de produzir desequilíbrios regulatórios e custos desproporcionais de conformidade.

4 ANÁLISE COMPARATIVA ENTRE LGPD E GDPR

Uma distinção inicial entre a LGPD e o GDPR manifesta-se no alcance territorial de cada diploma e nos critérios que orientam sua incidência. Ambos os regimes admitem a proteção de dados pessoais para além das fronteiras estatais em hipóteses determinadas (European Commission, 2025a; Bry Tecnologia, 2025); a forma de delinear tal projeção extraterritorial, entretanto, revela diferenças de concepção e de grau de detalhamento.

A LGPD incide sobre operações de tratamento realizadas por pessoas naturais ou jurídicas, de direito público ou privado, independentemente do suporte empregado ou do local

de armazenamento das informações. Sua aplicação verifica-se quando o tratamento ocorre em território nacional, quando há oferta de bens ou serviços a indivíduos localizados no país ou quando os dados pessoais se referem a pessoas situadas no Brasil (Belarmino *et al.*, 2024). A disciplina brasileira orienta-se, desse modo, para atividades vinculadas ao espaço econômico interno e para a proteção de titulares localizados no território nacional (Sarlet; Ruaro, 2021).

Quanto às exclusões, ambas as legislações apresentam similaridades: a LGPD não se aplica a tratamentos pessoais, jornalísticos, artísticos, acadêmicos, de segurança pública ou investigação criminal, enquanto o GDPR prevê exceções equivalentes para atividades domésticas, jornalísticas e de segurança pública (Serpro, 2025; GDPR-info.eu, 2025a). A LGPD, contudo, adiciona a nuance de isentar dados do exterior não compartilhados com agentes brasileiros, sem paralelo direto no GDPR.

A LGPD e o GDPR adotam definições amplas de dados pessoais e de operações de tratamento, assegurando proteção jurídica desde a coleta até a exclusão das informações, tanto em meio físico quanto digital (GDPR-info.eu, 2025a). A LGPD, embora inspirada em normas estrangeiras, possui características próprias adaptadas à realidade jurídica e institucional brasileira, enquanto a abordagem extraterritorial do GDPR é, em geral, mais clara e detalhada.

4.1 Bases Legais e Fundamentos

No GDPR, o consentimento livre, específico e informado é um dos pilares, complementado por bases como obrigação contratual, cumprimento de obrigação legal, proteção de interesses vitais, execução de tarefa de interesse público ou interesse legítimo do controlador (Bax *et al.*, 2020; Neves, 2021). A LGPD, por sua vez, adota uma estrutura comparável, estabelecendo múltiplas hipóteses de tratamento de dados que incluem o consentimento, cumprimento de obrigação legal ou regulatória, execução de contrato, exercício regular de direitos, proteção à vida ou incolumidade física, tutela da saúde, execução de políticas públicas, estudos por órgão de pesquisa, proteção do crédito, e interesse legítimo (Brasil, 2018).

Apesar das semelhanças, a LGPD, embora inspirada no GDPR, carece de regulamentações complementares claras, especialmente para operacionalizar certas disposições e definir algumas bases legais. Adicionalmente, o GDPR, com sua maior maturidade regulatória e um histórico de aplicação mais consolidado, consolidou mecanismos de verificação do legítimo interesse ou do interesse público que podem servir de parâmetro de comparação e aprendizado para o caso brasileiro (Feiler *et al.*, 2024).

4.2 Princípios Fundamentais

A Lei Geral de Proteção de Dados Pessoais enuncia um conjunto de princípios estruturantes destinados a orientar o tratamento de dados pessoais no Brasil, operando como parâmetro de legitimidade das práticas informacionais e como vetor de interpretação sistemática do regime jurídico instituído (Brasil, 2018). Tais princípios exprimem a proeminência adquirida, na experiência contemporânea, pela ética informacional, pela salvaguarda da dignidade humana e pela contenção do poder informacional exercido por agentes públicos e privados, em consonância com referências internacionais de governança de dados e em benefício da tutela jurídica dos titulares (GetPrivacy, 2025).

A LGPD consagra dez princípios fundamentais que delimitam juridicamente o tratamento de dados. A finalidade exige propósitos legítimos e previamente informados; a adequação impõe compatibilidade entre tratamento e contexto de coleta; e a necessidade consagra a proporcionalidade informacional, restringindo o tratamento ao mínimo indispensável.

No plano europeu, o GDPR estrutura o regime de proteção informacional a partir de princípios previstos no artigo 5º, que desempenham função equivalente de orientação normativa. O princípio da responsabilidade (*accountability*) atribui ao controlador o dever de demonstrar conformidade com o regulamento (GDPR.eu, 2025; ICO, 2025; European Commission, 2025a; Cloudian, 2025).

Apesar de diferenças terminológicas, há convergência material entre os regimes. Os princípios de finalidade, adequação e necessidade da LGPD correspondem funcionalmente à limitação da finalidade e à minimização de dados do GDPR. Livre acesso e transparência relacionam-se à exigência de tratamento lícito e transparente, enquanto qualidade dos dados aproxima-se do princípio da exatidão. Segurança e prevenção refletem a lógica de integridade e confidencialidade, e a responsabilização corresponde ao princípio de *accountability*. O GDPR explicita, ainda, a limitação temporal da conservação e a exigência de base legal para o tratamento. Essa aproximação normativa evidencia a difusão internacional de padrões de proteção de dados e a consolidação de parâmetros globais de governança informacional (Canaan, 2022).

No que se refere aos direitos dos titulares, ambos os regimes estruturam a proteção informacional a partir da autodeterminação informativa. LGPD e GDPR asseguram direitos de acesso, retificação, exclusão e controle do tratamento, embora o regulamento europeu

apresente maior detalhamento procedimental, especialmente quanto ao direito ao esquecimento e à portabilidade. No Brasil, a efetividade desses direitos depende da regulamentação infralegal e da atuação institucional da ANPD, evidenciando desafios de implementação e cultura de conformidade (Masseno; Martins, 2020; Bioni; Silva, 2022).

A LGPD estabelece direitos como confirmação da existência de tratamento, acesso aos dados, correção de informações, anonimização, bloqueio ou eliminação de dados irregulares, portabilidade, eliminação de dados tratados com consentimento, informação sobre compartilhamento, revogação do consentimento, oposição ao tratamento, revisão de decisões automatizadas e petição à autoridade nacional (Brasil, 2018; TJSP, 2025).

O GDPR confere ao titular, denominado *data subject*, direitos previstos principalmente nos artigos 12 a 22, incluindo informação, acesso, retificação, apagamento, limitação do tratamento, portabilidade, oposição, proteção contra decisões automatizadas, retirada do consentimento e reclamação à autoridade supervisora (GDPR-info.eu, 2025b; European Data Protection Board, 2024).

Essa convergência entre princípios estruturantes e direitos subjetivos evidencia a natureza sistêmica da proteção de dados pessoais, articulando diretrizes normativas e prerrogativas individuais como mecanismos complementares de limitação do fluxo informacional. Tal estrutura assume relevância particular no contexto da circulação transfronteiriça de dados, elemento central da economia digital contemporânea e fundamento para o exame dos mecanismos jurídicos de cooperação e soberania regulatória.

4.3 Transferências Internacionais de Dados Pessoais

A circulação transfronteiriça de dados pessoais assume relevo particular na salvaguarda da privacidade e na dinâmica do comércio digital em escala global, encontrando disciplina tanto na LGPD quanto no GDPR. Conforme assinala Neves (2022), ambos os regimes normativos se orientam pela proteção do direito fundamental aos dados pessoais, embora o façam por meio de soluções jurídicas e arranjos regulatórios que refletem tradições institucionais e condições econômicas distintas.

Impõe-se distinguir a transferência internacional de dados, caracterizada pelo envio deliberado de informações a entidade situada em outro país, do simples trânsito de dados, hipótese em que as informações apenas percorrem infraestrutura localizada no exterior sem destinação intencional a terceiros (Neves, 2022). Tal diferenciação, amparada em precedentes

europeus, previne leituras excessivamente restritivas e evidencia que a circulação internacional de dados não produz, em todas as situações, idênticos efeitos jurídicos.

No GDPR, a transferência para países terceiros ou organismos internacionais segue um sistema em camadas: é permitida quando a Comissão Europeia reconhece que o país destinatário oferece proteção adequada (Art. 45), ou por meio de garantias alternativas, como cláusulas contratuais padrão, regras corporativas vinculantes, códigos de conduta ou certificações (Art. 46). Exceções específicas podem ser aplicadas (Art. 49), mas a transferência regular depende principalmente de decisões de adequação e garantias, que constituem os pilares do regime (Neves, 2022).

A LGPD adota mecanismos semelhantes aos do GDPR, listando no Art. 33 hipóteses legais para transferência, como consentimento do titular, cláusulas contratuais específicas, normas corporativas globais e selos ou certificados de adequação (Brasil, 2018), cabendo à ANPD decidir sobre a adequação de outros países. Diferentemente do GDPR, porém, a LGPD não define uma hierarquia clara entre essas hipóteses, o que pode gerar interpretações diversas e insegurança jurídica para os operadores de dados (Neves, 2022).

Em termos conclusivos, LGPD e GDPR convergem na tutela dos dados pessoais em operações de alcance internacional e preveem instrumentos jurídicos para aludida finalidade, embora revelem diferenças quanto à ordenação das bases legais aplicáveis às transferências e ao grau de consolidação de seus procedimentos de reconhecimento de adequação. A distinção rigorosa entre transferência e mero trânsito de dados, aliada a uma leitura normativa que preserve os direitos dos titulares sem instaurar entraves desproporcionais, permanece como questão sensível para a estabilidade jurídica e para a circulação regular das atividades econômicas em escala global.

4.4 Obrigações das Organizações e Responsabilidades

A LGPD e o GDPR atribuem aos agentes de tratamento de dados pessoais deveres materiais que se projetam sobre a segurança, a transparência e a responsabilização das práticas informacionais. Exige-se das organizações a adoção de medidas técnicas e arranjos organizacionais idôneos à salvaguarda dos dados, bem como a capacidade de evidenciar, de modo verificável, a observância das normas aplicáveis. A instituição de um encarregado, na LGPD, ou de um *Data Protection Officer* (DPO), no GDPR, revela afinidade funcional entre os

regimes, ainda que não coincidam quanto à obrigatoriedade, incumbindo a tal figura o acompanhamento sistemático da conformidade interna (Lorenzon, 2021).

A LGPD impõe aos agentes de tratamento de dados pessoais um conjunto de deveres orientados à conformidade normativa e à salvaguarda efetiva das informações. Entre as exigências mais expressivas figuram a adoção de medidas de segurança proporcionais aos riscos, o registro das operações de tratamento, a indicação de encarregado, a elaboração de planos de resposta a incidentes, a disciplina das transferências internacionais e a realização de avaliações internas de risco (Brasil, 2018; Serpro, 2025).

A legislação estabelece, ainda, a responsabilidade solidária do controlador e do operador pelos danos advindos do tratamento quando se verifique a inobservância de obrigações legais (Brasil, 2018). No âmbito europeu, o GDPR atribui a controladores e operadores um rol abrangente de encargos voltados à conformidade permanente. Entre eles sobressaem a incorporação da proteção de dados desde a concepção e por configuração padrão, a realização de avaliações de impacto em hipóteses de elevado risco, a manutenção de registros das atividades de tratamento, a designação de DPO, a comunicação de incidentes à autoridade competente e aos titulares, a previsão de cláusulas contratuais atinentes à confidencialidade e à responsabilidade, bem como a observância de requisitos específicos para transferências internacionais, fundados em decisões de adequação, cláusulas contratuais padrão ou salvaguardas adicionais (GDPR-info.eu, 2025b; European Data Protection Board, 2024). Tais prescrições orientam a responsabilização institucional, a publicidade das práticas informacionais e a integridade do tratamento ao longo de todo o percurso dos dados.

4.5 Sanções e Mecanismos de Fiscalização

A eficácia de um regime jurídico de proteção de dados vincula-se, em larga medida, à solidez de seus instrumentos de controle e à aptidão de suas sanções para produzir efeito dissuasório. A LGPD e o GDPR instituem autoridades supervisoras e cominam penalidades para hipóteses de descumprimento, ainda que o façam por arranjos institucionais e com repercussões distintas.

No ordenamento brasileiro, a fiscalização incumbe à Autoridade Nacional de Proteção de Dados, criada pela própria lei com a atribuição de zelar pela observância das normas, expedir diretrizes, acompanhar práticas e exercer poder sancionador (Brasil, 2018). À ANPD são cometidas funções de natureza normativa, fiscalizatória e punitiva.

As sanções destinam-se a induzir padrões de conformidade e a refrear expedientes abusivos no manejo de dados pessoais. Facultou-se, ademais, aos titulares a apresentação de reclamações diretamente à ANPD quando não atendidas as suas pretensões, o que densifica uma atuação simultaneamente reativa e preventiva por parte da autoridade (ANPD, 2023a). A despeito do desenho normativo, a efetividade institucional ainda encontra entraves de ordem orçamentária e organizacional. A inexistência de autonomia plena, somada à carência de quadro próprio de servidores, restringe a amplitude e a celeridade da fiscalização diante da complexidade do ambiente digital brasileiro (Bezerra, 2019; Acioly et al., 2024).

No espaço europeu, a supervisão incumbe a autoridades nacionais independentes em cada Estado-Membro, as chamadas Data Protection Authorities (DPAs). O GDPR resguarda a independência funcional desses órgãos e impõe que disponham de meios humanos, técnicos e financeiros aptos ao exercício de suas atribuições (Art. 52, European Union, 2016). Ao Comitê Europeu de Proteção de Dados (EDPB) cabe a coordenação entre as autoridades, com vistas à convergência interpretativa e à cooperação transnacional (European Data Protection Board, 2024).

O regime sancionatório do GDPR apresenta severidade graduada conforme a natureza da infração e a capacidade econômica do agente, aferida a partir do faturamento anual global. Violações de menor gravidade, a exemplo do descumprimento de deveres formais, podem ensejar multas de até 10 milhões de euros ou 2% do faturamento anual, prevalecendo o montante superior. Infrações de maior relevo, atinentes a princípios estruturantes, direitos dos titulares ou transferências internacionais, admitem penalidades de até 20 milhões de euros ou 4% do faturamento anual global (GDPR-info.eu, 2025c).

Ambos os regimes estabelecem autoridades nacionais de supervisão com competências fiscalizatórias e sancionatórias e mecanismos para reclamações de titulares. Contudo, o arranjo europeu apresenta maior densidade institucional e histórico consolidado de aplicação, aliado a sanções calculadas sobre o faturamento global, ampliando seu efeito dissuasório e promovendo uniformidade na conformidade internacional (Magalhães, 2021; Feiler *et al.*, 2024).

No contexto brasileiro, embora o sistema sancionatório possua instrumentos relevantes de responsabilização, sua efetividade encontra-se condicionada ao processo ainda em curso de consolidação institucional da autoridade nacional e à progressiva sedimentação de práticas de fiscalização (Bezerra, 2019; Acioly *et al.*, 2024).

Apesar da convergência normativa, persistem diferenças significativas na capacidade de enforcement e na previsibilidade regulatória. A proteção de dados no Brasil dependerá do fortalecimento técnico e institucional da supervisão, da estabilidade interpretativa das normas e do amadurecimento da governança informacional, sendo sua efetividade vinculada à capacidade de transformar princípios em práticas regulatórias consistentes e confiáveis.

4.6 Desafios de implementação

Não obstante as afinidades conceituais e a convergência teleológica entre a LGPD e o GDPR, a efetivação do regime brasileiro de proteção de dados evidencia entraves de ordem prática. Sobressai, entre eles, o custo de adequação regulatória, cujo peso recai com maior intensidade sobre pequenas e médias empresas, muitas vezes desprovidas de meios financeiros e técnicos aptos a reordenar processos e sistemas organizacionais (Neves, 2023).

A esse quadro agrega-se a limitada disponibilidade de profissionais especializados em proteção de dados, segurança da informação e direito digital, circunstância que restringe a implementação consistente das exigências legais, sobretudo em domínios marcados por elevada complexidade informacional, a exemplo dos setores de saúde e tecnologia (Saldaña, 2019).

A efetividade normativa também se vê condicionada por fatores organizacionais e regulatórios mais amplos. A ausência de uma cultura institucional orientada à proteção da privacidade compromete a internalização dos deveres legais, uma vez que a conformidade formal não se traduz, por si só, em práticas consistentes de governança informacional. Paralelamente, a insuficiência de regulamentação complementar e de orientações específicas para contextos setoriais complexos contribui para a persistência de incertezas interpretativas e dificuldades operacionais na aplicação da lei. Esse quadro é agravado pela velocidade das transformações tecnológicas, que continuamente introduzem novas formas de tratamento de dados e desafiam a capacidade adaptativa das estruturas regulatórias existentes (Almeida; Soares, 2022).

A eficácia da tutela de dados pessoais no Brasil vincula-se à aptidão institucional para fiscalizar e sancionar. A ANPD, ainda em fase de consolidação, convive com limitações de ordem estrutural e operacional que repercutem no *enforcement* e na previsibilidade regulatória, em contraste com a experiência europeia, o que repercute na percepção de risco e nos incentivos à conformidade (Bezerra, 2019; Magalhães, 2021; Oliveira et al., 2025).

Este quadro indica a conveniência de ajustes normativos contínuos, acompanhados de investimentos consistentes em infraestrutura tecnológica, qualificação técnica e difusão de uma cultura de *compliance*. A superação dessas restrições reclama atuação concertada entre poder público, setor privado e sociedade, a fim de assegurar tutela efetiva dos dados pessoais no país, em sintonia com parâmetros internacionais representados pelo GDPR.

5 EFETIVIDADE REGULATÓRIA DA LGPD E DO GDPR: IMPACTOS, TENDÊNCIAS TECNOLÓGICAS E PERSPECTIVA ECONÔMICO-JURÍDICA

A desconformidade com regimes de proteção de dados, notadamente LGPD e GDPR, irradia efeitos que vão além da imposição de multas. Incidentes envolvendo dados pessoais costumam acarretar abalos reputacionais de grande monta e perdas financeiras significativas, ao mesmo tempo em que ampliam a exposição a responsabilidades civis e regulatórias, o que recomenda a instituição de densos arranjos de *compliance* (Neves, 2021). Entre as repercussões práticas, observam-se efeitos mediatos, como a rarefação da confiança do consumidor e a redução da competitividade empresarial. A experiência europeia revela que a aplicação reiterada de sanções, associada a políticas de transparência, opera como fator dissuasório e favorece a conformação de culturas organizacionais orientadas à proteção de dados.

No Brasil, ocorrências de vazamento em esferas públicas e privadas, inclusive em domínios sensíveis como serviços financeiros e telecomunicações, tornam visíveis fragilidades estruturais e limites de resposta institucional tempestiva, o que recomenda medidas preventivas e corretivas dotadas de efetividade (Neves, 2023). Tais episódios indicam que a tutela de dados reclama não apenas previsão normativa, mas também capacidade operacional para prevenir, detectar e reagir a incidentes.

O avanço de tecnologias, como a IA e o *big data* intensifica desafios regulatórios. A utilização massiva de dados para modelagem preditiva e formação de perfis pode reproduzir vieses e gerar discriminação algorítmica, ampliando riscos à igualdade e à autonomia individual (De Lucca *et al.*, 2023). A crescente opacidade de sistemas automatizados dificulta a compreensão das decisões baseadas em algoritmos, tensionando o direito à explicação previsto na LGPD (art. 20) e no GDPR (arts. 15(1)(h) e 22(3)). Embora tais dispositivos reconheçam o controle do titular sobre decisões automatizadas, sua efetividade enfrenta limites técnicos e comerciais.

Nesse quadro, instrumentos de governança, de natureza técnica e normativa, passam a ocupar posição de relevo. A incorporação de referenciais internacionais, a exemplo da ISO

27701, favorece a conformação das rotinas organizacionais às exigências jurídicas e robustece os dispositivos de segurança informacional (Chou *et al*., 2024). Experiências europeias de auditoria algorítmica e a formulação de matrizes de explicabilidade revelam um movimento de progressiva institucionalização de controles técnicos dirigidos a sistemas automatizados (European Data Protection Board, 2024). A regulação contemporânea orienta-se, por essa via, à harmonização entre o ímpeto inovador das tecnologias e a salvaguarda dos direitos fundamentais.

A natureza transnacional dos fluxos de dados impõe desafios adicionais de harmonização normativa. A circulação global de informações exige instrumentos jurídicos capazes de compatibilizar regimes distintos e assegurar níveis adequados de proteção (Pinho; Cavalcante, 2024). Apesar de esforços de padronização, como as *Standard Contractual Clauses* da União Europeia, persistem lacunas relevantes na construção de um sistema internacional uniforme de proteção de dados (Magalhães, 2021). A influência normativa europeia, frequentemente descrita como *Brussels effect*, demonstra a capacidade difusora do GDPR, mas também evidencia desafios de adaptação local e fragmentação regulatória.

Mecanismos como acordos de adequação e cláusulas contratuais padronizadas desempenham papel relevante na viabilização de transferências internacionais seguras, embora a ausência de harmonização plena ainda gere incerteza jurídica (Fernandes; Nuzzi, 2022). Decisões como Schrems II ilustram os efeitos da fragmentação normativa e reforçam a necessidade de cooperação internacional e coordenação entre autoridades regulatórias (European Data Protection Board, 2024).

Além da dimensão jurídica e tecnológica, a efetividade dos regimes de proteção de dados possui relevante dimensão econômica. A AED demonstra que a conformidade regulatória envolve custos imediatos, mas tende a gerar benefícios de longo prazo ao fortalecer a confiança na economia digital e reduzir assimetrias informacionais. A adoção de padrões inspirados no GDPR pode estimular inovação orientada à segurança, embora também imponha custos que afetam de forma mais intensa pequenas e médias empresas (Canaan, 2022). Ao mesmo tempo, a convergência regulatória pode reduzir incertezas e atrair investimentos, desde que acompanhada de fiscalização consistente e previsível (Bioni; Martins, 2022).

A experiência europeia indica que instrumentos como avaliações de impacto, notificação de incidentes e designação de encarregados tornaram-se práticas organizacionais consolidadas, contribuindo para elevação dos padrões de segurança. Persistem, contudo,

desafios relacionados a custos regulatórios e diferenças interpretativas entre autoridades nacionais.

A comparação entre LGPD e GDPR revela diferenças de efetividade associadas à maturidade institucional, ao volume de precedentes e à consolidação da cultura regulatória. O regime europeu opera com estrutura mais consolidada de fiscalização, enquanto o modelo brasileiro encontra-se em processo de fortalecimento institucional e difusão cultural da proteção de dados. Apesar dessas diferenças, a LGPD representa avanço significativo ao alinhar o Brasil a padrões internacionais e instituir um sistema nacional de governança informacional.

A efetividade de tais regimes vincula-se, em última instância, à incorporação orgânica da proteção de dados no interior das estruturas organizacionais, ao adensamento institucional das autoridades reguladoras e à aptidão para responder às mutações tecnológicas. A sedimentação de uma cultura de compliance, conjugada à cooperação internacional e ao aperfeiçoamento de mecanismos técnicos de governança, apresenta-se como via idônea para resguardar, com densidade real, os direitos fundamentais na economia digital contemporânea.

5.1 Recomendações e propostas de melhorias

À vista dos desafios delineados, o fortalecimento da tutela de dados reclama iniciativas articuladas: o adensamento institucional da ANPD, a aproximação entre regimes normativos em escala internacional e a incorporação de práticas internas consistentes pelas organizações. Arranjos de governança, como comitês dedicados à proteção de dados, facultam o acompanhamento sistemático de processos, a detecção de vulnerabilidades e a pronta implementação de respostas a incidentes, o que favorece a aderência à LGPD e ao GDPR e fomenta uma cultura organizacional orientada à privacidade e à segurança. Programas permanentes de formação e sensibilização, a exemplo de *workshops* e certificações, consolidam este compromisso e contribuem para a redução de ocorrências de segurança (Almeida; Soares, 2022; Chou *et al.*, 2024).

A mensuração da eficácia das medidas de proteção de dados por meio de indicadores claros, como redução de incidentes, frequência de auditorias e rapidez na resposta a violações, é determinante para ajustar estratégias de compliance e demonstrar o retorno do investimento em governança (Feiler *et al.*, 2024). Paralelamente, a ampliação da autonomia e do orçamento da ANPD, associada à contratação de especialistas e à implementação de auditorias regulares em setores estratégicos, é fundamental para conferir maior efetividade à fiscalização e à

aplicação de sanções (Saldaña, 2019). O estabelecimento de parcerias com universidades e centros de pesquisa permite a elaboração de guias interpretativos e recomendações setoriais, fornecendo subsídios técnicos para decisões regulatórias mais consistentes.

No plano normativo, propõe-se a instituição de comissões intersetoriais incumbidas de acompanhar os efeitos das tecnologias emergentes e de sugerir revisões periódicas do arcabouço legal, de modo a preservar sua aderência às inovações associadas ao *big data* e à IA. A participação do Brasil em instâncias internacionais e em tratativas de adequação também se revela pertinente, uma vez que a aproximação de regimes jurídicos e o emprego de cláusulas contratuais padronizadas, como as *Standard Contractual Clauses*, favorecem a circulação segura de dados e a tutela dos direitos dos titulares (Fernandes; Nuzzi, 2022; Neves, 2022).

À vista das limitações econômicas e formativas, a instituição de incentivos fiscais e de subsídios destinados a pequenas e médias empresas que invistam em programas de compliance e em tecnologias de proteção de dados tende a atenuar obstáculos de ingresso, ampliar a adesão a práticas de governança e estimular a competitividade no ambiente digital (Canaan, 2022). Paralelamente, soluções tecnológicas podem contribuir para o monitoramento contínuo da conformidade e para o mapeamento de fragilidades, reduzindo encargos regulatórios e ampliando a eficácia das ações da ANPD (Fornasier; Knebel, 2021; Chou *et al.*, 2024).

O incentivo à pesquisa e ao desenvolvimento, por intermédio de iniciativas acadêmicas e de inovação, constitui vetor adicional de aperfeiçoamento. Investigações voltadas à efetividade de mecanismos de *enforcement*, aos impactos das tecnologias emergentes e a soluções operacionais de governança fornecem subsídios para futuras revisões normativas e para o aprimoramento de práticas institucionais. Tal movimento cumulativo favorece o amadurecimento institucional e a construção de uma proteção de dados mais consistente e ajustada às transformações tecnológicas em curso.

Em síntese, a implementação coordenada dessas diretrizes concorre para a conformação de um ambiente digital seguro, transparente e resiliente. Para além da mitigação de riscos associados a violações de dados, as providências descritas incentivam a inovação responsável e contribuem para a harmonização entre dinamismo econômico e tutela de direitos fundamentais. Conforme assinalam Feiler *et al.* (2024), esse equilíbrio figura entre os desafios mais exigentes das legislações de proteção de dados e, simultaneamente, sustenta as bases de uma economia digital confiável e duradoura.

6 CONSIDERAÇÕES FINAIS

O estudo analisou a LGPD e o GDPR para avaliar sua capacidade de proteger efetivamente os titulares de dados, tema crucial diante do capitalismo de vigilância, em que *big data* e IA ampliam riscos à privacidade e à dignidade humana. Embora compartilhem princípios como finalidade, necessidade, adequação, transparência, segurança e *accountability*, diferenças de contexto, maturidade institucional e consolidação de práticas de compliance influenciam decisivamente sua eficácia prática.

A comparação revelou que o GDPR se beneficia de uma trajetória histórica mais longa e de uma estrutura institucional robusta, composta por autoridades nacionais independentes e coordenadas pelo *European Data Protection Board*, capazes de aplicar sanções dissuasoras e uniformizar a fiscalização. Em contraponto, a LGPD, embora represente avanço significativo no ordenamento jurídico brasileiro, enfrenta desafios estruturais e contextuais: a ANPD ainda consolida sua autonomia e capacidade operacional, e práticas de governança e compliance no Brasil apresentam menor tradição, gerando processos de adequação mais complexos, especialmente para pequenas e médias empresas.

Quanto aos direitos dos titulares, embora semelhantes, o GDPR conta com orientações consolidadas e precedentes que aumentam sua efetividade, enquanto a LGPD ainda carece de regulamentação complementar e de disseminação de conhecimento, limitando seu impacto. Além disso, o avanço de IA e *big data* exige a aplicação de *privacy by design e by default*, bem como auditorias algorítmicas para mitigar vieses e garantir transparência em decisões automatizadas.

A experiência europeia demonstra a importância crítica da autonomia institucional das autoridades reguladoras, da previsibilidade normativa e da aplicação efetiva e dissuasora de sanções. Tais elementos, se incorporados no contexto brasileiro, podem acelerar a maturação do sistema nacional, permitindo que a LGPD alcance plenamente seu potencial transformador. Ao mesmo tempo, inovações como a obrigatoriedade de designação de encarregado de dados e o princípio da não discriminação revelam contribuições originais do legislador brasileiro ao debate global sobre proteção de dados.

Ao término, o estudo revela que a tutela dos dados pessoais ultrapassa a observância meramente formal de deveres normativos, configurando pressuposto para a resguarda da dignidade, da liberdade informacional e do exercício efetivo da cidadania em sociedades permeadas por tecnologias digitais. A sedimentação de práticas de *compliance*, o adensamento

institucional, a aproximação entre regimes jurídicos e a formação continuada dos diversos atores sociais apresentam-se como exigências permanentes para que LGPD e GDPR realizem, de modo íntegro, sua vocação protetiva.

A investigação igualmente assinala a conveniência de pesquisas empíricas e setoriais, aptas a aferir repercussões econômicas e sociais, examinar a consistência de práticas de governança e oferecer subsídios à formulação de políticas públicas. A trajetória histórica da proteção da privacidade permanece aberta, reclamando vigilância atenta, prudência ética e compromisso efetivo com a preservação dos direitos fundamentais na experiência contemporânea do mundo digital.

REFERÊNCIAS

ACIOLY, L. A.; SOUZA, P. H. D.; AMARAL, B. A. Governança de dados e autonomia institucional da ANPD: diagnóstico e perspectivas. *Cadernos de Regulação Digital*, 2024.

ALMEIDA, S. do C. D.; SOARES, T. A. Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital. *Perspectivas em Ciência da Informação*, v. 27, n. 3, p. 26–45, 2022. Disponível em: https://doi.org/10.1590/1981-5344/25905. Acesso em: 12 jan. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Painel de processos sancionatórios*. Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/painel-de-processos-sancionatorios. Acesso em: 12 jan. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *ANPD aplica a primeira multa por descumprimento à LGPD*. Brasília, 6 jul. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd. Acesso em: 12 jan. 2026.

BAX, M. P.; BARBOSA, J. L. S. *Proposta de mecanismo de consentimento na Lei Geral de Proteção a Dados – LGPD*. Belo Horizonte: ECI/PPGGOC, Universidade Federal de Minas Gerais, 2020.

BELARMINO, G. S.; RICARTE, D. R. D.; MOTTA, G. H. A Lei Geral de Proteção de Dados do Brasil à luz do Regimento Europeu: um exame comparativo e prospectivo através de uma revisão sistemática. In: WORKSHOP SOBRE AS IMPLICAÇÕES DA COMPUTAÇÃO NA SOCIEDADE (WICS), 5., 2024. *Anais...* p. 1–15, 2024.

BEZERRA, A. C. Autonomia e estrutura da ANPD no contexto do direito administrativo sancionador. *Revista Brasileira de Direito Público*, v. 16, n. 65, p. 89–112, 2019.

BIONI, B. R.; SILVA, P. G. F.; MARTINS, P. B. L. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. *Cadernos Técnicos da CGU: Coletânea de Artigos da Pós-graduação em*

Ouvidoria Pública, v. 1, 2022. Disponível em: https://ojs.cgu.gov.br/index.php/cadernostecnicos/article/view/692. Acesso em: 12 jan. 2026.

BRADFORD, A. *The Brussels effect: how the European Union rules the world*. Oxford: Oxford University Press, 2020. Disponível em: https://doi.org/10.1093/oso/9780190088583.001.0001. Acesso em: 12 jan. 2026.

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

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 jan. 2026.

BRY TECNOLOGIA. *A quem se aplica a LGPD:* entenda o escopo da lei. 2025. Disponível em: https://www.bry.com.br/blog/a-quem-se-aplica-a-lgpd. Acesso em: 12 jan. 2026.

CANAAN, R. The effects on local innovation arising from replicating the GDPR into Brazil's General Data Protection Law. *Internet Policy Review*, v. 11, n. 1, 2022. Disponível em: https://policyreview.info/articles/analysis/replicating-gdpr-into-brazilian-general-data-protection-law. Acesso em: 12 jan. 2026.

CHOU, E. N. R.; ALBANO, C. J.; ALMEIDA, P. Lei Geral de Proteção de Dados: uma análise da ISO 27701 como ferramenta de controle para LGPD. *Revista Ifes Ciência*, v. 10, n. 1, p. 55–69, 2024.

CLOUDIAN. *Data protection principles*: core principles of the GDPR. 2025. Disponível em: https://cloudian.com/guides/data-protection/data-protection-principles-7-core-principles-of-the-gdpr. Acesso em: 12 jan. 2026.

DATA PROTECTION COMMISSION. *Your rights under the GDPR*. 2025. Disponível em: http://www.dataprotection.ie/en/individuals/rights-individuals-under-general-data-protection-regulation. Acesso em: 12 jan. 2026.

DE LUCCA, N.; MARTINS, G. M.; QUEIROZ, R. C. Z. Consumer personal data protection in Brazil and the state of California (USA): a critical analysis of the Brazilian General Data Protection Law (LGPD) and California Consumer Privacy Act (CCPA). *Brazilian Journal of Law, Technology and Innovation*, v. 1, n. 1, p. 38–57, 2023.

DERBLI, L. S. O transplante jurídico do Regulamento Geral de Proteção de Dados da União Europeia (GDPR) para o direito brasileiro. *E-Legis: Revista Eletrônica do Programa de Pós-Graduação da Câmara dos Deputados*, n. 30, p. 181–193, 2019.

DONEDA, D. *Da privacidade à proteção de dados pessoais:* fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019.

EUROPEAN COMMISSION. *Who does the data protection law apply to?* 2025. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-

organisations/application-regulation/who-does-data-protection-law-apply_en. Acesso em: 12 jan. 2026.

EUROPEAN DATA PROTECTION BOARD. *Coordinated enforcement action – overview 2018–2024*. 2024. Disponível em: https://www.edpb.europa.eu/system/files/2025-01/edpb_cef-report-2024_20250116_rightofaccess_en.pdf. Acesso em: 12 jan. 2026.

EUROPEAN UNION. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Acesso em: 12 jan. 2026.

ERICKSON, A. Comparative analysis of the EU's GDPR and Brazil's LGPD: enforcement challenges with the LGPD. *Brooklyn Journal of International Law*, v. 44, n. 2, art. 9, 2019. Disponível em: https://brooklynworks.brooklaw.edu/bjil/vol44/iss2/9. Acesso em: 12 jan. 2026.

FEILER, A. R.; GAZANIGA, F.; VIEIRA, T. O valor fundamental dos dados pessoais: uma análise comparativa entre a LGPD e GDPR sob a ótica da análise econômica do direito. *Revista de Direito*, v. 16, n. 2, p. 1–29, 2024. Disponível em: https://doi.org/10.32361/2024160217158. Acesso em: 14 jan. 2026.

FERNANDES, M. E.; NUZZI, A. P. E. Fundamentos da Lei Geral de Proteção de Dados (LGPD): uma revisão narrativa. *Research, Society and Development*, v. 11, n. 12, e310111234247, 2022. Disponível em: https://doi.org/10.33448/rsd-v11i12.34247. Acesso em: 14 jan. 2026.

FORNASIER, M. de O.; KNEBEL, N. M. P. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. *Revista Direito e Práxis*, v. 12, n. 2, p. 1002–1033, 2021. Disponível em: https://doi.org/10.1590/2179-8966/2020/46944. Acesso em: 14 jan. 2026.

GDPR-INFO.EU. *Art. 15 GDPR – right of access by the data subject*. 2025. Disponível em: https://gdpr-info.eu/art-15-gdpr. Acesso em: 14 jan. 2026.

GDPR-INFO.EU. *Art. 25 GDPR – data protection by design and by default*. 2025. Disponível em: https://gdpr-info.eu/art-25-gdpr. Acesso em: 14 jan. 2026.
GDPR-INFO.EU. *Art. 83 GDPR – general conditions for imposing administrative fines*. 2025. Disponível em: https://gdpr-info.eu/art-83-gdpr. Acesso em: 14 jan. 2026.

GDPR.EU. *What is GDPR, the EU's new data protection law?* 2025. Disponível em: https://gdpr.eu/what-is-gdpr. Acesso em: 14 jan. 2026.

GETPRIVACY. *10 princípios que norteiam o tratamento dos dados pessoais*. 2025. Disponível em: https://getprivacy.com.br/10-principios-tratamento-de-dados-pessoais-lgpd. Acesso em: 14 jan. 2026.

INTEGRITETSSKYDDSMYNDIGHETEN (IMY). *The purposes and scope of GDPR*. 12 maio 2021. Disponível em: https://www.imy.se/en/organisations/data-protection/this-applies-accordning-to-gdpr/the-purposes-and-scope-of-gdpr/. Acesso em: 14 jan. 2026.

JUSBRASIL. *O que a multa bilionária da Amazon pode te ensinar sobre a importância de adequar a sua empresa à LGPD*. 30 jul. 2021. Disponível em: https://www.jusbrasil.com.br/artigos/o-que-a-multa-bilionaria-da-amazon-pode-te-ensinar-sobre-a-importancia-de-adequar-a-sua-empresa-a-lgpd/1259088238. Acesso em: 14 jan. 2026.

LORENZON, L. N. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. *Revista do Programa de Direito da União Europeia*, n. 1, p. 39–52, 2021.

LUGATI, L. N.; ALMEIDA, J. E. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. *Revista de Direito*, v. 12, n. 2, 2020. Disponível em: https://doi.org/10.32361/2020120210597. Acesso em: 14 jan. 2026.

MAGALHÃES, M. A. de. Data protection regulation: a comparative law approach. *International Journal of Digital Law*, v. 2, n. 2, p. 33–53, 2021. Disponível em: https://doi.org/10.5380/IJDL.magalhaes.v.2.n.2. Acesso em: 14 jan. 2026.

MASSENO, M. D.; MARTINS, G. M.; FALEIROS JÚNIOR, J. L. de M. A segurança na proteção de dados: entre o RGPD europeu e a LGPD brasileira. *Revista do Cejur: Prestação Jurisdicional*, v. 8, n. 1, e346, p. 1–28, 2020. Disponível em: https://doi.org/10.21902/rctjsc.v8i1.346. Acesso em: 14 jan. 2026.

NEVES, J. H. *Análise da efetividade da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) referente a dados ofertados através de meio digital*. 2023. Trabalho de Conclusão de Curso (Graduação) — Universidade Estadual Paulista (UNESP).

NEVES, R. A. P. GDPR e LGPD: estudo comparativo. 2021. Monografia (Bacharelado) — Centro Universitário de Brasília (UniCEUB), Faculdade de Ciências Jurídicas e Sociais (FAJS).
NEVES, R. A. P. LGPD e GDPR: transferências internacionais de dados pessoais. In: NUNES, C. A. R. et al. (org.). *Anais de Artigos Completos do VII CIDH Coimbra 2022 – Volume 10*. [S.l.]: Brasílica; Edições Brasil, 2022. p. 65–76.

OLIVEIRA, J. B. de; NASCIMENTO, E. S. de O.; OLIVEIRA JÚNIOR, E. P. de; ALEXANDRE, W. do N. A proteção de dados pessoais e a aplicação da LGPD no Brasil. *Revista Nativa Americana de Ciências, Tecnologia & Inovação*, v. 7, n. 1, 2025.
PINHO, A. C. de O. M. C.; CAVALCANTE, M. S. B. Transferência internacional de dados pessoais: a importância do reconhecimento dos fluxos internacionais de dados para o Brasil. *Revista Lumen*, v. 9, n. 17, p. 202–224, 2024. Disponível em: https://doi.org/10.32459/2447-8717e273. Acesso em: 14 jan. 2026.

PORTER, M. E.; VAN DER LINDE, C. Toward a new conception of the environment-competitiveness relationship. *Journal of Economic Perspectives*, v. 9, n. 4, p. 97–118, 1995. Disponível em: https://doi.org/10.1257/jep.9.4.97. Acesso em: 14 jan. 2026.

SARLET, G. B. S.; RUARO, R. L. A proteção de dados sensíveis no sistema jurídico brasileiro à luz da Lei Geral de Proteção de Dados (LGPD – Lei 13.709/2018). *Revista Direitos Fundamentais & Democracia*, v. 26, n. 2, p. 81–106, 2021. Disponível em: https://doi.org/10.25192/issn.1982-0496.rdfd.v26i22172. Acesso em: 12 jan. 2026.

SERPRO. *Objetivo e abrangência da LGPD*. 2025. Disponível em: https://www.serpro.gov.br/lgpd/menu/tratamento-dos-dados/objetivo-e-abrangencia-da-lgpd. Acesso em: 12 jan. 2026.

SUPREMO TRIBUNAL FEDERAL. *Arguição de Descumprimento de Preceito Fundamental n.º 695*, Distrito Federal. Relator: Min. Gilmar Mendes. Decisão publicada no Diário da Justiça Eletrônico em 19 jun. 2023. 2022. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5957122. Acesso em: 12 jan. 2026.

TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO (TJSP). Direitos do titular – LGPD. 2025. Disponível em: https://www.tjsp.jus.br/LGPD/LGPD/DireitoTitular. Acesso em: 12 jan. 2026.

UNIÃO EUROPEIA. *Carta dos Direitos Fundamentais da União Europeia*. Jornal Oficial da União Europeia, C 326, p. 391–407, 2012. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A12012P%2FTXT. Acesso em: 12 jan. 2026.

ZUBOFF, S. *A era do capitalismo de vigilância*. Tradução de G. Schlesinger. Rio de Janeiro: Intrínseca, 2021.