

IMPACTOS DA COLETA MASSIVA DE DADOS E A PROTEÇÃO DA PRIVACIDADE: UMA ANÁLISE A PARTIR DA LGPD E DA EC N° 115/2022

**IMPACTS OF MASS DATA COLLECTION AND PRIVACY PROTECTION: AN
ANALYSIS BASED ON THE LGPD AND CONSTITUTIONAL AMENDMENT NO.
115/2022**

Ciências Humanas • 27/10/2026

REGISTRO DOI: [10.70773/revistatopicos/793079783](https://doi.org/10.70773/revistatopicos/793079783)

Sthefanny Pereira Nunes¹

Marília Freitas Lima²

RESUMO

Esta pesquisa analisa os impactos da coleta massiva de dados pessoais sobre a privacidade no contexto do capitalismo de vigilância e das tecnologias digitais. O problema consiste em investigar em que medida a Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/2018) e a Emenda Constitucional nº 115/2022 materializam o direito fundamental à privacidade e à autodeterminação informativa, atuando para impor limites à coleta abusiva e sanar a assimetria informacional entre corporações tecnológicas e usuários. Justifica-se pela relevância jurídica, social e econômica, ante a vulnerabilidade do cidadão digital diante de vazamentos de dados e fraudes virtuais no Brasil. Objetiva-se analisar a eficácia do arcabouço normativo brasileiro na tutela da privacidade, avaliando os limites ao tratamento de dados e o papel fiscalizador e pedagógico da Autoridade Nacional de Proteção de Dados (ANPD). Adota-se o método dedutivo, de abordagem qualitativa, fundamentado em pesquisa bibliográfica e documental, mediante análise crítica da legislação, doutrina e documentos institucionais. Os resultados demonstram que a elevação da proteção de dados a garantia fundamental (EC nº 115/2022) e os princípios da LGPD (como finalidade, transparência e necessidade) constituem avanços essenciais; contudo, sua efetividade prática enfrenta obstáculos severos, como a opacidade algorítmica, o mito do consentimento em contratos por adesão, o paradoxo da privacidade e entraves na ANPD. Conclui-se que o fardo da proteção de dados não deve repousar apenas sobre o titular, demandando atuação estatal firme, consolidação de cultura corporativa de Privacy by Design e investimento em educação digital para a efetivação da dignidade humana no ciberespaço.

Palavras-chave: Coleta Massiva de Dados; Proteção da Privacidade; Lei Geral de Proteção de Dados; Emenda Constitucional nº 115/2022.

Autodeterminação Informativa; Autoridade Nacional de Proteção de Dados.

ABSTRACT

This research analyzes the impact of the mass collection of personal data on privacy within the context of surveillance capitalism and digital technologies. The study investigates the extent to which the General Data Protection Law (LGPD, Law No. 13.709/2018) and Constitutional Amendment No. 115/2022 give effect to the fundamental right to privacy and informational self-determination, acting to limit abusive data collection and address the information asymmetry between tech corporations and users. The research is justified by its legal, social, and economic relevance, given the vulnerability of digital citizens to data breaches and online fraud in Brazil. It aims to analyze the effectiveness of the Brazilian regulatory framework in safeguarding privacy by evaluating limits on data processing and the oversight and educational roles of the National Data Protection Authority (ANPD). A deductive method with a qualitative approach is adopted, grounded in bibliographic and documentary research involving a critical analysis of legislation, legal doctrine, and institutional documents. The results demonstrate that elevating data protection to a fundamental guarantee (Constitutional Amendment No. 115/2022) and the principles of the LGPD (such as purpose, transparency, and necessity) represent essential advances; however, their practical effectiveness faces significant obstacles, such as algorithmic opacity, the myth of consent in adhesion contracts, the privacy paradox, and constraints affecting the ANPD. The study concludes that the burden of data protection should not rest solely on the data subject; rather, it requires firm state action, the consolidation of a corporate culture of "Privacy by Design," and investment in digital education to ensure

the realization of human dignity in cyberspace.

Keywords: Massive Data Collection; Privacy Protection; General Data Protection Law; Constitutional Amendment No. 115/2022. Informational Self-Determination; National Data Protection Authority.

1. INTRODUÇÃO

A transição acelerada para a sociedade da informação transformou a convivência digital em um ambiente de contínua exposição de dados pessoais. Diariamente, indivíduos conectam-se a aplicativos aparentemente gratuitos que alimentam um fluxo massivo de informações monitoradas. Esses rastros digitais são interpretados por algoritmos e convertidos em bens de elevado valor comercial para corporações. A difusão da inteligência artificial e a elaboração automatizada de perfis de consumo aprofundam a vulnerabilidade do cidadão. As chamadas Big Techs passaram a monopolizar o mercado global de tecnologia e a direcionar o comportamento das massas. Configura-se, assim, a lógica do capitalismo de vigilância, na qual a experiência humana privada torna-se matéria-prima lucrativa. Nesse contexto, a proteção da privacidade consolida-se como mecanismo indispensável para a manutenção da liberdade e autonomia. Este estudo analisa exatamente os reflexos dessa exposição massiva sobre a privacidade e a tutela jurídica dos titulares.

A problemática central do artigo reside na severa assimetria informacional entre plataformas digitais e usuários. As empresas atuam em posição de superioridade fática e técnica ao controlarem a arquitetura opaca de processamento de dados. Essa disparidade gera vulnerabilidades técnica, jurídica, fática e informacional que

impedem o controle real pelo cidadão. O consentimento manifestado em termos de uso extensos converteu-se em mera ficção legal e aceite mecânico. A incoerência entre o valor atribuído à proteção e a entrega frequente de dados por conveniência gera o paradoxo da privacidade. Paralelamente, vazamentos recorrentes e ataques cibernéticos expõem dados sensíveis a riscos de fraudes e discriminações. Diante dessa complexidade, o modelo clássico de autoproteção individual revela-se insuficiente. Torna-se necessário que o ordenamento jurídico intervenha diretamente no fluxo informacional para compensar essa desigualdade.

Em resposta a esse cenário, a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) estabeleceu um novo paradigma no país, a legislação visa salvaguardar os direitos fundamentais de liberdade e privacidade, promovendo a governança de dados. A legislação foi fortalecida pela Emenda Constitucional nº 115/2022, que elevou a proteção de dados a direito fundamental, essa alteração consolidou a autodeterminação informativa como importante garantia à dignidade humana. As operações de tratamento exigem estrita observância aos princípios da finalidade, adequação, transparência e boa-fé. Ademais, os dados pessoais sensíveis recebem proteção diferenciada diante de seu alto potencial discriminatório. O ordenamento jurídico impõe, assim, limites operacionais e éticos à exploração indiscriminada de informações.

No centro da estrutura de fiscalização e governança atua a Autoridade Nacional de Proteção de Dados (ANPD), Como autarquia de natureza especial, a ANPD possui competências para normatizar, fiscalizar, orientar e aplicar sanções. O órgão fomenta ações pedagógicas e incentiva a aplicação do conceito de Privacy by Design nas organizações. Contudo, a efetividade regulatória

enfrenta desafios práticos, como barreiras burocráticas, linguagem formal e plataformas digitais pouco intuitivas dificultam o acesso do titular leigo. Além disso, a expansão da inteligência artificial exige regulação constante para evitar discriminações automatizadas. A materialização do direito à privacidade depende do fortalecimento institucional da ANPD e da educação digital.

2. O CENÁRIO DA COLETA MASSIVA E A VULNERABILIDADE DO INDIVÍDUO

A transição acelerada para a sociedade da informação, conforme apontam Martins, Jorgetto e Sutti (2019), acabou por mitigar aspectos cruciais do que se concebe como vida privada. Nesse cenário, os indivíduos permanecem grande parte do dia conectados à rede por meio de aplicativos aparentemente gratuitos voltados a todas as esferas cotidianas.

Essa constante interação alimenta um fluxo massivo de dados pessoais que, interpretados por algoritmos eficientes, tornaram-se bens de elevado valor comercial. Assim, a utilização sistemática desses serviços digitais insere o cidadão em um contexto de constante exposição de suas informações e de sua própria intimidade. Proteger a privacidade torna-se, então, segundo Luz e Loreiro (2018), um mecanismo indispensável para a manutenção da liberdade e da autonomia de cada indivíduo frente às pressões externas.

A palavra vulnerabilidade, originada do termo em latim *vulnus*, remete à suscetibilidade do sujeito de sofrer danos, exigindo do direito a aplicação de normas protetivas. No cenário cibernético, essa fragilidade se manifesta de forma acentuada pelas dimensões

técnica, jurídica, fática e informacional, visto que o indivíduo comum carece de conhecimento especializado para compreender os sistemas que utiliza. A difusão da inteligência artificial e a elaboração automatizada de perfis de consumo aprofundam a vulnerabilidade informacional, alterando substancialmente o próprio mercado de consumo. Desse modo, ocorre uma sobreposição de fraquezas técnicas e econômicas que agravam significativamente a condição do cidadão perante os controladores.

A exposição decorrente da coleta em massa torna os indivíduos alvos fáceis de incidentes de segurança, vazamentos recorrentes e ataques cibernéticos e esse cenário abre espaço para a ocorrência de fraudes financeiras, roubo de identidade, assédio comercial por telemarketing e publicidades abusivas não autorizadas. Ademais, o extravio de dados pessoais sensíveis atinge os aspectos mais íntimos da vida do titular, gerando danos de ordem moral e patrimonial.

Frente à complexidade do cenário tecnológico e à sofisticação da mineração de dados, o modelo clássico de proteção individual de privacidade revela-se insuficiente. A doutrina adverte que não se deve depositar exclusivamente sobre os ombros dos titulares o fardo normativo de resguardar suas informações pessoais. Torna-se imperativo que o ordenamento jurídico intervenha diretamente no fluxo informacional, limitando a autonomia da vontade para compensar a extrema disparidade de forças. Nesse contexto, a Lei Geral de Proteção de Dados e a promulgação da Emenda Constitucional nº 115/2022 consagram à autodeterminação informativa como direito fundamental autônomo, essencial para a tutela da dignidade humana.

2.1. Riscos de Vigilância, Vazamentos Massivos e a Insegurança Digital

A relação constante com equipamentos portáteis, como smartphones e notebooks, criou uma dependência estrutural em que o sujeito fornece dados para realizar praticamente todas as atividades diárias. Essas trocas de informações ocorrem em uma arquitetura de redes que influencia o comportamento e gera situações de insegurança digital constante para os usuários.

Segundo Ralves e Vieira (2014) *apud* Gomes (2024), a convivência íntima com as facilidades tecnológicas contribui para a perda de visão do sujeito sobre as reais consequências dessa exposição massiva. Assim, a inserção de dados em plataformas digitais já não é percebida como um risco imediato, sendo tratada como uma comodidade necessária da vida moderna. Essa percepção distorcida aumenta a fragilidade do titular perante as corporações que gerenciam esses fluxos informacionais.

A privacidade, que outrora era vista como uma garantia jurídica ou um bem desfrutado de forma gratuita, passou a ser um recurso sob constante ataque e de alto custo. Morozov (2018) *apud* Gomes (2024) afirma que hoje é necessário gastar vultosos recursos e atenção para dominar as ferramentas e proteger minimamente a esfera íntima individual. A problemática central reside no fato de que o interesse das plataformas de tecnologia pelos dados pessoais visa a posterior comercialização e modulação algorítmica de perfis. O domínio sobre as informações pessoais tornou-se uma disputa desigual entre o cidadão e o imenso poder econômico das corporações globais.

No cenário atual, as informações dos indivíduos são coletadas como insumos de alto valor econômico por empresas e grandes corporações que dominam o mercado. A coleta massiva de dados pessoais é o motor que impulsiona o novo mercado informacional, transformando rastros digitais em mercadorias lucrativas.

Machado (2018) *apud* Gomes (2024) afirma que esses dados, captados pelas plataformas, representam a matéria-prima essencial para as estratégias de negócios contemporâneas. O valor econômico fundamental reside na capacidade técnica de segmentar o mercado e atrair consumidores específicos para produtos determinados por algoritmos. Essa dinâmica intensifica a exploração da subjetividade humana em prol do lucro corporativo desenfreado e da manipulação do consumo.

O desenvolvimento acelerado das Tecnologias de Informação e Comunicação (TICs) permitiu a estruturação de ambientes de Big Data³, onde o uso massivo de dados é a regra. Softwares e computadores de alto desempenho são produzidos especificamente para processar grandes volumes de dados e convertê-los em vantagens competitivas. Mendes (2014) complementa que essa utilização massiva por organismos estatais e privados apresenta desafios inéditos ao direito fundamental à privacidade dos cidadãos.

A necessidade informacional das organizações modernas remodela áreas de negócio, exigindo novas arquiteturas de armazenamento e segurança de dados. Contudo, o foco corporativo na proteção de dados muitas vezes prioriza a segurança contra terceiros, ignorando a necessária autonomia do titular.

As chamadas Big Techs⁴ detêm hoje o poder desproporcional de influenciar o comportamento e o consumo de massas a partir da manipulação de dados. Bernardo et al. (2021) destacam que a expansão das redes sociais permitiu que poucas empresas monopolizassem o mercado global de tecnologia. Essa prática busca legitimar a coleta massiva a todo custo, criando um jogo de interesses onde o lucro é o objetivo final. O enriquecimento dessas organizações ocorre em escala global, utilizando dados pessoais como elemento essencial de um sistema de mão única e opaco. Assim, o titular fornece a matéria-prima sem conhecer as estratégias utilizadas pelas corporações para a modulação algorítmica de sua própria vida.

A assimetria informacional entre as plataformas e os usuários é um dos principais fatores que acentuam a vulnerabilidade do indivíduo no ciberespaço. O aumento exponencial da quantidade de dados coletados reduz o conhecimento dos cidadãos sobre o uso real dessas informações sensíveis. Sousa, Barrancos e Maia (2019) pontuam que o uso de dados para o consumo de recursos ocasiona essa lacuna de conhecimento perigosa. O titular, muitas vezes, não compreende que ao interagir nas redes sociais está inserindo informações que impactam profundamente sua vida privada. Essa fragilidade é reforçada pela complexidade técnica dos sistemas de processamento massivo, que são quase sempre invisíveis ao usuário comum.

A permissão concedida por meio de termos de uso e diálogos convencionais influencia diretamente na formação de opinião e no controle social dos sujeitos. Meireles (2023) argumenta que o desejo de aderir a serviços "gratuitos" faz com que os usuários forneçam dados pessoais de forma natural. Entretanto, a maioria dos sujeitos

se abstém de ler os extensos documentos de privacidade devido à sua complexidade técnica e jurídica.

Freitas (2017) alega que, mesmo quando o usuário lê, o distanciamento entre a informação e a prática dificulta a compreensão real dos riscos. Assim, o consentimento torna-se uma ferramenta formal que viabiliza a manipulação algorítmica em vez de garantir a autonomia real do titular.

O fenômeno contemporâneo denominado "Capitalismo de Vigilância" define uma nova lógica de acumulação baseada na análise e previsão do comportamento humano. Zuboff (2018) infere que a captura secreta de dados é, muitas vezes, uma invasão silenciosa e erosiva dos direitos de privacidade. Nesse modelo, o sigilo institucional das corporações cresce enquanto a privacidade individual é corroída e transformada em valor de mercado.

As Big Techs utilizam a tecnologia para extrair valor de experiências humanas privadas sem o devido e esclarecido consentimento. Essa vigilância constante molda a subjetividade humana, orientando estrategicamente o desejo do consumidor para atingir objetivos lucrativos definidos por algoritmos.

Os riscos de vazamentos massivos e ataques de hackers representam uma ameaça severa à segurança digital e à intimidade do cidadão moderno. Casos recorrentes, como os vazamentos no Mercado Livre e em grandes instituições financeiras, evidenciam a fragilidade dos atuais sistemas de guarda. O pesquisador Martin Hron (2019) afirma ser impossível não reconhecer o caos causado por esses grandes vazamentos de dados nos últimos meses. Dados roubados resultam em fraudes, roubo de identidade e publicidades

indesejadas que violam a autonomia do indivíduo permanentemente. A insegurança digital torna-se, portanto, uma condição intrínseca ao uso das redes, onde o controle sobre o destino das informações é perdido.

A vulnerabilidade do titular é agravada pela capacidade tecnológica de processar dados sensíveis, como origem racial e convicções políticas. Esses dados, quando expostos ou tratados indevidamente pelas corporações, podem fomentar discriminações e atingir aspectos sociais da vida. Nascimento e Silva (2023) destacam que a disponibilidade indevida de dados favorece a identificação direta ou indireta do indivíduo, violando sua liberdade. A proteção desses dados é imprescindível para garantir que o desenvolvimento da personalidade ocorra sem interferências abusivas. Sem uma tutela jurídica eficaz e rigorosa, o titular fica dependente de decisões automatizadas discriminatórias baseadas em perfis opacos.

2.2. A Assimetria Informacional Entre Plataformas e Usuários

A assimetria informacional nas relações digitais contemporâneas caracteriza-se, primordialmente, pela acentuada disparidade de conhecimento técnico e factual existente entre os grandes provedores de serviços e os respectivos titulares de dados. Conforme apontam Oliveira e Accioly (2020 *apud* Takaku, 2022, p. 19), essa situação se configura quando uma das partes da relação jurídica detém mais informações do que a outra sobre os fatores determinantes de uma transação específica. Esse cenário gera um desequilíbrio conjuntural severo, no qual o fornecedor atua em uma posição de superioridade, intensificada pelo controle que as empresas exercem sobre a arquitetura dos sistemas de processamento. A relação deixa de se desenvolver de forma

espontânea para se tornar um campo de forças desproporcional, onde o usuário comum encontra-se em constante estado de fragilidade técnica. Portanto, a assimetria não constitui apenas um mero detalhe operacional, mas sim o pilar de modelos que exploram a vulnerabilidade informacional do cidadão comum.

O avanço de ferramentas como a inteligência artificial, o *machine learning* e o uso de algoritmos sofisticados permitiu que as empresas elevassem sua cognição para monitorar o comportamento humano na rede. Herscovici (2021) destaca que esse sistema opera através de uma opacidade intrínseca, permitindo que comportamentos oportunistas sejam desenvolvidos pelas plataformas em detrimento da transparência absoluta.

Enquanto o indivíduo é monitorado continuamente em suas atividades cotidianas, ele permanece incapaz de acompanhar quem compartilha seus dados pessoais e para quais finalidades específicas as informações são destinadas. Essa capacidade técnica diferenciada cria uma barreira de compreensão quase intransponível, onde o saber institucional das empresas corrói progressivamente a autonomia individual. Assim, o ambiente digital transforma-se em um controle que é exercido de maneira invisível sobre a totalidade da população conectada.

Existe uma distinção fundamental entre a informação de primeiro grau, cedida de forma consciente, e a de segundo grau, rastreada sem a intervenção direta do titular. Segundo Herscovici (2021), o usuário fornece a matéria-prima bruta (*raw material*) para o mercado informacional através de suas trajetórias sociais e culturais complexas realizadas cotidianamente no ambiente da rede.

A falta de transparência do sistema manifesta-se quando o indivíduo perde a gerência sobre as transações efetuadas com seus dados pessoais nos mercados secundários de informações. O usuário é, muitas vezes, despossuído de suas informações pessoais em um regime de escambo desigual por serviços tidos como gratuitos pelas plataformas digitais. Nessa dinâmica, o poder de barganha do cidadão é limitado frente aos gigantes tecnológicos que monetizam dados extraídos sem o controle real do titular.

A sociedade contemporânea prospera sob a lógica do capitalismo de vigilância, termo utilizado por Shoshana Zuboff para descrever a predição de desejos humanos como uma nova e valiosa fonte de riqueza. As plataformas digitais utilizam a coleta massiva de dados para modificar comportamentos e induzir escolhas de consumo ou até posicionamentos políticos específicos dos usuários na rede. Esse procedimento possui natureza invasiva, pois os algoritmos frequentemente baseiam-se em padrões passados para determinar trajetórias sociais futuras de forma potencialmente discriminatória.

A modulação algorítmica atua para reduzir a incerteza do mercado, convertendo a espontaneidade humana em ativos financeiros valiosos para os agentes controladores do sistema. Assim, a suposta neutralidade das ferramentas tecnológicas é refutada pela evidência de uma ingerência constante na esfera privada do cidadão comum.

A doutrina identifica diversas faces da fragilidade do titular de dados, destacando as vulnerabilidades técnica, jurídica, fática e informacional como obstáculos ao equilíbrio nas relações digitais. Segundo Simone Takaku (2022), fundamentada nas lições de Bruno Miragem (2020), na vulnerabilidade técnica o consumidor carece de conhecimento especializado para compreender o funcionamento

interno dos sistemas complexos que processam suas informações. Miragem destaca ainda a existência da "vulnerabilidade digital", que se manifesta na falta de habilidade ou familiaridade com o ambiente virtual, onde as escolhas são influenciadas por incentivos sensoriais e emocionais do design e do discurso da plataforma.

Os contratos por adesão, materializados nos extensos termos de uso e políticas de privacidade, são instrumentos de imposição unilateral dos fornecedores de serviços no ambiente digital. Cláusulas padronizadas e previamente definidas não permitem que o usuário discuta ou modifique substancialmente o conteúdo do que está aceitando para acessar o serviço. Estudos indicam que a maioria dos brasileiros é incapaz de interpretar esses textos devido à linguagem técnica densa e ao tamanho dos documentos. O aceite eletrônico, na prática, torna-se um ato mecânico de apenas correr a barra de rolagem, desprovido de qualquer manifestação de vontade consciente. Essa configuração contratual reforça a desigualdade de poder, pois o titular ignora os direitos e deveres inerentes à relação de tratamento estabelecida.

O consentimento, embora pilar da autodeterminação informativa, é frequentemente apontado como um mito ou uma ficção legal no cenário de hiperconectividade em que vivemos atualmente. A alternativa à não revelação de dados pessoais costuma ser a renúncia brutal a bens e serviços essenciais para a participação social e democrática. A liberdade de escolha fica prejudicada quando o usuário é constrangido a aceitar termos intrusivos sob a ótica restritiva do "pegar ou largar". Bruno Bioni (2021) argumenta que a multiplicidade de adjetivos atribuídos ao consentimento visa apenas marcar que o titular é incapaz de decidir sozinho sem a cooperação da contraparte. Sem essa cooperação leal, o controle

individual torna-se meramente formal, falhando em proteger a privacidade dos dados.

Segundo Daniel Solove (2009), barreiras cognitivas e estruturais dificultam o autogerenciamento efetivo da privacidade pelo indivíduo na sociedade da informação, envolvendo desafios na tomada de decisão e na escala do tratamento de dados. Esse cenário é marcado pelo chamado "paradoxo da privacidade", termo que Bruno Bioni (2021) utiliza para descrever a incoerência entre o valor que os titulares atribuem à proteção e as ações dissonantes de ceder dados por conveniência imediata.

O autor ressalta que o ser humano tende a priorizar gratificações instantâneas e zonas de conforto, desvalorizando prejuízos que podem ocorrer em um futuro distante. Solove (2009) aponta o "problema da combinação", no qual a multiplicidade de entes coletando dados fragmentados permite a formação de um retrato completo da personalidade do sujeito sem a sua participação ou conhecimento. Diante desse quadro de vulnerabilidade estrutural, Bioni (2021) conclui que o fardo da proteção de dados pessoais não deve repousar apenas sobre os ombros do titular.

A proteção de dados pessoais foi elevada ao status de direito fundamental no Brasil por meio da promulgação da Emenda Constitucional 115, em fevereiro de 2022. Essa positivação constitucional visa garantir ao indivíduo o domínio pleno sobre todos os movimentos de seus dados, desde a coleta até o compartilhamento. O direito à autodeterminação informativa permite que a pessoa decida como e onde suas informações pessoais serão expostas ao processamento automatizado do sistema. Contudo, a efetividade desse direito fundamental é posta

em xeque pela crescente capacidade tecnológica de análise comportamental. O Estado deve, portanto, atuar ativamente para coibir abusos e garantir que a proteção seja suficiente e necessária à dignidade humana.

3. O MARCO REGULATÓRIO DA LGPD E A ATUAÇÃO DA ANPD

3.1. A Eficácia Regulatória na Materialização do Direito Fundamental à Privacidade

A Lei Geral de Proteção de Dados (LGPD), registrada como a Lei nº 13.709/2018, estabeleceu um novo paradigma jurídico no Brasil ao regulamentar o tratamento de dados pessoais em meios digitais e físicos. Seu objetivo primordial é a salvaguarda dos direitos fundamentais de liberdade e de privacidade, além de promover o livre desenvolvimento da personalidade da pessoa natural. A norma surgiu da necessidade de impor limites ao tratamento indiscriminado de informações, conferindo segurança jurídica ao titular de dados.

A evolução das tecnologias digitais e a digitalização massiva das interações sociais impuseram ao Direito o desafio de tutelar a privacidade em um ambiente de constante troca de informações. Nesse contexto, a materialização do direito à privacidade no Brasil encontrou um marco decisivo com a promulgação da Lei Geral de Proteção de Dados (LGPD), inspirada em modelos internacionais como o GDPR europeu. A legislação busca não apenas estabelecer regras jurídicas, mas promover uma cultura de governança de dados que assegure a dignidade e a liberdade dos indivíduos no meio digital.

A eficácia regulatória desse sistema foi reforçada pela Emenda Constitucional nº 115/2022, que incluiu a proteção de dados pessoais no rol de direitos e garantias fundamentais da Constituição Federal. Essa alteração consolidou o chamado constitucionalismo digital, exigindo que o Estado adote ferramentas dinâmicas para a tutela desses direitos diante da celeridade das inovações tecnológicas. Assim, a proteção de dados deixou de ser vista como uma ferramenta acessória para ser reconhecida como um direito autônomo e fundamental.

Para que essa proteção seja efetiva, a LGPD estabelece princípios fundamentais como a finalidade, a boa-fé e a transparência, que devem orientar qualquer operação de tratamento de dados. Segundo Danilo Doneda (2021), o discurso sobre a privacidade contemporânea gira essencialmente em torno do controle sobre a informação pessoal, exigindo uma depuração constante do sentido instrumental do dado. Portanto, a materialização do direito depende da conformidade ética e técnica dos agentes de tratamento.

A Autoridade Nacional de Proteção de Dados (ANPD) surge como o órgão central para viabilizar essa regulação, detendo competências para fiscalizar, orientar e aplicar sanções. Como autarquia de natureza especial, a ANPD tem a missão de zelar pela proteção dos dados pessoais e assegurar que tanto o setor público quanto o privado cumpram as diretrizes legais. Sua atuação é considerada essencial para o desenvolvimento de uma cultura de privacidade sólida e enraizada no país.

Contudo, a eficácia regulatória enfrenta desafios estruturais significativos na consolidação da ANPD como uma autoridade plena. A complexidade burocrática e a linguagem técnica utilizada

pelo órgão muitas vezes elitizam o procedimento, criando entraves desnecessários para o cidadão comum.

Patricia Peck Pinheiro (2021) destaca que a dinâmica da era da informação exige uma mudança profunda na prática cotidiana do Direito, rompendo limites físicos e temporais. Na prática regulatória brasileira, observa-se um descompasso entre o rigor da norma e a realidade operacional, onde muitos titulares encontram obstáculos até para identificar o controlador de seus dados. Essa lacuna compromete a materialização do direito, pois a fiscalização limitada pode abrir brechas para abusos institucionais.

A aplicação de sanções administrativas é o instrumento de "ultima ratio" para garantir o cumprimento da lei. O caso da empresa Telekall Infoservice, a primeira a ser multada pela ANPD, representa um marco histórico, mas também revela limitações pela aplicação de valores considerados simbólicos diante do teto legal. Para especialistas, embora a multa demonstre que o órgão está disposto a agir, a eficácia pedagógica da sanção depende da proporcionalidade e da gravidade das infrações.

A ascensão da Inteligência Artificial (IA) intensifica a necessidade de uma gestão ética e transparente, exigindo que decisões automatizadas não violem direitos individuais. Conforme ressalta o professor Lucca Belli (2025), o desenvolvimento de soluções de IA no Brasil ainda carece de adequação plena à legislação de proteção de dados, apresentando falhas graves no uso indevido de informações pessoais. A regulação deve, portanto, ser capaz de acompanhar a evolução algorítmica para evitar discriminações automatizadas (Moreira *et al.*, 2025).

O setor público também enfrenta desafios específicos, onde a utilização de dados pessoais pelo Estado exige um estrito atendimento ao princípio da legalidade. A ausência de estruturas rígidas de proteção em bancos de dados governamentais pode resultar em vazamentos massivos, evidenciando falhas na tutela dos direitos dos cidadãos. A materialização da privacidade no setor público requer uma convergência entre a LGPD e a Lei de Acesso à Informação (LAI) (Paiva; Lanzillo, 2024).

Segundo Pinto e Danieletto (2025), a eficácia regulatória é prejudicada quando o titular é submetido a uma carga investigativa desproporcional para realizar uma denúncia. A exigência de contato prévio com o controlador, por exemplo, pode ser um fator desestimulante e desgastante, especialmente quando as empresas oferecem apenas respostas automatizadas e pouco explicativas. Essa burocracia desestimula a participação cidadã e enfraquece o papel fiscalizador da autoridade.

A transparência nas relações de consumo foi impulsionada pela exigência de consentimento explícito, forçando a revisão de contratos e termos de uso. Esse processo busca reduzir práticas abusivas e promover uma relação mais clara entre consumidores e organizações. Contudo, a materialização desse direito só ocorre plenamente quando o titular compreende como suas informações são tratadas e tem mecanismos reais para contestar usos indevidos. (Moreira *et al.*, 2025)

A análise qualitativa da atuação da ANPD sugere que o órgão ainda desempenha um papel que pode ser considerado figurativo por parte da população, dado o baixo número de processos finalizados nos últimos anos. A consolidação da autoridade depende da

superação de falhas de comunicação institucional e da disseminação de informações acessíveis sobre seus canais e procedimentos. Sem essa proximidade com o cidadão, a regulação permanece apenas no plano normativo. (Pinto; Danieleto, 2025)

Em conclusão, a eficácia regulatória na materialização do direito à privacidade no Brasil é um processo em construção que exige a integração de esforços legais, técnicos e educacionais. A LGPD e a EC 115/2022 fornecem o alicerce jurídico necessário, mas a efetividade depende da consolidação de uma cultura de proteção de dados que priorize o titular. Somente com uma ANPD estruturalmente fortalecida e instituições comprometidas com a ética digital será possível garantir o pleno exercício desse direito fundamental.

Cabe à ANPD elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade. O órgão atua como intérprete da lei, esclarecendo conceitos técnicos e estabelecendo padrões de segurança, sua existência é um requisito vital para a governança de dados em regimes democráticos modernos.

A ANPD atua como uma autarquia de natureza especial, vinculada ao Ministério da Justiça, com competência para zelar pela observância dos segredos comerciais e industriais. De acordo com Lima (2020), sua existência é vital para preencher as lacunas deixadas por legislações anteriores, como o Marco Civil da Internet, que carecia de um órgão fiscalizador específico. Além de fiscalizar, a autoridade possui o papel pedagógico de difundir na sociedade o conhecimento sobre as normas e as medidas de segurança adequadas, onde sua atuação equilibrada é o pilar que sustenta a confiança do cidadão no ambiente intensamente digitalizado.

A eficácia regulatória na materialização do direito à privacidade manifesta-se através da imposição de princípios como finalidade, necessidade, transparência e boa-fé. Esses fundamentos jurídicos coíbem o tratamento abusivo e exigem que os controladores de dados adotem medidas preventivas contra vazamentos e acessos não autorizados. Carvalho (2022) ressalta que o mapeamento do ciclo de vida dos dados é a primeira medida essencial para identificar riscos elevados nas operações.

Ao exercer sua função reguladora, a ANPD garante que os agentes de tratamento sigam diretrizes estritas e sofram sanções administrativas em caso de descumprimento. Portanto, a materialização real do direito depende da capacidade do Estado em impor limites objetivos à coleta massiva e indiscriminada.

No cenário empresarial, a LGPD impulsionou uma mudança estrutural e cultural, transformando a proteção de dados em um diferencial estratégico e ético para as organizações, onde as empresas passaram a investir em ferramentas de segurança mais robustas, para mitigar riscos de espionagem e ataques cibernéticos. Conforme Pontes (2020), a adoção de medidas proativas de segurança fortalece a imagem das instituições no mercado e consolida a fidelização e confiança dos consumidores. A atuação da ANPD motiva, especialmente as médias e grandes empresas, a priorizarem a conformidade legal para evitar danos severos à reputação corporativa. Desse modo, o marco regulatório promove uma governança de dados mais transparente, responsável e ética no país.

Apesar da legislação, o titular de dados ainda enfrenta vulnerabilidades acentuadas pela assimetria informacional e pela

crescente complexidade tecnológica. Bioni (2021) descreve o chamado "paradoxo da privacidade" como a incoerência entre o valor que os indivíduos atribuem à proteção e a conveniência de ceder dados por serviços gratuitos. Muitas vezes, o consentimento torna-se uma mera ficção legal, pois os termos de uso são extensos e de difícil compreensão para o cidadão comum. A inserção de dados em plataformas digitais é percebida como uma comodidade necessária, mascarando os riscos de vigilância e modulação algorítmica constante. Diante disso, a proteção estatal deve transcender o mero formalismo jurídico para assegurar a autonomia real do titular.

A atuação da ANPD enfrenta desafios estruturais que comprometem sua consolidação plena como autoridade máxima de proteção de dados no Brasil. Pinto e Danieleto (2025) apontam que a linguagem formal e os sites eletrônicos mal organizados impõem barreiras ao acesso do cidadão leigo ao órgão. A dificuldade em distinguir entre denúncia e petição de titular gera insegurança jurídica e afasta o indivíduo da busca pela tutela de seus direitos fundamentais. Logo, a eficácia da lei esbarra na necessidade urgente de uma estrutura administrativa mais acessível, intuitiva e inclusiva.

O reconhecimento da proteção de dados como um direito autônomo e fundamental decorre da compreensão de que as informações pessoais são extensões da própria personalidade humana. Conforme assevera Doneda (2011), esse controle efetivo sobre os dados é essencial para a garantia da dignidade humana no ambiente do ciberespaço. Mendes (2014) acrescenta que a proteção jurídica deve ser canalizada para o desenvolvimento integral do ser humano, superando a visão meramente técnica ou comercial. A autodeterminação informativa permite que a pessoa decida como e

onde suas informações pessoais serão expostas ao processamento automatizado do sistema. Assim, o Estado tem o dever de atuar ativamente para coibir abusos que violem essa esfera íntima protegida.

O poder sancionatório da ANPD, embora previsto legalmente, ainda apresenta resultados modestos em termos de penalidades efetivas aplicadas desde sua criação. O caso da empresa Telekall Infoservice⁵, primeira a ser multada, exemplifica a atuação do órgão contra o uso indevido de dados para fins de propaganda eleitoral. No entanto, a aplicação de sanções deve observar critérios técnicos rigorosos como a gravidade da infração e a condição econômica do agente infrator.

Para que a LGPD não seja vista apenas como uma norma figurativa, é necessário que as punições administrativas tragam seriedade e senso de urgência ao tema. A materialização do direito fundamental exige, portanto, um equilíbrio constante entre a orientação educativa e o rigor punitivo.

Em última análise, a eficácia regulatória na proteção da privacidade no Brasil depende do fortalecimento contínuo da ANPD e do investimento em educação digital. A superação da fragilidade do titular no ambiente virtual requer que o conhecimento sobre a lei permita o exercício real da autodeterminação informativa. Conforme Sarlet (2021), a proteção de dados tornou-se um instrumento vital para a salvaguarda da liberdade em uma sociedade intensamente datificada. O marco regulatório da LGPD é o ponto de partida, mas sua materialização plena exige uma cultura de privacidade enraizada em todos os setores sociais. Somente assim, o direito à

proteção de dados deixará de ser uma promessa normativa para tornar-se uma realidade efetiva.

3.2. Limites Ao Tratamento de Dados e o Papel Fiscalizador da Autoridade Nacional de Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD) estabelece limites rigorosos ao tratamento de informações, fundamentados no princípio da autodeterminação informativa. Conforme Nascimento e Silva (2023), o tratamento de dados não possui caráter absoluto, devendo permitir que o titular exerça controle real sobre seus movimentos informacionais. A norma impõe que qualquer operação de tratamento respeite a dignidade da pessoa humana e o livre desenvolvimento da personalidade. Nesse contexto, a legislação deixa de ser um conjunto de regras técnicas para se tornar um instrumento ético de proteção.

Portanto, o marco regulatório brasileiro exige que o fluxo de dados ocorra sob limites claros e transparentes no ambiente digital. A conformidade legal depende da compreensão de que os dados são extensões da personalidade individual, sendo assim, a autodeterminação informativa funciona como a barreira principiológica fundamental contra abusos institucionais.

A eficácia da proteção de dados baseia-se na aplicação de princípios como finalidade, adequação e necessidade, conforme previsto no artigo 6º da lei. O princípio da necessidade é central, pois determina a limitação do tratamento ao mínimo necessário para a realização das finalidades pretendidas. Segundo Moreira et al. (2025), a regra do "mínimo necessário" orienta que as empresas colem apenas dados essenciais e suficientes para cada atividade. Qualquer coleta de

dados pessoais que exceda o escopo legítimo e informado é considerada abusiva perante o ordenamento jurídico.

Para que o tratamento seja lícito, ele deve estar amparado em uma das dez bases legais previstas no artigo 7º da LGPD. O consentimento do titular é a base mais conhecida, porém não é a única, existindo exceções para o cumprimento de obrigações legais ou regulatórias. Segundo Nascimento e Silva (2023), no setor público, as bases legais são ainda mais específicas e fundamentam-se no estrito interesse coletivo.

A legislação busca impedir que o dado pessoal seja utilizado como mero recurso econômico sem o devido respaldo jurídico. Conforme Paiva e Lanzillo (2024), a correta identificação da hipótese legal é o que garante a segurança operacional das instituições. A identificação da base legal correta funciona como um limite operacional e ético inafastável para qualquer controlador. Sem essa fundamentação, a atividade de tratamento torna-se irregular e passível de graves punições administrativas.

Os dados pessoais sensíveis, que revelam convicção religiosa, origem racial ou dados de saúde, possuem limites de tratamento ainda mais restritivos. A LGPD confere a essas informações uma proteção especial devido ao alto potencial discriminatório e danos irreversíveis à intimidade. De acordo com Nascimento e Silva (2023), o extravio desses dados pode acarretar consequências severas nos âmbitos social, emocional e financeiro do indivíduo. O tratamento dessas categorias exige salvaguardas específicas, como o consentimento destacado ou finalidades de prevenção à fraude.

A Autoridade Nacional de Proteção de Dados monitora com rigor essas operações para coibir abusos algorítmicos. A sensibilidade da informação impõe ao controlador o dever de implementar medidas técnicas e administrativas reforçadas.

O tratamento de dados é compreendido como um ciclo de vida que abrange desde a coleta e processamento até a eliminação definitiva. Segundo Moreira et al. (2025), o mapeamento desse ciclo é a medida primordial para identificar riscos e vulnerabilidades institucionais. A retenção das informações não pode ser perpétua, devendo cessar assim que a finalidade original for atingida ou o prazo legal expirar. O descarte ético e seguro é uma obrigação do controlador, muitas vezes auxiliada pela expertise de profissionais arquivistas.

A transparência sobre a temporalidade dos dados é exigida para evitar acúmulos desnecessários de informações pessoais. Conforme as fontes, o gerenciamento temporal funciona como um limite técnico essencial para a conformidade legal. Assim, o controle sobre o fluxo informacional é um direito assegurado pela Constituição Federal.

A Autoridade Nacional de Proteção de Dados (ANPD) surge como o órgão centralizador da estratégia regulatória e fiscalizadora no Brasil. Criada pela Lei nº 13.853/2019, a autarquia possui autonomia técnica e decisória para implementar as diretrizes da LGPD. Segundo Pinto e Danieletto (2025), a existência de uma autoridade forte é requisito vital para a governança digital democrática. Suas missões abrangem desde a edição de normas técnicas até a interpretação dos dispositivos legais. O órgão atua como guardião da privacidade, mediando as relações de poder entre cidadãos, mercado e Estado.

Cabe à ANPD zelar pela proteção dos dados pessoais e promover a conscientização sobre normas de segurança. Portanto, a autoridade é a peça-chave na estrutura regulatória, garantindo que a tecnologia respeite a dignidade humana.

O papel fiscalizador da ANPD é exercido através de ciclos de monitoramento que analisam o comportamento dos agentes de tratamento. Segundo Pinto e Danieletto (2025), esses instrumentos servem para planejar e direcionar as ações da Coordenação-Geral de Fiscalização. A autoridade tem o poder de solicitar relatórios de impacto para avaliar se operações oferecem riscos às liberdades dos titulares. A fiscalização não visa apenas a punição, mas a promoção de uma cultura de conformidade e boas práticas.

O monitoramento ativo é fundamental para mitigar a assimetria informacional entre grandes plataformas e usuários. A ANPD processa denúncias e petições para verificar indícios de irregularidades que afetem a coletividade. Assim, a vigilância estatal é o instrumento que assegura a materialização das garantias previstas na LGPD.

A competência sancionatória permite à ANPD aplicar penalidades administrativas que variam de advertências a multas de até R\$ 50 milhões. Essas sanções são aplicadas após processo administrativo que deve garantir o contraditório e a ampla defesa ao agente. O modelo de valoração das multas adota critérios técnicos como gravidade da infração, boa-fé e reincidência.

A punição funciona como um desestimulante para práticas abusivas e vazamentos massivos de informações. Conforme Pinto e Danieletto (2025), a consolidação do poder sancionador é vital para

criar senso de urgência nos controladores. Embora o número de sanções ainda seja reduzido, seu impacto simbólico é relevante para a regulação do mercado. Logo, o rigor punitivo é o último recurso regulatório para proteger o direito à autodeterminação informativa.

Apesar da atuação ativa da ANPD, a estrutura de requerimentos ainda enfrenta desafios que afetam sua plena eficácia prática. Relatórios de 2023 indicam que cerca de 43% das petições de titulares não são analisadas por falta de requisitos básicos. Pinto e Danieletto (2025) apontam que falhas na comunicação institucional dificultam o acesso do cidadão comum ao órgão. Muitos titulares possuem dificuldades em compreender a linguagem técnica e os limites de competência da autoridade nacional. A assimetria informacional reflete-se na fragilidade do indivíduo ao formalizar reclamações contra “gigantes” do setor. Superar esses obstáculos estruturais é fundamental para que a ANPD não seja percebida apenas como figurativa.

A função educativa da ANPD é um pilar preventivo essencial para fomentar uma cultura de privacidade enraizada no Brasil. O órgão elabora guias orientativos que auxiliam empresas e entes públicos na adaptação aos parâmetros da lei. Tais manuais visam empoderar os titulares sobre seus direitos e a importância da proteção de dados sensíveis.

O incentivo ao conceito de *Privacy by Design* assegura a privacidade desde a concepção de novos produtos e serviços. A capacitação técnica das equipes nas organizações é sugerida como medida essencial para garantir a segurança informacional. Assim, a regulação pedagógica eleva o padrão de proteção em todo o meio digital brasileiro.

A comunicação transparente é crucial para minimizar prejuízos financeiros e emocionais resultantes de violações de dados. O mapeamento constante de vulnerabilidades previne o acesso não autorizado por técnicas de engenharia social. Segundo Moreira et al. (2025), a adoção de medidas técnicas e administrativas é uma responsabilidade corporativa contínua. A ANPD orienta sobre a adoção de padrões mínimos de segurança proporcionais ao risco de cada atividade. Portanto, a proteção técnica contra ameaças cibernéticas é um limite inafastável para a conformidade legal.

No setor público, o tratamento de dados pessoais possui limites específicos baseados na legalidade e no interesse social. Segundo o artigo 23 da LGPD, as instituições estatais devem ser transparentes sobre as finalidades e práticas de suas atividades. O tratamento estatal deve restringir-se ao mínimo necessário para a execução de competências e serviços públicos. A fiscalização da ANPD estende-se aos órgãos do governo, visando evitar incidentes que comprometam a credibilidade estatal. Dessa forma, o Estado deve atuar como custodiante ético e transparente das informações da população.

Em conclusão, a eficácia regulatória na proteção da privacidade depende da integração entre limites legais e fiscalização estatal ativa. O marco regulatório da LGPD oferece os instrumentos necessários para garantir a transparência informacional no Brasil. O papel da ANPD é vital para transformar a norma em realidade cotidiana, apesar de enfrentar desafios burocráticos.

O reconhecimento constitucional do tema assegura que a privacidade prevaleça sobre lucros predatórios originados da mercantilização de dados. É imperativo que as organizações

brasileiras desenvolvam uma cultura de proteção de dados enraizada em princípios éticos. O fortalecimento da autoridade fiscalizadora e a educação da população são os caminhos para consolidar a dignidade humana no ciberespaço. Assim, o país avança na construção de um ambiente digital seguro e cidadão.

4. CONSIDERAÇÕES FINAIS

A transição acelerada para a sociedade da informação transformou a convivência digital em um ambiente de contínua exposição da intimidade e de vulnerabilidade dos indivíduos. A rotina conectada alimenta um fluxo massivo de dados pessoais que, interpretados por algoritmos sofisticados, convertem-se em bens de elevado valor comercial no mercado informacional. A constante coleta de dados insere o cidadão em uma arquitetura de redes que condiciona hábitos e fragiliza a percepção sobre os reais riscos dessa exposição. Esse cenário é agravado pela capacidade tecnológica de processamento de dados sensíveis e pelos recorrentes incidentes de segurança e vazamentos massivos que expõem os titulares a fraudes e danos morais. Diante dessa conjuntura, a proteção da privacidade consolida-se como garantia indispensável para a preservação da autonomia e da liberdade no ciberespaço.

A pesquisa evidenciou que as relações digitais são marcadas por uma profunda assimetria informacional entre as Big Techs e os usuários comuns. As plataformas exercem um controle opaco sobre os sistemas de processamento, utilizando ferramentas de inteligência artificial para monitorar o comportamento e modular escolhas de consumo sem a ciência efetiva do público. Além disso, a adesão a contratos por adesão e termos de uso extensos converteu o consentimento em mera ficção legal e ato mecânico de aceitação.

Esse panorama acentua o paradoxo da privacidade, no qual os indivíduos valorizam a proteção de seus dados, mas os cede rotineiramente em troca da conveniência de serviços ditos gratuitos. Assim, resta evidente que a tutela do cidadão não pode repousar apenas na autoproteção individual.

No âmbito normativo, a promulgação da Lei Geral de Proteção de Dados (LGPD — Lei nº 13.709/2018) e a promulgação da Emenda Constitucional nº 115/2022 representam avanços cruciais na ordem jurídica brasileira. Ao elevar a proteção de dados pessoais à categoria de direito fundamental autônomo, o constituinte derivado blindou a matéria e consagrou à autodeterminação informativa como aspecto central da dignidade humana. O marco regulatório impõe limites objetivos ao tratamento ao exigir obediência estrita aos princípios da finalidade, da transparência e, sobretudo, da necessidade ou limitação ao mínimo indispensável. Ademais, a legislação reservou proteção ainda mais rigorosa aos dados sensíveis, exigindo salvaguardas reforçadas devido ao seu elevado potencial discriminatório.

A instituição da Autoridade Nacional de Proteção de Dados (ANPD) como autarquia de natureza especial consolidou o pilar de fiscalização, normatização e sanção no país. O estudo ressalta que o papel da ANPD engloba a promoção do Privacy by Design e a aplicação de penalidades administrativas que podem alcançar até R\$ 50 milhões. Contudo, identificou-se que a autoridade enfrenta desafios para consolidar sua eficácia plena, marcados por um alcance sancionatório ainda modesto e por entraves burocráticos e comunicacionais.

Sob a ótica da conformidade corporativa e institucional, o trabalho demonstra que a proteção de dados deve ser incorporada à cultura organizacional como diferencial ético e estratégico. A implementação de programas de governança exige o mapeamento contínuo do ciclo de vida dos dados, abrangendo desde a coleta legítima até o descarte seguro e definitivo. No setor público, impõe-se a harmonização entre a transparência estatal exigida pela Lei de Acesso à Informação e a guarda rígida das bases de dados governamentais para evitar vazamentos em massa. Assim, o cumprimento do artigo 23 da LGPD exige que o Estado atue como custodiante ético dos dados dos cidadãos.

Conclui-se que a efetividade regulatória da privacidade no Brasil é um processo contínuo que demanda a integração de ferramentas jurídicas, tecnológicas e educativas. Diante da expansão acelerada da inteligência artificial e da mineração de dados, torna-se imperativo fortalecer a atuação fiscalizadora da ANPD e desburocratizar seus canais de denúncia. Além disso, a superação da vulnerabilidade do titular depende de investimentos permanentes em educação digital, permitindo o exercício consciente da autodeterminação informativa. Somente mediante a convergência entre o rigor punitivo estatal, a responsabilidade corporativa e o empoderamento do cidadão será possível assegurar a dignidade humana no ambiente virtual.

REFERÊNCIAS BIBLIOGRÁFICAS

BELLI, Lucca. **Governança digital e direitos fundamentais no ciberespaço**. Rio de Janeiro: FGV, 2025.

BERNARDO, Ana Julia et al. **10 anos da Lei de Acesso à Informação: de onde viemos e para onde vamos.** São Paulo: Artigo 19, 2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** 3. ed. Rio de Janeiro: Forense, 2021.

CARVALHO, Douglas Belchior de. **As Big Techs e a moderação de conteúdo eleitoral.** 2022. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Faculdade de Direito, Universidade Presbiteriana Mackenzie, São Paulo, 2022.

DONEDA, Danilo. **A proteção de dados como um direito fundamental.** Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

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

FREITAS, Juarez. **A interpretação sistemática do direito.** 5. ed. São Paulo: Malheiros, 2017.

GOMES, Giara Maria. **A coleta de dados pessoais pelas redes sociais digitais com impactos sobre a privacidade.** 2024. 75 f. Trabalho de Conclusão de Curso (Bacharelado em Biblioteconomia) – Centro de Humanidades, Universidade Federal do Ceará, Fortaleza, 2024.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Venceslau. Término do tratamento de dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados**

e suas repercussões no direito brasileiro. São Paulo: Revista dos Tribunais, 2023. p. 219-241.

HERSCOVICI, Alain. **Big data, rastreabilidade e assimetrias de informação: opacidade, ingerência e democracia.** Nova Economia, Belo Horizonte, v. 31, n. 3, p. 981-1010, set./dez. 2021. Disponível em: <https://doi.org/10.1590/0103-6351/6075>.

HRON, Martin. **Pesquisas em segurança de dispositivos e vulnerabilidade digital em vazamentos massivos.** In: Avast Security Research, 2019.

LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a efetividade da Lei Geral de Proteção de Dados.** São Paulo: Almedina, 2020.

LUZ, Pedro Henrique Machado da; LOREIRO, Maria Fernanda Battaglin. **Privacidade e proteção de dados pessoais: os novos desafios na sociedade em rede.** Meritum, Belo Horizonte, v. 13, n. 1, p. 69-86, jan./jun. 2018.

MARTINS, Marcelo Guerra; JORGETTO, Leonardo Felipe de Melo Ribeiro Gomes; SUTTI, Alessandra Cristina Arantes. **Big data e a proteção do direito à privacidade no contexto da sociedade da informação.** Revista Jurídica Cesumar, Maringá, v. 19, n. 3, p. 705-725, set./dez. 2019. Disponível em: <https://doi.org/10.17765/2176-9184.2019v19n3p705-725>.

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

MIRAGEM, Bruno. **Princípio da vulnerabilidade: perspectiva atual e funções no direito do consumidor contemporâneo.** In: MARQUES, Claudia Lima (org.). Direito do consumidor: 30 anos do CDC: da consolidação como direito fundamental aos atuais desafios da sociedade. Rio de Janeiro: Forense, 2020.

MOREIRA, Mayume Caires et al. **A aplicação da LGPD nas atividades empresariais: desafios, impactos e responsabilidades.** In: CONGRESSO DE DIREITO UNICESUMAR, 2., 2025, Maringá. Anais eletrônicos [...]. Maringá: UniCesumar, 2025. p. 284-293. ISBN 978-65-978610-0-2.

NASCIMENTO, Bruna Laís Campos do; SILVA, Edilene Maria da. **Lei Geral de Proteção de Dados (LGPD) e repositórios institucionais: reflexões e adequações.** Em Questão, Porto Alegre, v. 29, e-127314, 2023. DOI: <https://doi.org/10.1590/1808-5245.29.127314>. Disponível em: <https://doi.org/10.1590/1808-5245.29.127314>.

PAIVA, Thairone de Sousa; LANZILLO, Anderson Souza da Silva. **Proteção de dados pessoais no Brasil: os limites da regulamentação e da regulação da LGPD no constitucionalismo digital brasileiro.** Revista Controle, Fortaleza, v. 22, n. 1, p. 239-262, jan./jun. 2024.

PINHEIRO, Patrícia Peck. **#DireitoDigital.** 7. ed. São Paulo: Saraiva Jur, 2021.

PINTO, Isabela Rodrigues; DANIELETTI, Maria Augusta Grande. **A atuação da ANPD e os desafios estruturais para sua consolidação no Brasil.** Cadernos Jurídicos da FADI, [S. l.], v. 7, 2025.

PONTES, Marco Aurelio Muniz de; SILVA, Diogo Severino Ramos da. **A LGPD através da criptografia em empresas privadas: uma revisão da literatura.** Derecho y Cambio Social, v. 19, n. 70, p. 1-15, 2020.

SALESFORCE BRASIL. **Big Data: o que é, importância e exemplos.** [S. l.]: Salesforce Brasil Blog, 8 fev. 2024. Disponível em: <https://www.salesforce.com/br/blog/o-que-e-big-data/>. Acesso em: 4 jun. 2026.

SARLET, Ingo Wolfgang. **O direito à proteção de dados como um direito fundamental autônomo no Brasil.** 2021. (Obra referenciada conforme as citações diretas das fontes consultadas).

SOLOVE, Daniel J. **Understanding privacy.** Cambridge: Harvard University Press, 2009.

SOUSA, Rosilene Paiva Marinho de; BARRANCOS, Jacqueline Echeverría; MAIA, Manuela Eugênio. **Acesso à informação e ao tratamento de dados pessoais pelo poder público.** Informação & Sociedade: Estudos, João Pessoa, v. 29, n. 1, p. 237-251, 2019.

TAKAKU, Simone Rodrigues de Oliveira. **Os desafios associados à proteção dos titulares de dados nos contratos por adesão: uma análise do direito à privacidade diante da assimetria informacional do consumidor.** Brasília: IDP, 2022.

ZUBOFF, Shoshana. **The age of surveillance capitalism: the fight for a human future at the new frontier of power.** New York: PublicAffairs, 2018.

¹ Graduanda do curso de Direito pelo Centro Universitário de Goiatuba/Goiás (Unicerrado/GO).

² Doutora pelo Programa de Pós-Graduação em Sociologia e Direito da Universidade Federal Fluminense (PPGSD/UFF). Mestra em Direito Público pela Universidade Federal de Uberlândia (UFU). Docente efetiva do Curso de Direito do Centro Universitário de Goiatuba/Goiás (UniCerrado/GO).

³ O **Big Data** é conceituado como um termo que descreve o imenso volume e o complexo conjunto de dados gerados diariamente na sociedade digital, abrangendo informações coletadas de diversas fontes, como redes sociais e dispositivos conectados.

⁴ O termo **Big Techs** refere-se às grandes empresas de tecnologia que dominam setores específicos e cujos produtos e serviços são utilizados e comercializados em escala global.

⁵ A Telekall Infoservice, microempresa do ramo de telefonia com sede em Vila Velha (ES), tornou-se a primeira entidade a receber uma sanção pecuniária aplicada pela Autoridade Nacional de Proteção de Dados (ANPD) em julho de 2023. A condenação, no valor total de R\$ 14.400,00, decorreu de infrações aos artigos 7º e 41 da LGPD, referentes ao tratamento de dados pessoais sem base legal para fins de oferta de listas de contatos de WhatsApp em propaganda eleitoral e à ausência de indicação de um encarregado de dados (DPO).