FACULDADES INTEGRADAS ASMEC POUSO ALEGRE - MG

ROBERTO PROENÇA COSTA

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): AVANÇOS, DESAFIOS E IMPACTOS NO ORDENAMENTO JURÍDICO E NAS RELAÇÕES SOCIAIS NO BRASIL

POUSO ALEGRE - MG

2025

FACULDADES INTEGRADAS ASMEC POUSO ALEGRE - MG

ROBERTO PROENÇA COSTA

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): AVANÇOS, DESAFIOS E IMPACTOS NO ORDENAMENTO JURÍDICO E NAS RELAÇÕES SOCIAIS NO BRASIL

Trabalho de conclusão de curso apresentado no Curso de Direito da Faculdade de Negócios de Pouso Alegre, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Thiago Antônio Batista

POUSO ALEGRE - MG

2025

Costa, Roberto Proença.

A lei geral de proteção de dados pessoais (LGPD): avanços, desafios e impactos no ordenamento jurídico e nas relações sociais no Brasil

Roberto Proença Costa.
Orientação de Thiago Antônio Batista - Pouso Alegre - MG - 2025

Inclui bibliografias: P. 24

Trabalho de Conclusão de Curso (Faculdades Integradas ASMEC Unisepe).

FACULDADES INTEGRADAS ASMEC POUSO ALEGRE- MG
CURSO DE DIREITO

Discente
ROBERTO PROENÇA COSTA

Orientador
THIAGO ANTÔNIO BATISTA

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): AVANÇOS, DESAFIOS E IMPACTOS NO ORDENAMENTO JURÍDICO E NAS RELAÇÕES SOCIAIS NO BRASIL

Trabalho de conclusão de curso apresentado ao Curso de Direito da Faculdade Integrada ASMEC - Pouso Alegre - MG, como requisito parcial para obtenção do título de Bacharel em Direito.

Prof. Thiago Antônio Batista
Orientador

Avaliadora 1

Avaliador 2

Pouso Alegre/MG
2025

DEDICATÓRIA

A minha esposa e filhos e aos professores.

SUMÁRIO

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): AVANÇOS, DESAFIOS E IMPACTOS NO ORDENAMENTO JURÍDICO E NAS RELAÇÕES SOCIAIS NO BRASIL

Roberto Proença Costa[1]
Thiago Antônio Batista[2]

Resumo:
Este artigo analisa os principais aspectos da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), destacando seus fundamentos, princípios e implicações práticas para indivíduos, organizações e o Estado. Por meio de revisão bibliográfica e análise jurisprudencial, examina-se a atuação da Autoridade Nacional de Proteção de Dados (ANPD), os desafios de adequação enfrentados por empresas e órgãos públicos, e os reflexos da norma na tutela de direitos fundamentais, como a privacidade e a autodeterminação informativa. Os resultados indicam que, apesar de avanços significativos, persistem lacunas regulatórias e dificuldades de implementação, exigindo constante atualização normativa e cultural.

Palavras-chave: LGPD. Proteção de Dados. Privacidade. ANPD. Direito Digital.

Abstract:
This article analyzes the main aspects of the General Data Protection Law (Law No. 13,709/2018), highlighting its foundations, principles, and practical implications for individuals, organizations, and the State. Through a bibliographic review and jurisprudential analysis, it examines the role of the National Data Protection Authority (ANPD), the compliance challenges faced by companies and public agencies, and the law's impact on the protection of fundamental rights such as privacy and informational self-determination. The findings indicate that, despite significant progress, regulatory gaps and implementation difficulties persist, requiring constant normative and cultural updates.

Keywords: LGPD. Data Protection. Privacy. ANPD. Digital Law.

[1] Discente no curso de Direito da Faculdade de Negócios de Pouso Alegre/MG - ASMEC
[2] Docente no curso de Direito da Faculdade de Negócios de Pouso Alegre/MG - ASMEC

INTRODUÇÃO

A sociedade contemporânea vive imersa em uma transformação digital sem precedentes. O avanço acelerado das tecnologias da informação e da comunicação potencializou o uso da internet, das redes sociais, dos aplicativos e dos sistemas digitais em praticamente todas as esferas da vida social, econômica e política. Essa expansão trouxe consigo um volume crescente de dados pessoais coletados, processados e armazenados por empresas privadas, órgãos públicos e organizações da sociedade civil. Informações como nome, endereço, hábitos de consumo, dados financeiros, biométricos e de geolocalização passaram a constituir recursos estratégicos, convertendo-se em ativos de elevado valor econômico e político (Fernandes; Nuzzi, 2022; Medeiros, 2024).

Nesse contexto, emergiu a necessidade de uma legislação específica capaz de assegurar a proteção da privacidade e dos direitos fundamentais dos cidadãos frente à exploração indiscriminada de seus dados. Até a promulgação da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), o ordenamento jurídico brasileiro contava apenas com normas esparsas e setoriais sobre o tema, como o Código de Defesa do Consumidor (1990) e o Marco Civil da Internet (2014), insuficientes para enfrentar os novos desafios impostos pela economia digital (Medeiros, 2024).

Inspirada no Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR – General Data Protection Regulation), em vigor desde 2018, a LGPD foi concebida para uniformizar regras, definir princípios e estabelecer garantias para o tratamento de dados pessoais no Brasil. Sua finalidade primordial é equilibrar inovação tecnológica e desenvolvimento econômico com a tutela da privacidade e da autodeterminação informativa, assegurando ao titular maior controle sobre o fluxo de suas informações.

Todavia, desde sua entrada em vigor em 2020, a lei tem revelado desafios significativos quanto à sua implementação e efetividade. Questões como a adaptação de pequenas e médias empresas, a capacitação de profissionais especializados, a fragilidade da Autoridade Nacional de Proteção de Dados (ANPD) em seus primeiros anos de atuação e a baixa conscientização social sobre os direitos previstos na lei configuram obstáculos à sua plena consolidação (Pereira, 2024). Assim, o problema que se impõe é compreender de que maneira a LGPD vem sendo aplicada na prática e em que medida tem sido capaz de proteger efetivamente os direitos fundamentais dos cidadãos em meio à crescente digitalização das relações sociais e econômicas no Brasil.

2. REFERENCIAL TEÓRICO

2.1 Direito fundamental à privacidade e proteção de dados

O direito à privacidade no Brasil possui fundamento constitucional desde 1988, quando a Constituição Federal, em seu artigo 5º, incisos X e XII, assegurou a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, bem como o sigilo da correspondência, das comunicações telegráficas, de dados e telefônicas, salvo por ordem judicial em hipóteses legalmente previstas (Arantes, 2024; Medeiros, 2024). Trata-se de uma garantia essencial vinculada diretamente ao princípio da dignidade da pessoa humana (art. 1º, III), que busca proteger os indivíduos contra ingerências indevidas do Estado e de agentes privados.

Durante muitos anos, entretanto, a proteção de dados pessoais era tratada apenas de forma reflexa, por meio da tutela da privacidade e da intimidade. O advento da sociedade da informação, com a intensificação do uso de tecnologias digitais e a massificação do comércio eletrônico, tornou os dados pessoais um recurso estratégico, dotado de valor econômico e político, exigindo regulamentação específica. Nesse contexto, surgiram marcos normativos como o Código de Defesa do Consumidor (1990), que protege dados em cadastros de crédito, e o Marco Civil da Internet (2014), que estabelece princípios de privacidade e neutralidade da rede.

O reconhecimento do dado pessoal como direito fundamental autônomo foi fortalecido com a Emenda Constitucional nº 115/2022, que incluiu a proteção de dados expressamente no rol dos direitos fundamentais, acrescentando o inciso LXXIX ao art. 5º da Constituição. Esse movimento aproximou o Brasil de tendências internacionais, especialmente da União Europeia, que desde a Diretiva 95/46/CE e, mais recentemente, com o Regulamento Geral sobre a Proteção de Dados (GDPR), já reconhecia a proteção de dados como pilar democrático e requisito para o exercício da cidadania digital.

A proteção de dados pessoais no Brasil consolida-se como um direito fundamental, especialmente após a Emenda Constitucional nº 115/2022. Para Doneda (2019; 2020), essa conquista legislativa não se limita à salvaguarda da intimidade, mas constitui expressão da autodeterminação informativa, conferindo ao indivíduo o poder de controlar o fluxo de suas informações pessoais.

A doutrina brasileira (Doneda, 2019; 2020) tem sustentado que a proteção de dados transcende a simples guarda da intimidade, representando uma dimensão da chamada autodeterminação informativa, isto é, o poder do indivíduo de controlar o fluxo de suas

informações pessoais. Assim, dados pessoais não são apenas informações técnicas ou mercadológicas, mas extensões da personalidade humana, cuja manipulação indevida pode afetar liberdades individuais, oportunidades sociais e até mesmo a própria democracia.

Nesse sentido, a LGPD (Lei nº 13.709/2018) surge como um desdobramento normativo da proteção constitucional, consolidando a ideia de que a tutela jurídica de dados pessoais é condição para a efetividade do Estado Democrático de Direito e para a preservação dos direitos fundamentais na era digital.

2.2 Princípios da LGPD

A Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) – estabelece, em seu artigo 6º, um conjunto de princípios que norteiam o tratamento de dados pessoais no Brasil. Eles constituem parâmetros interpretativos obrigatórios, funcionando como balizas que limitam o poder das organizações e garantem ao titular maior previsibilidade quanto ao uso de suas informações.

A finalidade deve sempre estar vinculada a um propósito legítimo, específico e previamente informado ao titular. Isso evita práticas abusivas, como a coleta de informações "genéricas" que podem ser reutilizadas de forma indiscriminada. Exemplo prático: uma instituição financeira que solicita dados para abertura de conta não pode, posteriormente, utilizá-los para campanhas de marketing sem consentimento adicional.

A adequação exige que o tratamento esteja de acordo com o contexto em que os dados foram coletados, respeitando a relação entre finalidade e forma de utilização. Um dado fornecido para inscrição em concurso público, por exemplo, não pode ser compartilhado para fins comerciais, pois estaria em desacordo com a finalidade original. A necessidade impõe a limitação do tratamento ao mínimo indispensável. O princípio atua como antídoto contra a coleta excessiva, forçando os agentes de tratamento a justificarem a pertinência de cada dado. No comércio digital, por exemplo, não é razoável exigir o número do CPF para acessar meramente um catálogo de produtos online.

O livre acesso do titular deve ter a possibilidade de acompanhar o ciclo de vida de seus dados. Esse princípio garante não apenas a visualização, mas também a compreensão de como, por quem e por quanto tempo os dados são tratados. A efetivação do livre acesso exige mecanismos de comunicação acessíveis, como portais online de privacidade. A qualidade dos dados determina que os dados tratados sejam claros, exatos, relevantes e atualizados. A manutenção de registros incorretos pode gerar danos concretos, como negativa de crédito ou

erro em diagnósticos médicos. A jurisprudência recente tem reconhecido esse princípio ao condenar empresas que mantêm cadastros desatualizados, causando constrangimento ao consumidor.

A transparência obriga os agentes de tratamento a fornecerem informações inteligíveis sobre seus procedimentos, evitando linguagens técnicas de difícil compreensão. Segundo Doneda (2019), a transparência é o princípio que mais dialoga com o fortalecimento da cidadania digital, pois permite ao titular avaliar os riscos e decidir conscientemente sobre a entrega de seus dados. A segurança estabelece a adoção de medidas técnicas e administrativas adequadas para evitar acessos não autorizados, destruição, perda ou divulgação indevida de dados pessoais. Essa diretriz está diretamente ligada às práticas de segurança da informação, como criptografia, controle de acessos e políticas de backup.

A prevenção complementa o princípio da segurança ao enfatizar a adoção de medidas proativas. Em vez de reagir apenas após incidentes de vazamento, a LGPD exige que organizações implementem mecanismos preventivos, como avaliações de impacto e auditorias periódicas. A responsabilização e prestação de contas (accountability), indica que os agentes de tratamento devem demonstrar não apenas a conformidade formal, mas a eficácia das medidas adotadas. Esse princípio reflete a lógica contemporânea da governança corporativa: não basta cumprir a lei, é preciso comprovar a efetividade das práticas de proteção de dados.

A doutrina ressalta que tais princípios não são meramente enunciativos, mas normas jurídicas vinculantes que balizam tanto a interpretação judicial quanto à atuação administrativa da Autoridade Nacional de Proteção de Dados (ANPD). Eles traduzem o esforço legislativo em harmonizar dois pólos em tensão: de um lado, o livre fluxo de informações em uma economia digitalizada; de outro, a proteção da esfera privada e a dignidade da pessoa humana.

Em termos práticos, a aplicação desses princípios tem inspirado decisões judiciais que reconhecem a responsabilidade objetiva de empresas em casos de vazamentos ou usos abusivos de dados, mesmo quando não há demonstração explícita de culpa. Trata-se de uma leitura que reforça a função pedagógica da LGPD, buscando consolidar uma cultura de privacidade no Brasil.

2.3 Jurisprudência inicial sobre tratamento irregular de dados

Desde a entrada em vigor plena da LGPD, em setembro de 2020, o Poder Judiciário brasileiro passou a ser instado a decidir sobre situações envolvendo tratamento irregular de

dados pessoais. As primeiras demandas ajuizadas concentraram-se em casos de vazamentos de informações, uso indevido para fins de marketing e compartilhamento sem consentimento, refletindo o crescimento de incidentes de segurança noticiados no país.

Em linhas gerais, os tribunais têm reconhecido a responsabilidade civil dos agentes de tratamento, aplicando o artigo 42 da LGPD, que impõe a reparação de danos materiais e morais sempre que houver violação à legislação de proteção de dados. Essa disposição dialoga com o Código de Defesa do Consumidor e com a própria Constituição Federal, que consagram a tutela da intimidade, da privacidade e da dignidade da pessoa humana.

Diversas decisões, tanto em juizados especiais quanto em tribunais estaduais, têm reconhecido que a mera exposição de dados pessoais já caracteriza dano moral presumido, independentemente de comprovação de prejuízo econômico. Por exemplo, em casos de inclusão indevida de consumidores em cadastros restritivos de crédito ou de envio massivo de e-mails publicitários sem consentimento, os juízes têm fixado indenizações por violação da autodeterminação informativa. Em alguns julgados, o valor fixado variou de R$ 3.000,00 a R$ 10.000,00, de acordo com a gravidade da falha e a condição econômica do ofensor.

A jurisprudência também vem enfrentando situações complexas de vazamentos em larga escala, muitas vezes envolvendo bancos de dados de órgãos públicos ou empresas de grande porte. Em 2021, por exemplo, tribunais reconheceram a possibilidade de indenização coletiva a consumidores em razão de falhas de segurança que expuseram informações de milhões de brasileiros. Nessas hipóteses, a discussão judicial tem girado em torno da necessidade de comprovação do dano concreto ou da adoção da teoria do risco da atividade, que responsabiliza objetivamente o agente de tratamento pela violação, conforme previsto no artigo 44 da LGPD.

Outro ponto relevante diz respeito ao papel da Autoridade Nacional de Proteção de Dados (ANPD). Embora sua atuação inicial tenha sido mais orientativa, alguns tribunais já vêm utilizando pareceres e guias da ANPD como parâmetros de interpretação. Isso reforça o caráter dinâmico da jurisprudência, que tende a se consolidar a partir da interação entre decisões judiciais, doutrina especializada e normativos expedidos pelo órgão regulador.

Não obstante os avanços, há desafios significativos. Ainda não há uniformidade quanto aos critérios para fixação do valor das indenizações e tampouco consenso sobre a extensão da responsabilidade de controladores e operadores em casos de falhas de terceiros. Em alguns julgados, prevaleceu a responsabilidade objetiva do controlador, enquanto outros admitiram excludentes previstas no artigo 43 da LGPD, como a comprovação de que o dano decorreu de culpa exclusiva do titular ou de terceiros.

Em síntese, a jurisprudência inicial demonstra uma postura protetiva e pedagógica, buscando desestimular práticas abusivas e incentivar a implementação de programas de compliance digital, políticas de segurança da informação e capacitação de colaboradores. Contudo, a consolidação de entendimentos uniformes pelo Superior Tribunal de Justiça (STJ) e, futuramente, pelo Supremo Tribunal Federal (STF), será decisiva para a efetividade plena da LGPD no ordenamento jurídico brasileiro.

3. METODOLOGIA

O presente artigo adota uma abordagem qualitativa e exploratória, centrada na revisão bibliográfica e documental acerca da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) e suas repercussões no ordenamento jurídico e nas relações sociais no Brasil.

A escolha metodológica fundamenta-se no método dedutivo, partindo da análise das normas constitucionais e infraconstitucionais que estruturam o direito fundamental à privacidade e à proteção de dados, seguido do exame empírico de produções acadêmicas, relatórios oficiais da Autoridade Nacional de Proteção de Dados (ANPD) e jurisprudências iniciais sobre tratamento irregular de dados pessoais.

O corpus da pesquisa foi delimitado por meio de levantamento realizado em bases acadêmicas e científicas, especialmente o Google Acadêmico e os Periódicos CAPES, utilizando como palavra-chave principal: “A Lei Geral de Proteção de Dados Pessoais (LGPD): Avanços, Desafios e Impactos no Ordenamento Jurídico e nas Relações Sociais no Brasil”.

Em complemento, foram empregados descritores correlatos como Impacto LGPD, Importância LGPD, Proteção de dados e GDPR, a fim de ampliar o alcance dos resultados.

Os critérios de inclusão das obras analisadas consideraram:

- publicações acadêmicas com abordagem direta da LGPD;
- textos que discutem os princípios do art. 6º da lei, os direitos dos titulares e a responsabilização de agentes;
- estudos que tratam das sanções e da atuação da ANPD;
- trabalhos que estabelecem paralelos comparativos com o Regulamento Geral de Proteção de Dados (GDPR).

Como critérios de exclusão, foram desconsiderados textos opinativos sem embasamento técnico-jurídico, duplicatas e materiais sem aderência temática.

A análise dos dados seguiu uma lógica interpretativo-descritiva, buscando identificar padrões argumentativos na literatura, apontar convergências e divergências doutrinárias e mapear decisões judiciais que fixam indenizações por danos decorrentes de vazamento ou uso irregular de dados. O enfoque recaiu sobre os fundamentos jurídicos, os efeitos práticos da aplicação da LGPD em organizações públicas e privadas e a conformidade com padrões internacionais de proteção de dados.

A metodologia adotada visa, portanto, compreender a LGPD como marco regulatório brasileiro, analisando seus avanços, desafios de implementação e impactos sociais, bem como contribuir para o debate acadêmico acerca da consolidação do direito fundamental à proteção de dados no país.

4. DESENVOLVIMENTO

4.1. Contexto Histórico da LGPD

O debate em torno da proteção da privacidade e dos dados pessoais ganhou força no Brasil a partir dos anos 2000, com a intensificação do uso da internet, das redes sociais e do comércio eletrônico. A crescente digitalização da sociedade transformou os dados em recursos estratégicos de valor econômico e político, expondo os cidadãos a riscos como fraudes, monitoramento abusivo, vazamentos em massa e uso indevido de informações pessoais (Oliveira; Monteiro, 2024).

Antes da edição da LGPD, a legislação brasileira já oferecia proteções pontuais, mas fragmentadas. O Código de Defesa do Consumidor (1990) tratava da proteção de informações em cadastros de crédito; a Lei do Cadastro Positivo (2011) regulava a utilização de dados financeiros; a Lei de Acesso à Informação (2011) reforçava a transparência na administração pública; e o Marco Civil da Internet (2014) estabelecia princípios gerais para o uso da rede, incluindo garantias relacionadas à privacidade e à neutralidade. Contudo, não havia um diploma normativo abrangente e sistemático que unificasse princípios, direitos e deveres no tratamento de dados pessoais.

A experiência internacional foi determinante para a formulação da legislação nacional. Em especial, o Regulamento Geral sobre a Proteção de Dados (GDPR), aprovado pela União Europeia em 2016 e em vigor desde 2018, tornou-se referência global ao instituir padrões rígidos de consentimento, transparência, proporcionalidade e responsabilização. Esse

regulamento estabeleceu que apenas países com legislação equivalente poderiam manter fluxos internacionais de dados com a União Europeia, o que pressionou o Brasil a acelerar sua própria regulação, sob pena de restrições em transações econômicas e tecnológicas.

Como observa Doneda (2019; 2020), a LGPD representa um avanço normativo comparável ao GDPR europeu, pois institucionaliza no ordenamento jurídico brasileiro princípios universais de privacidade e de limitação do uso dos dados, estruturando uma nova cultura jurídica voltada à transparência e à confiança digital.

No Brasil, a tramitação da LGPD foi marcada pela forte mobilização da sociedade civil, de entidades empresariais e de especialistas em direito digital. O escândalo internacional da Cambridge Analytica, envolvendo o uso indevido de dados de milhões de usuários do Facebook, intensificou a percepção da urgência de uma lei específica e contribuiu para a rápida aprovação do texto final em 2018.

Assim, foi sancionada a Lei nº 13.709/2018, estabelecendo princípios, direitos e deveres para o tratamento de dados pessoais por pessoas físicas, empresas e órgãos públicos. A lei foi posteriormente alterada pela Lei nº 13.853/2019, que criou a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por zelar pela aplicação da LGPD (Medeiros, 2024).

Inicialmente prevista para entrar em vigor em 2020, sua plena aplicação ocorreu em setembro de 2020, após adiamentos relacionados à pandemia de COVID-19. As sanções administrativas, por sua vez, passaram a ser aplicadas somente a partir de agosto de 2021, em respeito ao período de adaptação concedido às organizações.

A aprovação da LGPD representou, portanto, não apenas um avanço normativo interno, mas também a inserção do Brasil em um cenário internacional que reconhece a proteção de dados como requisito indispensável para a economia digital, a competitividade global e a preservação da cidadania na era da informação.

4.2. Estrutura e Aplicabilidade da Lei

A LGPD organiza-se em torno de conceitos fundamentais, princípios, direitos e deveres que orientam o tratamento de dados pessoais em todo o território nacional. Ao definir dado pessoal como qualquer informação que identifique ou possa identificar uma pessoa natural, a lei abrange desde dados triviais, como nome, endereço e CPF, até informações mais sofisticadas, como geolocalização, histórico de navegação e identificadores eletrônicos. Essa definição ampla garante que mesmo dados aparentemente neutros, quando combinados,

possam ser protegidos, já que possibilitam a identificação indireta do indivíduo (Medeiros, 2024).

Além disso, a lei distingue os dados sensíveis, cuja natureza requer proteção especial. Incluem-se nessa categoria informações que possam revelar origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dados referentes à saúde, vida sexual, bem como dados genéticos e biométricos. Esses dados exigem bases legais mais restritivas e consentimento específico, dada a possibilidade de discriminação ou violação grave de direitos fundamentais (Coelho, 2023; Fernandes; Nuzzi, 2022).

No que se refere aos direitos dos titulares, o artigo 18 da LGPD representa um marco ao consolidar a chamada autodeterminação informativa. Entre os principais direitos assegurados estão:

- a confirmação da existência de tratamento, possibilitando ao cidadão saber se seus dados estão sendo coletados e usados;
- o acesso aos dados, incluindo sua origem, finalidade e destinatários;
- a correção de dados incompletos ou desatualizados;
- a anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos;
- a portabilidade dos dados a outro fornecedor de serviço;
- a informação sobre compartilhamento de dados com terceiros;
- e a revisão de decisões automatizadas, especialmente relevantes diante do avanço da inteligência artificial e de algoritmos preditivos (Pereira, 2024; Fernandes; Nuzzi, 2022).

Esses direitos fortalecem a cidadania digital, colocando o indivíduo no centro do processo decisório e exigindo das organizações transparência e responsabilidade no uso das informações. Doneda (2019) ressalta que a positivação desses direitos marca a transição de um modelo baseado apenas em obrigações contratuais e de consumo para um regime de direito fundamental autônomo, no qual o cidadão é sujeito ativo da proteção de seus dados.

No âmbito da operacionalização, a LGPD define dois principais agentes de tratamento: o controlador, responsável por tomar as decisões sobre a coleta, armazenamento e uso de dados, e o operador, que executa o tratamento em nome do controlador. Ambos têm deveres específicos e podem ser responsabilizados solidariamente em caso de incidentes ou danos causados a titulares. Essa lógica busca garantir que todos os envolvidos no ciclo de vida dos dados estejam submetidos a regras claras de responsabilidade.

Para coordenar e fiscalizar a aplicação da lei, foi criada a Autoridade Nacional de Proteção de Dados (ANPD) pela Lei nº 13.853/2019. A ANPD é responsável por editar regulamentos e orientações técnicas, aplicar sanções administrativas (advertências, multas de até 2% do faturamento, bloqueio ou eliminação de dados, suspensão de atividades), além de atuar em campanhas de conscientização e na promoção da cultura de privacidade. Sua atuação tem sido fundamental na mediação entre inovação tecnológica e proteção de direitos, tornando-se referência para empresas, órgãos públicos e cidadãos (Fernandes; Nuzzi, 2022).

É importante ressaltar que a LGPD tem aplicabilidade extraterritorial, ou seja, estende-se a qualquer operação de tratamento de dados realizada no Brasil ou que tenha por objetivo ofertar bens e serviços a pessoas localizadas no território nacional, ainda que o controlador ou operador esteja situado fora do país. Essa previsão amplia a efetividade da lei e alinha o Brasil aos padrões internacionais estabelecidos pelo GDPR (Oliveira; Monteiro, 2024).

Assim, a estrutura da LGPD combina elementos normativos e institucionais capazes de resguardar os dados pessoais como bens jurídicos essenciais, reforçando a proteção da privacidade, a dignidade da pessoa humana e a confiança social na economia digital.

4.3. Desafios de Implementação

Apesar de representar um avanço legislativo sem precedentes no país, a LGPD enfrenta obstáculos significativos em sua efetiva implementação, revelando a distância entre a previsão normativa e a realidade organizacional brasileira.

Um dos principais entraves são os custos de adequação, especialmente para pequenas e médias empresas (PMEs). A conformidade exige investimentos em infraestrutura tecnológica, revisão de contratos, auditorias de processos internos, treinamento de colaboradores e contratação de especialistas em proteção de dados. Enquanto grandes corporações dispõem de equipes multidisciplinares e orçamento para criar programas robustos de compliance, muitas PMEs não possuem recursos financeiros ou know-how suficientes, tornando a adequação um fardo desproporcional (Mendanha et al., 2025). Essa desigualdade pode gerar uma competitividade assimétrica, em que apenas empresas mais estruturadas conseguem alinhar-se às exigências legais, enquanto pequenos negócios ficam vulneráveis a sanções e à perda de credibilidade no mercado.

Outro desafio relevante é a cultura organizacional. Muitas empresas brasileiras ainda veem a proteção de dados como uma obrigação burocrática, e não como uma política

estratégica. Essa visão reducionista faz com que medidas sejam adotadas apenas de forma superficial, sem transformar práticas internas ou envolver gestores e colaboradores em uma cultura de privacidade e segurança. A falta de profissionais especializados, como o Encarregado de Proteção de Dados (DPO), agrava a situação: embora a LGPD exija a designação desse responsável, o mercado ainda não dispõe de mão de obra qualificada suficiente para atender à alta demanda (Coelho, 2023).

Além disso, a segurança da informação permanece como um dos maiores gargalos. O Brasil está entre os países que mais sofrem com ataques cibernéticos, o que amplia os riscos de vazamentos em larga escala. Casos de exposição de milhões de dados de usuários em serviços digitais e de instituições públicas reforçam a vulnerabilidade do ecossistema informacional brasileiro. Esses incidentes não apenas comprometem a confiança do consumidor, mas também geram danos reputacionais irreparáveis, ações judiciais e a possibilidade de sanções severas pela ANPD, incluindo multas milionárias e restrições de operação (Fernandes; Nuzzi, 2022).

A ausência de conscientização da população também figura como um desafio estrutural. Grande parte dos titulares de dados ainda desconhece seus direitos previstos no artigo 18 da LGPD, como o de exigir a exclusão de informações, questionar decisões automatizadas ou solicitar a portabilidade de seus dados. Essa lacuna informacional fragiliza a efetividade da lei, pois o exercício dos direitos depende, em grande medida, do conhecimento e da atuação ativa do cidadão (Pereira, 2024).

Por fim, deve-se considerar que a implementação da LGPD exige uma articulação contínua entre tecnologia, governança corporativa e política pública. Sem investimentos em educação digital, campanhas de conscientização, incentivo governamental às pequenas empresas e fortalecimento da Autoridade Nacional de Proteção de Dados (ANPD), a lei corre o risco de permanecer como um marco normativo de alto valor simbólico, mas de aplicação desigual e limitada na prática.

4.4. Impactos Sociais e Jurídicos

A LGPD trouxe impactos expressivos tanto nas relações privadas quanto no setor público. No plano social, houve uma mudança significativa na relação entre consumidores e empresas, uma vez que os titulares passaram a exigir maior clareza, segurança e justificativa sobre a utilização de suas informações pessoais. Essa alteração reforçou a ideia de que a privacidade não é apenas um direito individual, mas também um elemento de cidadania

digital, capaz de influenciar decisões de consumo. Cada vez mais, a proteção de dados passou a ser percebida como um diferencial competitivo, fortalecendo a confiança do cliente e agregando valor à marca (Sell; Trindade, 2024).

Do ponto de vista organizacional, a lei impulsionou a adoção de novas práticas de governança e compliance. As empresas precisaram implementar políticas de privacidade mais acessíveis e transparentes, elaborar Relatórios de Impacto à Proteção de Dados Pessoais (RIPD), criar protocolos de segurança para incidentes e desenvolver canais de atendimento direto ao titular. Essas medidas, antes vistas como custos adicionais, hoje são incorporadas como ativos estratégicos de gestão, pois contribuem para a reputação da empresa, para a fidelização de clientes e para a prevenção de litígios judiciais (Mendanha et al., 2025).

No âmbito jurídico, a LGPD consolidou um regime robusto de responsabilidade civil e administrativa. O artigo 42 da lei prevê a reparação de danos materiais e morais, individuais e coletivos, decorrentes de violações de dados pessoais, estabelecendo inclusive a possibilidade de responsabilidade solidária entre controladores e operadores. Além disso, a ANPD ganhou poder para aplicar sanções administrativas que variam de advertências a multas de até 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração, além de bloqueio e eliminação de dados ou mesmo suspensão das atividades de tratamento (Coelho, 2023). Esses mecanismos representam um avanço em termos de efetividade regulatória, ainda que a jurisprudência esteja em fase inicial de consolidação, com decisões pontuais reconhecendo indenizações por danos morais mesmo sem prejuízo material direto.

No setor público, os reflexos da LGPD no governo digital são profundos. Órgãos da administração passaram a ser pressionados a adotar medidas de segurança da informação e protocolos de privacidade, especialmente em áreas sensíveis como saúde, educação e segurança pública. A digitalização acelerada de serviços durante a pandemia de COVID-19 tornou ainda mais urgente a adequação das bases de dados governamentais. Em instituições de saúde, por exemplo, o tratamento de dados sensíveis de pacientes exige rigor redobrado, sob pena de exposição de informações extremamente pessoais e discriminatórias (Pereira, 2024).

Além disso, a LGPD fortalece a democracia informacional ao exigir que o poder público seja transparente no uso e compartilhamento de dados pessoais, ao mesmo tempo em que protege os cidadãos contra práticas abusivas. Esse movimento aproxima o Brasil das melhores práticas internacionais e cria condições para que a confiança do cidadão nos serviços públicos digitais seja reforçada, reduzindo a percepção de arbitrariedade e aumentando a legitimidade do Estado no uso de informações pessoais (Medeiros, 2024).

Assim, observa-se que a LGPD não apenas alterou práticas empresariais e governamentais, mas também reconfigurou a cultura jurídica e social em torno da privacidade e da proteção de dados, elevando o tema ao centro do debate sobre cidadania, inovação tecnológica e direitos fundamentais.

CONSIDERAÇÕES FINAIS

A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) representou um marco jurídico e social no Brasil, ao consolidar a proteção da privacidade e dos dados pessoais como um direito fundamental. Inspirada no Regulamento Europeu (GDPR), a lei buscou alinhar o país às melhores práticas internacionais, estabelecendo princípios, direitos e deveres claros para indivíduos, empresas e órgãos públicos.

Ao longo deste estudo, foi possível verificar que a LGPD trouxe avanços expressivos, sobretudo ao reconhecer a autodeterminação informativa como eixo central da cidadania digital, ao criar mecanismos de responsabilização e ao instituir a Autoridade Nacional de Proteção de Dados (ANPD) como órgão regulador e fiscalizador.

No entanto, também se evidenciaram desafios relevantes em sua implementação. Os custos de adequação para pequenas e médias empresas, a carência de profissionais especializados, a ausência de uma cultura organizacional voltada à privacidade e os frequentes casos de ataques cibernéticos e vazamentos de dados indicam que ainda há um longo caminho para a efetivação plena da lei.

Do ponto de vista social e econômico, a LGPD alterou a forma como os cidadãos se relacionam com empresas e com o próprio Estado, fazendo da proteção de dados um diferencial competitivo e um requisito de legitimidade democrática. No setor público, a exigência de maior transparência e segurança no tratamento de dados reforçou a confiança do cidadão nos serviços digitais, contribuindo para o fortalecimento da democracia informacional.

Assim, pode-se concluir que a LGPD constitui não apenas um marco legislativo, mas também um instrumento transformador da cultura jurídica e social brasileira, ao promover maior equilíbrio entre inovação tecnológica, desenvolvimento econômico e salvaguarda de direitos fundamentais.

Para que a lei cumpra integralmente sua finalidade, é imprescindível o fortalecimento contínuo da ANPD, a ampliação de políticas de educação digital e a difusão de práticas de governança de dados em todos os setores da sociedade. Apenas com esse esforço conjunto,

envolvendo Estado, empresas e cidadãos, será possível consolidar uma cultura de proteção de dados que garanta confiança, segurança e dignidade na era digital.

REFERÊNCIAS BIBLIOGRÁFICAS

ARANTES, Gustavo Luciano Santos. **A Lei Geral de Proteção de Dados e o Direito à Privacidade**: limite ao acesso de dados. TCC (Bacharel em Direito), Faculdade de Direito da Universidade Federal de Uberlândia/UFU, Uberlândia/MG, 2024.

COELHO, Randys Machado. **Protegendo a Privacidade dos Dados Pessoais no Brasil**: Análise da Lei de Proteção dos Dados (LGPD). TCC (Bacharelado em Sistemas de Informação): Universidade Estadual de Goiás, Curso de Sistemas de Informação, Porangatu/GO, 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. A proteção de dados pessoais como direito fundamental. **Revista de Direito Administrativo**, Rio de Janeiro, v. 280, n. 1, p. 259-278, 2020.

FERNANDES, Marcelo Eloy; NUZZI, Ana Paula Eloy. Fundamentos da Lei Geral de Proteção de Dados (LGPD): uma revisão narrativa. **Research, Society and Development**, v. 11, n. 12, e310111234247, 2022.

MEDEIROS, Niâni Guimarães Lima de. A Evolução da Proteção de Dados no Brasil: uma Análise Histórica e Legislativa até o Advento da LGPD. **Ciências Jurídicas**, v. 25, n. 2, p. 86-91, 2024.

MENDANHA, Daniel Silva et al. Impactos da Lei Geral de Proteção de Dados (LGPD) no Comércio Digital no Brasil. **Nativa – Revista de Ciências Sociais do Norte de Mato Grosso**, v. 2, n. 1, 2025.

OLIVEIRA, Rodrigo de; MONTEIRO, Michael Lemes. A Proteção de Dados Pessoais no Brasil: impacto e implicações da LGPD. In: ESTALD, Amanda de Souza et. al. **Rumo à conexão integral**: explorando fronteiras multidisciplinares. Belo Horizonte - MG: Editora Poisson, 2024, p. 56-66.

PEREIRA, Victor Schlichting. **Impactos da LGPD na Sociedade Brasileira**. Goiânia/GO: Pontifícia Universidade Católica de Goiás, Escola de Direito e Relações Internacionais, 2024.

SELL, Luis Cesar; TRINDADE, Rangel Oliveira. Impactos na Privacidade, Segurança e Confiança nas Relações Digitais nas Empresas: Desafios e Perspectivas na Era da Lei Geral de Proteção de Dados (Lei N. 13.709/2018). **DIREITO EM REVISTA**, n. 37, p. 185–222, 2025. Disponível em: https://www.revistas.cesul.br/rdr/article/view/9. Acesso em: 3 set. 2025.