

# A IMPLEMENTAÇÃO DA LGPD NO CENÁRIO EMPRESARIAL BRASILEIRO: DESAFIOS JURÍDICOS E ESTRATÉGIAS DE COMPLIANCE

THE IMPLEMENTATION OF THE LGPD IN THE BRAZILIAN BUSINESS  
ENVIRONMENT: LEGAL CHALLENGES AND COMPLIANCE STRATEGIES

Ciências Sociais Aplicadas • 14/06/2026

REGISTRO DOI: [10.70773/revistatopicos/781462764](https://doi.org/10.70773/revistatopicos/781462764)

Bob Marley Veras Mouta<sup>1</sup>

Luis Antonio da Silva Barros<sup>2</sup>

Rossana Barros<sup>3</sup>

## RESUMO

**Introdução:** A crescente digitalização das relações sociais, econômicas e empresariais intensificou a circulação de dados pessoais, tornando indispensável a criação de mecanismos jurídicos voltados à proteção da privacidade e da autodeterminação informativa dos indivíduos. Nesse contexto, a Lei Geral de Proteção de Dados Pessoais consolidou-se como importante instrumento de regulamentação do tratamento de dados pessoais no Brasil.

**Objetivo:** analisar os principais aspectos da LGPD na atuação das empresas brasileiras, especialmente quanto aos desafios relacionados à implementação prática da proteção de dados pessoais. **Materiais e Método:** A pesquisa caracteriza-se como bibliográfica, de natureza qualitativa e abordagem descritiva, sendo desenvolvida a partir da análise de legislações, doutrinas, artigos científicos e produções acadêmicas relacionadas à proteção de dados, privacidade, governança corporativa e compliance digital.

**Resultados:** Os resultados demonstram que muitas empresas ainda enfrentam dificuldades relacionadas à interpretação da legislação, adaptação tecnológica, ausência de cultura organizacional voltada à privacidade e limitação de recursos técnicos e financeiros, especialmente nas micro e pequenas empresas. Observou-se também que programas de compliance, políticas de governança de dados, treinamentos internos e mecanismos de segurança da informação contribuem significativamente para a redução de riscos jurídicos, financeiros e reputacionais. **Contribuição Científica:** O estudo contribui para o aprofundamento do debate acadêmico acerca da proteção de dados pessoais no Brasil, evidenciando a importância da integração entre Direito, tecnologia e gestão organizacional na consolidação de práticas empresariais éticas e compatíveis com os direitos fundamentais.

**Conclusão:** Conclui-se que a efetividade da LGPD depende não apenas da existência de

normas jurídicas, mas também da construção de uma cultura corporativa pautada na transparência, responsabilidade e respeito à privacidade, transformando a proteção de dados em elemento estratégico para a sustentabilidade e credibilidade das empresas na sociedade digital contemporânea.

**Palavras-chave:** LGPD; Proteção de Dados; Compliance Digital.

## **ABSTRACT**

**Introduction:** The growing digitization of social, economic, and business relationships has intensified the circulation of personal data, making it essential to establish legal mechanisms aimed at protecting individuals' privacy and informational self-determination. In this context, the General Personal Data Protection Law (LGPD) has established itself as an important regulatory instrument for the processing of personal data in Brazil. **Objective:** To analyze the main impacts of the LGPD on the operations of Brazilian companies, particularly regarding the challenges related to the practical implementation of personal data protection. **Materials and Method:** This study is a bibliographic, qualitative research with a descriptive approach, based on the analysis of legislation, legal doctrine, scientific articles, and academic works related to data protection, privacy, corporate governance, and digital compliance. **Results:** The results demonstrate that many companies still face difficulties related to the interpretation of legislation, technological adaptation, the absence of an organizational culture focused on privacy, and limited technical and financial resources, especially in micro and small enterprises. It was also observed that compliance programs, data governance policies, internal training, and information security mechanisms contribute significantly to reducing legal, financial, and reputational risks. **Scientific Contribution:** This study contributes to the academic debate on personal data protection in Brazil,

highlighting the importance of integrating law, technology, and organizational management to establish ethical business practices that are consistent with fundamental rights. **Conclusion:** It is concluded that the effectiveness of the LGPD depends not only on the existence of legal norms but also on the development of a corporate culture grounded in transparency, accountability, and respect for privacy, transforming data protection into a strategic element for the sustainability and credibility of companies in contemporary digital society.

**Keywords:** LGPD; Data Protection; Digital Compliance.

## 1. INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais representou um marco relevante no ordenamento jurídico brasileiro ao estabelecer regras específicas para a coleta, o tratamento, o armazenamento e o compartilhamento de dados pessoais. Mais do que uma legislação de caráter burocrático, a LGPD consolidou a compreensão de que os dados pessoais estão diretamente relacionados à dignidade da pessoa humana e aos direitos fundamentais da personalidade (Galdino; Faria, 2021).

A construção normativa da proteção de dados no Brasil não ocorreu de maneira imediata, mas resultou de um processo gradual de evolução constitucional e legislativa. A Constituição da República Federativa do Brasil de 1988 já assegurava, em seu artigo 5º, os direitos à intimidade, à vida privada e à inviolabilidade das comunicações (Brasil, 1988). Posteriormente, o Marco Civil da Internet fortaleceu a disciplina jurídica do ambiente digital ao estabelecer princípios relacionados à privacidade, à proteção de dados e à responsabilidade no uso da internet.

Diante desse cenário, as empresas brasileiras passaram a enfrentar o desafio de adequar suas estruturas internas às exigências impostas pela LGPD. A implementação da legislação não se resume à elaboração formal de documentos ou políticas internas, mas exige mudanças organizacionais, culturais e tecnológicas voltadas à criação de práticas efetivas de governança de dados. As organizações que adotam medidas transparentes e éticas no tratamento de informações pessoais tendem a fortalecer a confiança dos consumidores e a obter vantagem competitiva no mercado. Assim, surge o seguinte problema de pesquisa: de que maneira a LGPD tem impactado a atuação das empresas brasileiras e quais são os principais desafios enfrentados na implementação efetiva da proteção de dados pessoais no ambiente corporativo?

O objetivo geral deste estudo consiste em analisar os impactos principais aspectos da LGPD na atuação das empresas brasileiras, especialmente quanto aos desafios relacionados à implementação prática da proteção de dados pessoais. Como objetivos específicos, busca-se compreender a evolução histórica e jurídica da proteção de dados no Brasil; examinar os impactos da legislação de proteção de dados nas práticas empresariais; e identificar as estratégias de compliance voltadas à adequação e à efetividade da proteção de dados pessoais no ambiente corporativo.

Quanto à metodologia, a pesquisa caracteriza-se como bibliográfica, de natureza qualitativa e abordagem descritiva, sendo desenvolvida a partir da análise de livros, artigos científicos, legislações e produções doutrinárias relacionadas à proteção de dados pessoais, privacidade e direito digital. O estudo fundamenta-se em autores nacionais e estrangeiros que discutem os efeitos jurídicos e sociais

da transformação digital e da tutela dos dados pessoais no contexto contemporâneo.

A relevância deste trabalho justifica-se pela crescente importância da proteção de dados na sociedade da informação e pela necessidade de compreender os impactos jurídicos, econômicos e sociais decorrentes da aplicação da LGPD no Brasil. Além de contribuir para o aprofundamento do debate acadêmico sobre privacidade e direito digital, o estudo também possui relevância prática, considerando que a adequação à legislação pode representar não apenas o cumprimento de uma obrigação legal, mas também um diferencial competitivo para empresas que buscam fortalecer a confiança dos consumidores e aprimorar seus processos internos de governança e segurança da informação.

## **2. RESULTADOS E DISCUSSÕES**

### **2.1. Fundamentos Jurídicos da Proteção de Dados e a LGPD no Brasil**

#### **2.1.1. Conceitos Fundamentais da Proteção de Dados Pessoais e da Privacidade**

A proteção de dados pessoais tornou-se um dos principais temas do Direito contemporâneo em razão da crescente digitalização das relações sociais, econômicas e institucionais. A Lei Geral de Proteção de Dados Pessoais estabelece que dado pessoal é toda informação relacionada à pessoa natural identificada ou identificável, abrangendo não apenas elementos tradicionais, como nome e CPF, mas também dados de localização, hábitos de consumo, registros eletrônicos e informações de navegação na internet (LGPD, art. 5º).

Já o tratamento de dados compreende qualquer operação realizada com essas informações, incluindo coleta, armazenamento, compartilhamento, utilização, eliminação e transferência. (LGPD, art. 5º, inciso X). Nesse contexto, a legislação busca assegurar que o uso dessas informações ocorra de maneira transparente, legítima e compatível com os direitos fundamentais dos titulares.

A noção contemporânea de privacidade ultrapassa a ideia clássica do simples “direito de ser deixado em paz”, passando a envolver a autodeterminação informativa, ou seja, o poder do indivíduo de controlar a circulação e a utilização de seus próprios dados (Garbaccio; Kischelewski, 2024).

Para Doneda (2015), a proteção de dados pessoais representa uma extensão da tutela da personalidade humana no ambiente digital, uma vez que os dados refletem aspectos da identidade e da vida privada dos indivíduos. O autor destaca que a privacidade assume um caráter relacional, relacionado à forma como a pessoa administra sua exposição perante a sociedade e os mecanismos tecnológicos contemporâneos.

Nesse sentido, Couto (2002) afirma que a LGPD surgiu como consequência da necessidade de adaptação do ordenamento jurídico brasileiro às transformações tecnológicas e às novas formas de tratamento massivo de informações pessoais, alinhando-se às tendências internacionais de tutela da privacidade e da autodeterminação informativa.

Segundo Bruno Bioni (2019), os extensos termos de uso e políticas de privacidade acabam tornando o consentimento uma manifestação muitas vezes automática e pouco consciente. Trata-se

de uma crítica à lógica do “tudo ou nada”, na qual o usuário precisa aceitar integralmente as condições impostas pelas plataformas digitais para acessar determinados serviços.

Assim, o modelo atual de tratamento de dados frequentemente dificulta o exercício efetivo da liberdade do titular. Diante disso, Bioni (2019) defende a adoção da granularidade das autorizações, permitindo que o titular escolha de maneira específica quais tratamentos deseja autorizar, fortalecendo, assim, a proteção da autonomia informacional do cidadão.

### **2.1.2. Evolução Normativa da Proteção de Dados no Brasil**

A construção normativa da proteção de dados no Brasil ocorreu de forma gradual, acompanhando as transformações tecnológicas e o avanço da sociedade da informação. A Constituição da República Federativa do Brasil de 1988 foi o primeiro marco relevante ao assegurar, no artigo 5º, inciso X (Brasil, 1988), a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

Embora não tratasse especificamente da proteção de dados pessoais, a Constituição estabeleceu os fundamentos para a tutela jurídica da privacidade no ordenamento brasileiro. Posteriormente, surgiram legislações setoriais que passaram a disciplinar determinadas formas de tratamento de informações pessoais, como o Código de Defesa do Consumidor (art. 43), que regulamentou bancos de dados de consumo, e a Lei do Cadastro Positivo (Lei 12.414/2011, alterada pela LC 166/2019).

Conforme destaca Doneda (2021), a proteção de dados pessoais constitui um desdobramento do direito à privacidade e da própria tutela da personalidade humana no ambiente digital. Nesse

contexto, a proteção de dados passou a ocupar posição central nas discussões jurídicas contemporâneas, especialmente diante da intensa expansão das tecnologias digitais e do crescimento exponencial da circulação de informações na sociedade em rede.

Doneda (2021) explica que a evolução tecnológica demonstrou que a proteção da privacidade precisava ultrapassar a visão tradicional centrada apenas na confidencialidade das comunicações, passando a abranger a circulação e o tratamento massivo de dados pessoais em diferentes contextos sociais e econômicos.

O grande avanço legislativo no ambiente digital ocorreu com o Marco Civil da Internet, instituído pela Lei nº 12.965/2014, que consolidou princípios relacionados à proteção da privacidade, à neutralidade da rede e à proteção de dados pessoais no uso da internet, contudo, o Marco Civil possuía alcance restrito ao ambiente online, o que evidenciou a necessidade de uma legislação geral aplicável a todos os setores da sociedade (Saraiva; Souza; Soares, 2024).

Conforme observa Pinheiro (2018), a LGPD buscou equilibrar o desenvolvimento econômico e tecnológico com a proteção dos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade humana, nesse cenário, foi criada a Lei Geral de Proteção de Dados Pessoais, inspirada principalmente no modelo europeu do Regulamento Geral de Proteção de Dados (GDPR).

A consolidação desse processo ocorreu com a Emenda Constitucional nº 115/2022, que incluiu a proteção de dados pessoais no rol dos direitos e garantias fundamentais previstos na

Constituição Federal. Dessa forma, a proteção de dados passou a possuir status constitucional autônomo, reforçando a importância da tutela da identidade digital e da autodeterminação informativa na sociedade contemporânea.

### **2.1.3. Princípios, Bases Legais e Direitos dos Titulares na LGPD**

A Lei Geral de Proteção de Dados Pessoais instituiu um sistema jurídico fundamentado em princípios que orientam todas as atividades de tratamento de dados pessoais. Entre os principais princípios previstos no artigo 6º destacam-se a finalidade, a adequação, a necessidade e a transparência. O princípio da finalidade (art. 6º, inciso I) determina que o tratamento deve possuir propósitos legítimos, específicos e previamente informados ao titular.

Já a adequação exige compatibilidade entre o tratamento realizado e as expectativas legítimas do cidadão (art. 6º, inciso II). O princípio da necessidade estabelece que somente os dados estritamente indispensáveis devem ser coletados, combatendo práticas excessivas de retenção de informações (art. 6º, inciso III). Segundo Maldonado e Blum (2020), esses princípios funcionam como parâmetros éticos e jurídicos indispensáveis para garantir a legitimidade do tratamento de dados pessoais.

A LGPD também estabelece as chamadas bases legais, que correspondem às hipóteses autorizadoras do tratamento de dados. Embora o consentimento seja uma das bases mais conhecidas, ele não constitui a única possibilidade prevista pela legislação. A lei admite o tratamento de dados para cumprimento de obrigação legal, execução contratual, proteção da vida, tutela da saúde,

exercício regular de direitos, proteção do crédito e legítimo interesse do controlador (LGPD, art 7º), entre outras hipóteses.

Para Bruno Bioni (2019), o consentimento deve ser compreendido como manifestação livre, informada e inequívoca, sendo necessário evitar situações em que o titular seja compelido a aceitar integralmente políticas abusivas para acessar serviços essenciais.

O art. 18 da lei (Brasil, 2018) garante ao cidadão o direito de acessar suas informações, solicitar correção de dados incompletos ou desatualizados, requerer anonimização ou eliminação de informações desnecessárias, revogar o consentimento e solicitar a portabilidade dos dados para outro fornecedor de serviços, destacando que a LGPD se refere aos direitos assegurados aos titulares dos dados pessoais.

Maldonado e Blum (2019) ressaltam que a LGPD transforma o indivíduo em verdadeiro sujeito ativo da proteção de dados, atribuindo-lhe maior controle sobre sua identidade digital. Além disso, a implementação prática desses direitos exige que empresas e instituições adotem mecanismos efetivos de transparência, segurança da informação e governança de dados, fortalecendo a cultura de compliance e proteção da privacidade no ambiente corporativo brasileiro.

## **2.2. A LGPD NO CONTEXTO EMPRESARIAL: Obrigações e Impactos nas Relações de Negócios**

### **2.2.1. Papéis, Responsabilidades e Governança no Tratamento de Dados Pessoais**

A implementação da Lei Geral de Proteção de Dados Pessoais transformou profundamente a estrutura organizacional das empresas brasileiras, exigindo a definição clara de responsabilidades relacionadas ao tratamento de dados pessoais. A legislação estabelece três figuras centrais nesse processo: o controlador, o operador e o encarregado pelo tratamento de dados (LGPD, art. 5º), também conhecido como *Data Protection Officer* (DPO).

O controlador é o agente responsável pelas decisões referentes às finalidades, meios e condições do tratamento dos dados pessoais, enquanto o operador realiza o tratamento em nome do controlador, seguindo suas instruções (LGPD, art. 5º, Incisos VI, VII). Já o encarregado atua como canal de comunicação entre a empresa, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), exercendo funções de orientação, fiscalização interna e atendimento às demandas relacionadas à privacidade e proteção de dados (LGPD, art. 5º, Inciso VIII).

Maldonado e Blum (2020), destacam que as decisões acerca da coleta, compartilhamento, armazenamento e segurança das informações constituem atribuições centrais do controlador, envolvendo aspectos técnicos, organizacionais e jurídicos. Nesse contexto, a governança de dados passou a representar elemento essencial para a conformidade empresarial. As organizações precisam estruturar processos internos capazes de assegurar transparência, segurança da informação e responsabilização no tratamento de dados pessoais.

Para Pinheiro (2026), a definição clara das responsabilidades entre os agentes de tratamento fortalece a cultura de compliance e reduz riscos decorrentes de incidentes de segurança e descumprimento

legal. A presença do encarregado demonstra o compromisso institucional com a proteção de dados e facilita a comunicação entre a empresa e os titulares das informações. Dessa forma, a LGPD não apenas criou novas obrigações jurídicas, mas também impulsionou mudanças estruturais na administração corporativa, exigindo maior integração entre setores jurídicos, tecnológicos e de gestão.

### **2.2.2. Obrigações Práticas de Adequação e Estratégias de Compliance Empresarial**

A adequação à Lei Geral de Proteção de Dados Pessoais exige das empresas a implementação de medidas práticas permanentes voltadas à proteção das informações pessoais. Entre as principais obrigações destacam-se o mapeamento de dados, a elaboração de políticas de privacidade transparentes, a gestão adequada do consentimento e a utilização responsável das bases legais previstas na legislação (Lima; Garrido, 2022).

De acordo com Ruaro e Silva (2023), o mapeamento de dados constitui uma das primeiras etapas do processo de conformidade, pois permite identificar quais dados são coletados, onde estão armazenados, com quem são compartilhados e qual a finalidade de cada tratamento realizado. Segundo Maldonado e Blum (2020), a compreensão do ciclo de vida das informações é indispensável para assegurar o cumprimento dos princípios da finalidade, necessidade e adequação previstos na LGPD.

Os termos de uso e políticas de privacidade frequentemente apresentam linguagem excessivamente técnica e extensa, dificultando a compreensão efetiva pelos titulares dos dados. Bioni (2019) critica os modelos tradicionais de consentimento baseados

em textos extensos e excessivamente técnicos, afirmando que tais práticas dificultam a compreensão efetiva do titular e tornam o consentimento meramente formal.

Para Bauman e Lyon (2013), a sociedade contemporânea é marcada pelo fortalecimento de mecanismos de vigilância e controle informacional, nos quais os indivíduos frequentemente cedem dados pessoais sem plena consciência das consequências decorrentes desse compartilhamento. A chamada granularidade das autorizações, permitindo que o usuário escolha especificamente quais tratamentos deseja autorizar, afastando a lógica do “tudo ou nada” presente em muitas plataformas digitais.

É importante destacar que a transparência nas relações entre empresas e titulares dos dados é fundamental, pois as políticas de privacidade devem ser claras, acessíveis e compreensíveis, permitindo que o cidadão tenha plena ciência acerca do uso de suas informações pessoais (Galdino; Faria, 2021). Além do consentimento, as empresas também podem utilizar outras bases legais previstas na LGPD, como o legítimo interesse, desde que observados critérios de proporcionalidade e respeito aos direitos fundamentais dos titulares. A utilização dessa base exige análise cuidadosa sobre a finalidade do tratamento, a necessidade da coleta e os impactos sobre a privacidade do indivíduo (Barbosa, 2026).

Conforme aponta Barbieri Advogados (2026), muitas organizações ainda enfrentam dificuldades na implementação de programas efetivos de compliance, especialmente em relação à documentação das operações de tratamento, prevenção de vazamentos e elaboração de relatórios de impacto à proteção de dados. Dessa forma, a conformidade com a LGPD demanda investimentos

contínuos em segurança da informação, treinamento de equipes e fortalecimento da cultura organizacional voltada à proteção da privacidade.

### **2.3. Impactos da LGPD nas Relações Contratuais e nos Setores Empresariais**

Na contemporaneidade, marcada pela intensa produção e circulação de dados, praticamente todas as atividades humanas deixam registros digitais capazes de revelar hábitos, preferências, localização e padrões de comportamento. Sensores, algoritmos e plataformas digitais monitoram continuamente os usuários, muitas vezes sem plena compreensão acerca da extensão do tratamento realizado sobre seus dados pessoais (Alfonsin, 2022).

A LGPD produziu impactos significativos nas relações contratuais empresariais, tornando indispensável a inclusão de cláusulas específicas relacionadas à proteção de dados pessoais em contratos de prestação de serviços, parcerias comerciais e compartilhamento de informações.

Pinheiro (2026) observa que a formalização dessas obrigações contratuais fortalece a transparência nas relações empresariais e assegura mecanismos de responsabilização entre os agentes envolvidos no tratamento de dados. As relações entre controladores e operadores passaram a exigir definição detalhada das responsabilidades de cada parte, incluindo regras sobre segurança da informação, confidencialidade, comunicação de incidentes e responsabilização por eventuais danos decorrentes de vazamentos de dados.

A realização de *due diligence* em fornecedores tornou-se prática essencial para reduzir riscos relacionados ao compartilhamento inadequado de informações pessoais. As empresas passaram a avaliar previamente o grau de maturidade de seus parceiros em relação à proteção de dados, verificando políticas de segurança, programas de compliance e capacidade técnica para prevenção de incidentes. Para Maldonado e Blum (2020), a proteção de dados deixou de representar apenas obrigação legal isolada, passando a integrar a estratégia corporativa e os mecanismos de governança empresarial.

Os impactos da LGPD são percebidos de maneira mais intensa em setores que realizam tratamento massivo de informações pessoais, como comércio eletrônico, saúde, instituições financeiras e empresas de tecnologia. No setor da saúde, por exemplo, o tratamento de dados sensíveis exige medidas rigorosas de segurança e confidencialidade em razão da natureza extremamente privada das informações médicas (Chicarelli; Mozaner; Ferrer, 2024).

Já no setor financeiro, a preocupação concentra-se na prevenção de fraudes e na proteção de dados bancários e de crédito. As micro e pequenas empresas, por sua vez, enfrentam desafios específicos relacionados à limitação de recursos financeiros e à ausência de equipes especializadas em proteção de dados (Ferreira; Souza Neto; Ferneda, 2022).

Conforme apontam Saraiva, Souza e Soares (2024), organizações que conseguem estruturar programas efetivos de compliance e proteção de dados tendem a fortalecer sua reputação institucional, aumentar a confiança dos consumidores e obter vantagem competitiva no mercado contemporâneo.

## **2.4. Os Principais Desafios Jurídicos e Práticos na Implementação da LGPD e as Estratégias de Compliance no Ambiente Empresarial**

### **2.4.1. Desafios Jurídicos e Responsabilidade no Tratamento de Dados Pessoais**

A implementação da Lei Geral de Proteção de Dados Pessoais ainda apresenta inúmeros desafios jurídicos para as empresas brasileiras, especialmente em razão das incertezas interpretativas existentes em torno de alguns conceitos previstos na legislação. A base legal do legítimo interesse, por exemplo, continua sendo uma das hipóteses mais complexas de aplicação prática, exigindo das organizações análises individualizadas e criteriosas acerca da proporcionalidade do tratamento realizado.

As empresas precisam avaliar constantemente se o uso dos dados corresponde legitimamente às expectativas dos titulares e se existem medidas suficientes de transparência e segurança capazes de justificar o tratamento sem consentimento expresso (Bioni, 2019).

A LGPD não atua de maneira isolada no ordenamento jurídico brasileiro, coexistindo com normas como o Código de Defesa do Consumidor, a Constituição da República Federativa do Brasil de 1988 e legislações setoriais relacionadas à transparência, ao acesso à informação e à defesa do consumidor. Essa convivência normativa exige das empresas uma interpretação sistemática e integrada das diferentes obrigações legais aplicáveis ao tratamento de dados pessoais.

Segundo Pinheiro (2026), a proteção de dados deve ser compreendida dentro de um modelo jurídico multidisciplinar, no

qual a LGPD dialoga com outras normas de proteção dos direitos fundamentais. Na mesma linha, Viviane Nóbrega Maldonado e Renato Opice Blum (2020) destacam que o chamado “diálogo das fontes” é essencial para harmonizar as exigências regulatórias existentes e evitar conflitos interpretativos.

Outro aspecto relevante refere-se à responsabilização civil, administrativa e reputacional decorrente do tratamento inadequado de dados pessoais. A LGPD prevê responsabilidade solidária entre controlador e operador quando houver descumprimento das obrigações legais ou contratuais relacionadas ao tratamento de dados (LGPD, art 42, § 1º). Dessa forma, o titular não precisa identificar qual integrante da cadeia de tratamento foi diretamente responsável pelo dano sofrido, podendo buscar reparação perante qualquer agente envolvido na operação (Maldonado; Blum, 2020).

Doneda (2021), a proteção de dados pessoais passou a representar um elemento central da tutela da dignidade humana no ambiente digital, tornando inevitável a ampliação da responsabilidade das organizações quanto à preservação da privacidade e da segurança informacional.

#### **2.4.2. Desafios Operacionais, Tecnológicos e Estruturais à Proteção de Dados Pessoais nas Empresas Brasileiras**

No âmbito operacional, um dos principais obstáculos enfrentados pelas empresas quanto à proteção de dados pessoais refere-se à ausência de controle efetivo sobre os dados pessoais tratados internamente. Muitas organizações ainda não possuem inventários completos das informações armazenadas, desconhecendo quais

dados circulam em seus setores, onde estão localizados e quais finalidades justificam sua manutenção.

A ausência desse mapeamento dificulta a aplicação dos princípios da finalidade, necessidade e minimização previstos na LGPD. Para Maldonado e Blum (2020), a adequação à legislação depende diretamente da capacidade da empresa de compreender o ciclo de vida das informações pessoais, desde a coleta até o descarte definitivo.

Vazamentos de dados, ataques cibernéticos e falhas humanas passaram a representar riscos permanentes para organizações de todos os portes, assim evidenciando que se trata de um desafio significativo que está relacionado aos incidentes de segurança e à vulnerabilidade dos sistemas tecnológicos utilizados pelas empresas (Couto, 2022).

Nesse panorama, a atualização de sistemas legados, estruturas tecnológicas, antigas que não foram desenvolvidas sob a lógica da proteção de dados, exige investimentos elevados em infraestrutura, segurança da informação e capacitação técnica. Segundo Bioni (2019), a adequação à LGPD não depende apenas da implementação de softwares específicos, mas da reconstrução dos próprios processos organizacionais a partir da lógica do *privacy by design*, incorporando a privacidade desde a concepção das atividades empresariais.

As micro, pequenas e médias empresas enfrentam dificuldades ainda maiores em razão da limitação de recursos financeiros e da escassez de profissionais especializados em proteção de dados e compliance digital. Muitas organizações não possuem

departamentos jurídicos estruturados nem equipes de tecnologia capacitadas para implementar programas robustos de governança da informação (Garbaccio; Kischelewski, 2024).

Ferreira, Souza Neto e Ferneda (2022) afirmam que a maturidade do compliance em proteção de dados depende não apenas de ferramentas tecnológicas, mas também da integração entre gestão, segurança da informação e cultura organizacional. Da mesma forma, Alfonsin (2022) observa que setores sensíveis, como a saúde, enfrentam desafios adicionais em razão do tratamento de dados sensíveis e da necessidade de adoção de medidas rigorosas de confidencialidade e segurança.

O avanço da inteligência artificial, do Big Data e das tecnologias de análise preditiva ampliou significativamente os riscos relacionados ao tratamento automatizado de informações pessoais. Sistemas algorítmicos podem reproduzir discriminações, tomar decisões automatizadas opacas e utilizar dados para finalidades não previstas inicialmente pelo titular.

Para Ruaro e Silva (2023), o desenvolvimento tecnológico exige constante atualização da interpretação jurídica da proteção de dados, especialmente diante das novas formas de vigilância digital e exploração econômica das informações pessoais.

### **2.4.3. Estratégias de Compliance e Caminhos para a Efetividade da Proteção de Dados no Âmbito Empresarial Brasileiro**

Diante dos desafios jurídicos e operacionais impostos pela LGPD, o compliance em proteção de dados passou a ocupar posição estratégica dentro das organizações. A conformidade legal deixou de ser percebida apenas como obrigação burocrática e passou a

integrar os mecanismos de governança corporativa, gestão de riscos e fortalecimento da reputação institucional.

Lima e Garrido (2022), a implementação de programas de compliance voltados à LGPD permite que as organizações desenvolvam maior segurança jurídica, transparência e confiança nas relações empresariais e de consumo.

Entre as principais estratégias de adequação destaca-se o mapeamento completo dos fluxos de dados pessoais, permitindo que a empresa identifique quais informações coleta, como são utilizadas, por quanto tempo permanecem armazenadas e com quem são compartilhadas. Esse processo deve ser acompanhado da elaboração de políticas internas claras, revisão contratual com fornecedores e criação de canais de atendimento aos titulares dos dados (Saraiva; Souza; Soares, 2024).

Barbieri Advogados (2026) tratam das empresas que implementam estruturas preventivas de governança conseguem reduzir significativamente os riscos de sanções administrativas, vazamentos de informações e litígios judiciais relacionados à privacidade.

Outra medida essencial refere-se à capacitação contínua dos colaboradores e ao fortalecimento da cultura organizacional voltada à proteção de dados. A ausência de conscientização interna ainda representa um dos maiores obstáculos à efetividade da LGPD, uma vez que falhas humanas continuam figurando entre as principais causas de incidentes de segurança.

Para Chicarelli, Mozaner e Ferrer (2024), o compliance deve ser compreendido como instrumento permanente de fortalecimento da segurança da informação e da ética empresarial, exigindo

participação ativa da liderança organizacional e integração entre setores jurídicos, tecnológicos e administrativos.

A adoção de ferramentas preventivas, como o Relatório de Impacto à Proteção de Dados (RIPD), também representa importante mecanismo de gestão de riscos e demonstração de boa-fé perante a Autoridade Nacional de Proteção de Dados.

Barbosa (2026) fala que as empresas que negligenciam práticas preventivas e programas de governança tendem a enfrentar consequências financeiras severas, especialmente diante do aumento da fiscalização e da aplicação de sanções pela ANPD. Nesse cenário, o compliance efetivo depende da consolidação de uma cultura de privacidade capaz de equilibrar inovação tecnológica, desenvolvimento econômico e proteção dos direitos fundamentais dos titulares dos dados pessoais.

A efetividade da proteção de dados no ambiente corporativo exige mudança estrutural na forma como as empresas compreendem o valor das informações pessoais. Conforme ressaltam Almeida e Soares (2022), a sociedade contemporânea é marcada pela intensa circulação de dados no ambiente digital, tornando indispensável a construção de modelos empresariais pautados na transparência, responsabilidade e respeito à privacidade.

Dessa forma, organizações que incorporam a proteção de dados como elemento central de sua estratégia institucional não apenas reduzem riscos jurídicos, mas também fortalecem sua credibilidade, competitividade e confiança perante consumidores e parceiros comerciais.

### **3. CONCLUSÃO**

O uso das diretrizes da LGPD no Brasil mudou de forma drasticamente positiva o mundo digital, no que tange a proteção dos direitos dos cidadãos com relação a proteção e tratamento de dados pessoais. Ela garante privacidade e segurança nos mais diversos setores da economia e ampara a dignidade das pessoas com ética e transparência.

Conclui-se que a LGPD, não define apenas regras e diretrizes, atua como um tipo de tratado entre as empresas e as pessoas, garantindo ética e confiança no tratamento das informações obtidas. Implementar as políticas necessárias para o fiel cumprimento da Lei, ainda é um grande desafio, principalmente para as pequenas e média empresas, pois obstáculos ainda persistem, principalmente no que diz respeito a mão de obra qualificada e ainda a aversão do que é novo, com descrença na expectativa dos resultados satisfatórios.

Um aspecto central para a efetiva conformidade com a LGPD consiste na clara delimitação de responsabilidades. Essa distinção contribui para a estruturação adequada da cadeia de responsabilidades e reduz o risco de que uma organização assuma integralmente os ônus decorrentes de falhas cometidas por terceiros (Pinheiro, 2018). A adequação de “sistemas legados” representa um dos principais entraves, uma vez que muitos deles foram desenvolvidos sem considerar os requisitos de proteção de dados. Diante disso, torna-se essencial a adoção do princípio do Privacy by Design, que prevê a incorporação de medidas de privacidade desde as fases iniciais de concepção e desenvolvimento de projetos. Com o avanço acelerado da inteligência artificial previsto para o biênio 2025/2026, essa adaptação deverá ocorrer de maneira ainda mais

dinâmica, de forma a acompanhar a evolução tecnológica sem comprometer os direitos dos titulares.

Caso contrário, o avanço tecnológico poderá ocorrer em detrimento da transparência e da efetiva tutela dos direitos fundamentais dos titulares de dados. Paralelamente, a Autoridade Nacional de Proteção de Dados (ANPD) tem intensificado a aplicação de sanções administrativas, enquanto o mercado exerce sua própria forma de accountability: as empresas que descumprem as normas de proteção de dados enfrentam perda de clientes, afastamento de parceiros comerciais e danos significativos à sua reputação institucional (Pinheiro, 2018). Sob uma perspectiva jurídica, a LGPD não deve ser compreendida meramente como um conjunto de formalidades burocráticas ou obrigações documentais. Quando as organizações internalizam efetivamente os valores éticos e os princípios da proteção de dados em sua cultura corporativa, elas constroem um ativo intangível de extrema relevância: a confiança dos titulares, dos consumidores e do mercado. Em um ambiente digital altamente competitivo, essa confiança emerge como um dos recursos mais estratégicos e valiosos para a sustentabilidade e a longevidade das marcas.

Portanto, o sucesso depende de criar uma cultura de privacidade de verdade, com líderes que incentivem e treinem as equipes continuamente. A LGPD tem potencial para equilibrar inovação com respeito aos direitos das pessoas, fazendo com que cada cidadão tenha mais controle sobre a própria vida digital. Cabe a empresários, advogados, órgãos públicos e toda a sociedade trabalhar junto para que essa lei não fique só no papel, mas vire uma ferramenta que impulse um crescimento econômico mais ético e sustentável.

## REFERÊNCIAS BIBLIOGRÁFICAS

ALFONSIN, Taiane Meirelles. **Gestão de compliance adequada à Lei Geral de Proteção de Dados na área da saúde**. Porto Alegre, 2022. 112 f. Dissertação (Mestrado) – Programa de Mestrado Profissional em Direito – Universidade do Vale do Rio do Sinos – UNISINOS, 2022.

ALMEIDA, Siderly do Carmo Dahle de. SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital. **Perspectivas em Ciência da Informação**, v.27, n. 3, p. 26-45, jul/set 2022. DOI: <http://dx.doi.org/10.1590/1981-5344/25905>. Disponível em: <https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/?format=pdf&lang=pt>. Acesso em: 22 abr. 2026.

BARBIERI ADVOGADOS. **LGPD para empresas**: obrigações, sanções e conformidade jurídica. [S. l.], 2026. Disponível em: Artigo completo. Acesso em: 25 maio 2026.

BARBOSA, Yêda Maria Ferreira. Compliance e LGPD: erros que geram multas milionárias. **Migalhas**, nº 6.355, fev. 2026. Disponível em: <https://www.migalhas.com.br/depeso/450435/compliance-e-lgpd-erros-que-geram-multas-milionarias>. Acesso em: 05 mai. 2026.

BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. ISBN 978-85-309-8328-4.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 1988. Disponível em:

[http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicaocompila.do.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompila.do.htm). Acesso em: 22 abr. 2026.

BRASIL. **Lei do Cadastro Positivo**. Brasil. Lei nº 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Diário Oficial da União, Brasília, DF, 10 jun. 2011. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/l12414.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm). Acesso em: 16 maio 2026.

BRASIL. **Lei Complementar nº 166, de 8 de abril de 2019**. Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores. Diário Oficial da União, Brasília, DF, 9 abr. 2019. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/lcp/lcp166.htm](https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp166.htm). Acesso em: 16 maio 2026.

BRASIL. **Lei Geral de Proteção de Dados Pessoais**. Brasil. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: Brasília, DF, 15 ago. 2018.

BRASIL. **Código de Defesa do Consumidor**. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: Brasília, DF, 12 set. 1990.

BRASIL. **Emenda Constitucional nº 115**, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Diário Oficial da União: Brasília, DF, 11 fev. 2022.

CHICARELLI, Ana Laura Gonçalves; MOZANER, Victória Cassia; FERRER, Walkiria Martinez Heinrich. Compliance como ferramenta de efetivação da segurança da informação na empresa. **Revista Brasileira de Direito Empresarial**, Florianópolis, Brasil, v. 9, n. 2, 2024.

DOI: 10.26668/IndexLawJournals/2526-0235/2023.v9i2.10199.

Disponível em:

<https://indexlaw.org/index.php/direitoempresarial/article/view/10199>.

Acesso em: 15 mai. 2026.

COUTO, Isabeli Cintra. Aplicação do programa de compliance nas empresas brasileiras à luz do Marco Civil da Internet e da Lei Geral de Proteção de Dados. **Revista de Iniciação Científica e Extensão da Faculdade de Direito de Franca**, ISSN 2675-0104 – v.7, n.1, dez. 2022.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2021.

DONEDA, Danilo. Princípios e proteção de dados pessoais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III: marco civil da internet**. São Paulo: Quartier Latin, 2015.

FERREIRA, Joel Mateus Lopes. SOUZA NETO, João. Ferneda, EDILSON. Modelo de maturidade de compliance à LGPD – Lei Geral de Proteção de Dados Pessoais. **Revista Gestão do Conhecimento e Tecnologia da Informação**, 6:61-72, 2022.

GARBACCIO, G. Ladeira; KISCHELEWSKI, F Lubieska N. Governança e boas práticas na Lei Geral de Proteção de Dados por meio da conformidade, da gestão de riscos e da accountability. **Revista Brasileira de Estudos Políticos**, v. 128, 15 jul. 2024. Disponível em:

<https://pos.direito.ufmg.br/rbep/index.php/rbep/article/view/894/719>.

Acesso em: 20 mai. 2026.

GALDINO, Willames José Moraes. FARIA, Emerson Oliveira de. A atuação da Lei Geral de Proteção de Dados (LGPD) frente compliance. **Semana Acadêmica Revista Científica**, Fortaleza-CE. Ed. 212. V. 9. Ano 2021. DOI: <http://dx.doi.org/10.35265/2236-6717-212-9370>. Disponível em:

[https://semanaacademica.org.br/system/files/artigos/1.willames.\\_a\\_atuacao\\_da\\_lei\\_geral\\_de\\_protecao\\_de\\_dados\\_lgpd\\_frente\\_compliance\\_artigo\\_revista.pdf](https://semanaacademica.org.br/system/files/artigos/1.willames._a_atuacao_da_lei_geral_de_protecao_de_dados_lgpd_frente_compliance_artigo_revista.pdf). Acesso em: 20 mai. 2026.

LIMA, Ricardo Alves de. GARRIDO, Guilherme Leite. Lei Geral de Proteção de Dados Pessoais (LGPD) e compliance: um panorama da adequação normativa para organizações contemporâneas. **Revista Eletrônica do Curso de Direito da UFSM**, v. 17, n. 1 / 2022 e68680. DOI: 10.5902/1981369468680. Disponível em: <https://periodicos.ufsm.br/revistadireito/article/view/68680>. Acesso em: 13 mai. 2026.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). **LGPD: Lei Geral de Proteção de Dados comentada**. 2. ed. São Paulo: Thomson Reuters, 2020.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. Ed. 5º, São Paulo: Saraiva, 2026.

RUARO, Regina. SILVA, Fabrizio Predebon da. Os fundamentos da lei geral de proteção de dados (Lei nº 13.709/2018). **RJLB**, Ano 9, nº 4, 1371-1413, 2023. Disponível em: [https://www.cidp.pt/revistas/rjlb/2023/4/2023\\_04\\_1371\\_1413.pdf](https://www.cidp.pt/revistas/rjlb/2023/4/2023_04_1371_1413.pdf).

Acesso em: 13 mai. 2026.

SARAIVA, Juliana; SOUZA, Cleidson de; SOARES, Sérgio. Desafios de Compliance da LGPD: Implantação na Indústria de Software Brasileira. In: Workshop sobre Aspectos Sociais, Humanos e Econômicos de Software (WASHES), 9., 2024, Brasília/DF. **Anais** [...]. Porto Alegre: Sociedade Brasileira de Computação, 2024. p. 193-198. ISSN 2763-874X. DOI: <https://doi.org/10.5753/washes.2024.3079>.

---

Artigo apresentado ao Curso de Direito do Centro Universitário Santa Terezinha - CEST, para obtenção do grau de Bacharel em Direito.

<sup>1</sup> Graduando em Direito. Centro Universitário Santa Terezinha - CEST. São Luís, Maranhão, Brasil.

<sup>2</sup> Administrador, Graduando em Direito. Centro Universitário Santa Terezinha - CEST. São Luís, Maranhão, Brasil.

<sup>3</sup> Orientadora.