

LGPD E PROTEÇÃO DE DADOS PESSOAIS: DESAFIOS E PERSPECTIVAS LGPD

AND PERSONAL DATA PROTECTION: CHALLENGES AND PERSPECTIVES

Artigo submetido em 26 de maio de 2026

Artigo aprovado em 27 de maio de 2026

Artigo publicado em 27 de maio de 2026

Scientia et Ratio

Volume 6 – Número 10 – 2026

ISSN 2525-8532

Autor:

Walbery Freire Barbosa[1]

Igor Câmara de Araújo[2]

RESUMO: Este artigo analisa os desafios e as perspectivas da proteção de dados pessoais no Brasil a partir da Lei Geral de Proteção de Dados Pessoais. O estudo parte do problema da efetividade da legislação diante da rápida transformação tecnológica e da ampliação do tratamento de dados por organizações públicas e privadas. O objetivo consiste em examinar os principais entraves à aplicação da lei nas organizações brasileiras e discutir as perspectivas da proteção de dados diante de tecnologias emergentes, como inteligência artificial e Big Data. Para isso, adota-se abordagem qualitativa, com procedimento bibliográfico e análise de produções doutrinárias e científicas sobre o tema. Os resultados

indicam que a efetivação da lei ainda depende do fortalecimento da governança de dados, da capacitação de profissionais, da adoção de medidas de segurança da informação e da consolidação de uma cultura de privacidade. Verifica-se, ainda, que o avanço de tecnologias emergentes exige mecanismos mais sofisticados de prevenção, auditabilidade, transparência e responsabilidade no tratamento de dados. Conclui-se que a legislação representa avanço significativo no ordenamento jurídico brasileiro, mas sua plena eficácia requer articulação entre regulação, inovação tecnológica, educação digital e compromisso institucional com a proteção da privacidade e dos direitos fundamentais.

Palavras-chave: proteção de dados pessoais. privacidade. tecnologias emergentes.

ABSTRACT: This article analyzes the challenges and perspectives of personal data protection in Brazil based on the General Data Protection Law. The study addresses the problem of the law's effectiveness in the context of rapid technological transformation and the expansion of data processing by public and private organizations. Its objective is to examine the main obstacles to the implementation of the law in Brazilian organizations and to discuss the prospects for data protection in the face of emerging technologies, such as artificial intelligence and Big Data. To this end, the research adopts a qualitative approach, based on bibliographic procedure and the analysis of doctrinal and scientific literature on the subject. The findings indicate that the effectiveness of the law still depends on stronger data governance, professional training, the adoption of information security measures, and the consolidation of a privacy culture. The study also shows that the advance of emerging technologies requires more sophisticated mechanisms of prevention, auditability, transparency, and accountability in data processing. It is concluded that the law represents a significant advance in the Brazilian legal system, but its full effectiveness requires articulation between regulation, technological innovation, digital education, and institutional commitment to privacy and fundamental rights protection.

Keywords: personal data protection. privacy. emerging technologies.

1 INTRODUÇÃO

A proteção de dados pessoais tornou-se um dos temas centrais da sociedade contemporânea, especialmente com a rápida expansão do mundo digital e o aumento exponencial da coleta de informações. As inovações tecnológicas, aliadas à digitalização de interações sociais, comerciais e políticas, trouxeram inúmeros benefícios, mas também desafios éticos, legais e técnicos para a proteção da privacidade. Nesse cenário, o estudo da proteção de dados pessoais na era digital se mostra urgente, dada a crescente relevância da segurança das informações e dos direitos fundamentais dos indivíduos. O mundo digital, atualmente essencial para inúmeras atividades cotidianas, gera um fluxo massivo de dados, desde preferências de consumo até informações sensíveis, como registros financeiros e de saúde.

Com a proliferação de redes digitais e plataformas eletrônicas, os dados pessoais são frequentemente coletados e utilizados sem o consentimento adequado dos titulares, expondo usuários a riscos à privacidade. Grandes empresas e corporações utilizam algoritmos para tratar esses dados, criando perfis que muitas vezes são explorados para finalidades que os usuários desconhecem, como direcionamento de publicidade e decisões automatizadas. O escândalo da Cambridge Analytica exemplifica o uso indevido dessas informações, mostrando como práticas inadequadas de coleta de dados podem ameaçar a integridade da privacidade dos indivíduos. O problema central, então, está na capacidade das legislações, como a LGPD, de proteger esses direitos em meio ao avanço tecnológico (Souza, 2025).

A criação da Lei Geral de Proteção de Dados (LGPD) em 2018 foi uma resposta às crescentes preocupações com a privacidade no ambiente digital, alinhando o Brasil a padrões internacionais de proteção de dados, como o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia. No entanto, a aplicação da LGPD ainda enfrenta desafios, principalmente em setores que precisam se adaptar rapidamente às exigências legais.

A era digital, marcada pelo uso intensivo de algoritmos e tecnologias emergentes como Big Data e inteligência artificial, impõe desafios inéditos à proteção de dados pessoais. Assim, analisar criticamente a legislação vigente é essencial para propor soluções eficazes que garantam os direitos dos titulares de dados. O estudo busca, portanto, fornecer subsídios teóricos e práticos para o fortalecimento da LGPD, destacando a relevância de uma fiscalização mais robusta, maior conscientização pública e desenvolvimento de ferramentas tecnológicas que garantam a segurança das informações (Salomão; Leonarde, 2026).

A LGPD apesar de representar um avanço significativo para a proteção de dados no Brasil, enfrenta dificuldades em assegurar a privacidade dos indivíduos em um cenário tecnológico em constante mudança. A hipótese é que a legislação, em sua forma atual, ainda não consegue acompanhar plenamente as rápidas inovações tecnológicas, especialmente no que se refere ao uso de algoritmos e inteligência artificial. Essas inovações exigem revisões contínuas da lei e a adoção de práticas mais rigorosas de fiscalização e conscientização para garantir a eficácia da proteção de dados (Souza, 2025).

O objetivo do estudo é evidenciar os desafios e perspectivas jurídicas na interpretação e aplicação da LGPD, especialmente em face da rápida evolução tecnológica e das novas formas de tratamento de dados. A proposta central é identificar os desafios e perspectivas de adaptação de empresas e órgãos públicos às exigências legais e o impacto das novas tecnologias e apontar as lacunas na segurança dos dados pessoais e dos direitos dos indivíduos no ambiente digital (Menolli *et al.*, 2025).

Este trabalho busca contribuir para o debate sobre o futuro da proteção de dados no Brasil, oferecendo uma análise crítica dos desafios impostos pela era digital à aplicação da LGPD. A pesquisa também visa analisar e evidenciar possíveis melhorias na legislação, com base nas dificuldades enfrentadas por empresas, organizações e profissionais do Direito, com o intuito de assegurar a privacidade e a segurança das informações pessoais no Brasil.

2 DESENVOLVIMENTO TEÓRICO

• DESAFIOS DA EFETIVAÇÃO DA LGPD NAS ORGANIZAÇÕES BRASILEIRAS

A efetivação da Lei Geral de Proteção de Dados Pessoais nas organizações brasileiras constitui um dos mais relevantes desafios do cenário jurídico e empresarial contemporâneo. Embora a Lei n.º 13.709/2018 tenha inaugurado um novo paradigma de tutela da privacidade e de responsabilização no tratamento de dados pessoais, sua implementação prática ainda ocorre de maneira desigual, gradual e, em muitos casos, insuficiente.

Isso ocorre porque a incidência da LGPD não se limita à imposição de comandos normativos abstratos; ao contrário, ela exige uma transformação concreta na forma como as organizações coletam, armazenam, compartilham, utilizam e descartam informações pessoais.

Nesse sentido, o problema da efetivação não decorre apenas da novidade legislativa, mas da necessidade de reorganização de estruturas administrativas, tecnológicas e culturais que historicamente não foram pensadas a partir da lógica da proteção de dados.

Souza (2025) observa que a LGPD passou a exigir das empresas práticas rigorosas de compliance, políticas de proteção de dados eficazes e investimentos em treinamento e segurança, o que demonstra que a lei alterou de modo profundo o ambiente institucional brasileiro. De forma convergente, Salomão e Leonarde (2026) sustentam que a LGPD representa um arcabouço jurídico robusto para a governança de dados, mas sua concretização exige interpretação contínua, adaptação institucional e capacidade de resposta frente à crescente complexidade tecnológica.

A primeira dificuldade para a efetivação da LGPD nas organizações brasileiras está na passagem da conformidade formal para a conformidade material. Em muitos contextos, a adequação à lei ainda é compreendida como mera formalidade documental, resumida à

elaboração de políticas de privacidade, termos de uso, formulários de consentimento ou comunicados internos padronizados. Esse movimento, embora relevante, é insuficiente quando desacompanhado de alteração real dos fluxos de tratamento de dados.

A proteção de dados não se realiza apenas com produção documental, mas com revisão das rotinas institucionais, delimitação de finalidades, redução da coleta excessiva, controle de acessos, definição de responsabilidades e criação de procedimentos de monitoramento. Por isso, Feigelson e Siqueira (2019, p. 18) afirmam que “a adequação das organizações à LGPD requer mudanças significativas em suas políticas de gestão de dados”, o que confirma que a lei exige transformação estrutural, e não apenas adaptação superficial.

Sob o mesmo raciocínio, Souza (2025) destaca que a implementação da LGPD implica ajuste de sistemas internos, capacitação profissional e mudança nos processos organizacionais. Assim, um dos maiores obstáculos à efetivação da norma reside justamente na tendência de diversas organizações em reduzir a proteção de dados a um protocolo burocrático, sem promover mudança efetiva na cultura de tratamento das informações pessoais.

Essa dificuldade se agrava porque a LGPD exige uma nova racionalidade organizacional, fundada na prevenção, na responsabilidade e na transparência. A cultura administrativa tradicional de muitas instituições brasileiras foi formada em um contexto no qual dados pessoais eram tratados como ativos livremente apropriáveis, passíveis de coleta ampla, armazenamento indefinido e compartilhamento sem detalhamento claro ao titular.

A LGPD rompe com essa lógica ao afirmar princípios como finalidade, adequação, necessidade, transparência, segurança e responsabilização, o que obriga as organizações a reverem suas práticas mais básicas. Nesse ponto, Doneda (2021) é central ao associar a proteção de dados à autodeterminação informativa e à construção de uma cultura de privacidade. Segundo Souza (2025), a autodeterminação informativa constitui o alicerce de qualquer legislação protetiva, porque desloca o foco do mero interesse econômico no dado

para o reconhecimento do titular como sujeito de direitos.

Esse aspecto é decisivo: sem a internalização da ideia de que dados pessoais não são simples insumos operacionais, mas projeções da personalidade e da vida privada, a conformidade tende a permanecer limitada ao plano formal. Em outras palavras, a efetivação da LGPD demanda mudança cultural, e mudanças culturais são mais lentas, complexas e profundas do que mudanças meramente documentais.

Bezerra e Waltz (2014, p. 162) afirmam que “a proteção de dados pessoais exige, além de regulamentação jurídica, um esforço educativo voltado para os cidadãos”, o que demonstra que a efetivação da lei depende também de consciência social e informacional. Nas organizações brasileiras, essa dificuldade se manifesta de diversas formas: canais de atendimento pouco acessíveis, respostas genéricas às solicitações dos titulares, linguagem excessivamente técnica nas políticas de privacidade e incapacidade de localizar, com precisão, os dados tratados em diferentes setores ou sistemas. Assim, o problema não é apenas jurídico, mas também operacional. Quando a organização não possui mapeamento dos fluxos de dados, a resposta ao titular tende a ser lenta, incompleta ou inconsistente, o que enfraquece a própria promessa democrática da LGPD.

Esse quadro remete a uma exigência central da efetivação: o desenvolvimento de estruturas de governança de dados. A literatura analisada por Souza (2025) confere especial relevância a esse conceito, sobretudo a partir das contribuições de Batistella (2024). A governança de dados compreende o conjunto de políticas, procedimentos, responsabilidades e mecanismos de monitoramento por meio dos quais a organização administra o ciclo de vida dos dados pessoais e demonstra conformidade com a legislação.

Nesse sentido, Batistella (2024) sustenta que as empresas precisam desenvolver estruturas robustas para monitorar, avaliar e ajustar suas práticas de proteção de dados, o que envolve treinamento, auditorias periódicas, mecanismos de revisão e nomeação de encarregado. A

importância dessa abordagem está no fato de que a LGPD não se satisfaz com uma postura passiva. Ao contrário, ela pressupõe atuação preventiva, capacidade de resposta e demonstração contínua de diligência. Sem governança, a proteção de dados fica fragmentada entre setores, dependente de iniciativas isoladas e vulnerável à informalidade. Com governança, a conformidade passa a integrar a estratégia institucional. Por isso, a efetivação da LGPD exige não apenas conhecimento jurídico, mas também desenho organizacional coerente com a lógica da responsabilização.

A necessidade de governança, contudo, expõe a profunda desigualdade existente entre as organizações brasileiras. Grandes empresas, em regra, possuem maior capacidade de investimento em consultorias, softwares, auditorias, equipes jurídicas e programas de cibersegurança. Pequenas e médias empresas, ao contrário, frequentemente operam com estruturas enxutas, baixa maturidade digital e recursos limitados. Esse descompasso é um dos fatores mais relevantes para explicar a implementação desigual da LGPD no país. Amaral (2016) enfatiza que os custos de adaptação recaem de forma particularmente intensa sobre pequenos e médios empreendimentos, que precisam investir em tecnologia, capacitação e reestruturação de processos para atender às exigências da lei.

Além disso, o autor destaca a escassez de profissionais especializados como entrave adicional à conformidade completa. Não se trata, portanto, apenas de resistência organizacional, mas de limitação material concreta. Muitas empresas reconhecem a necessidade de adequação, mas não dispõem de condições financeiras, técnicas ou humanas para implementá-la com a profundidade necessária. Em razão disso, a efetivação da LGPD no Brasil não pode ser analisada de forma homogênea, como se todas as organizações partissem do mesmo patamar estrutural.

Ao lado dos custos econômicos, a carência de pessoal qualificado representa uma barreira prática de primeira grandeza. A implementação da LGPD pressupõe profissionais capazes de

compreender bases legais, princípios de tratamento, segurança da informação, governança de dados, resposta a incidentes e direitos dos titulares. Souza (2025) aponta que a falta de profissionais qualificados impõe às empresas a necessidade de investir em treinamentos internos e estratégias de longo prazo para formar equipes capazes de lidar com os novos deveres regulatórios. Essa insuficiência é especialmente sensível em organizações que não possuem departamentos jurídicos ou tecnológicos consolidados. Além disso, a complexidade do tema exige formação interdisciplinar: não basta conhecer apenas o texto legal, assim como não basta dominar apenas a infraestrutura técnica.

A efetivação da LGPD depende da articulação entre direito, gestão, tecnologia e ética institucional. Quando esse diálogo não ocorre, surgem soluções incompletas: ou prevalece uma leitura puramente jurídica, desconectada das operações reais, ou uma resposta estritamente técnica, incapaz de enfrentar os fundamentos normativos da proteção de dados. Por essa razão, o treinamento contínuo de colaboradores não pode ser tratado como medida acessória. Ao contrário, ele é uma das bases da efetivação da LGPD no ambiente organizacional.

Salomão e Leonarde (2026), ao discutir a relação entre LGPD e inteligência artificial, lembram que a lei exige medidas de segurança, técnicas e administrativas, aptas a proteger os dados contra acessos não autorizados, perdas, alterações e tratamentos inadequados. Isso mostra que a efetivação da lei não pode ser pensada apenas em termos de política institucional; ela exige infraestrutura, monitoramento, autenticação, controle de acesso, rastreabilidade e capacidade de reação a incidentes. A existência de norma sem mecanismo efetivo de proteção transforma a conformidade em mera aparência.

A ênfase na segurança torna-se ainda mais importante quando se considera que muitas organizações brasileiras tratam dados em ecossistemas digitais complexos, com múltiplos fornecedores, plataformas terceirizadas, serviços em nuvem, softwares compartilhados e operadores externos. Isso significa que a conformidade não depende apenas da atuação

direta da organização, mas de toda a cadeia de tratamento. Souza (2025) destaca que a necessidade de gerenciar a conformidade de terceiros e parceiros comerciais aumenta a complexidade das operações e pressiona a estrutura de compliance das empresas.

Em outras palavras, uma empresa pode elaborar boas políticas internas, mas ainda assim permanecer vulnerável se seus parceiros tratarem dados de forma inadequada. Esse cenário exige *due diligence* contratual, revisão de cláusulas de proteção de dados, monitoramento contínuo de fornecedores e delimitação clara de responsabilidades entre controladores e operadores. A efetivação da LGPD, portanto, não é apenas um problema interno; trata-se também de um desafio relacional, que exige governança ampliada sobre fluxos informacionais que extrapolam os limites físicos da própria organização.

No que se refere à responsabilidade civil, os desafios à efetivação da LGPD nas organizações brasileiras exigem que a proteção de dados seja compreendida não apenas como obrigação formal de conformidade, mas como dever permanente de prevenção, controle e reparação. Isso significa que o tratamento inadequado de dados pessoais não se esgota na esfera administrativa ou reputacional, podendo também gerar consequências patrimoniais e jurídicas

quando produz danos aos titulares. Em termos práticos, a responsabilidade civil assume papel estratégico porque obriga as organizações a saírem de uma lógica reativa, baseada apenas na resposta ao incidente, para adotar uma postura preventiva, fundada na gestão de riscos, na diligência e na demonstração de cuidado institucional.

No contexto mais recente, esse debate torna-se ainda mais sensível diante do uso crescente de sistemas automatizados, da circulação massiva de dados e da ampliação da dependência organizacional de tecnologias baseadas em inteligência artificial, o que tensiona os parâmetros tradicionais de imputação de responsabilidade e de prova do dano. Salomão e Leonarde (2026) os autores mencionam ainda que questões como a responsabilidade civil

objetiva ou subjetiva por danos causados por algoritmos, a opacidade algorítmica e os desafios de auditoria e transparência ainda permanecem insuficientemente explorados na literatura nacional. Em termos organizacionais, isso significa que a adoção de tecnologias inteligentes não reduz o dever de cuidado; ao contrário, eleva o nível de exigência sobre quem desenvolve, contrata, implementa ou utiliza tais sistemas. Quanto mais complexa a tecnologia empregada no tratamento de dados, maior tende a ser a necessidade de documentação, supervisão, validação e mecanismos de revisão humana. A efetivação da LGPD, portanto, exige que as organizações assumam responsabilidade não apenas pelos dados que armazenam, mas também pelos processos decisórios que constroem a partir desses dados.

Nessa perspectiva, a efetivação da LGPD não depende apenas da existência de sanções ou da elaboração de documentos formais, mas da consolidação de uma nova ética institucional orientada à responsabilidade. É justamente nesse ponto que o desafio brasileiro se torna mais complexo: implementar uma legislação moderna em um ambiente ainda marcado por desigualdades estruturais, carências técnicas e práticas organizacionais sedimentadas em lógica anterior à proteção de dados.

2.2. PERSPECTIVAS DA PROTEÇÃO DE DADOS PESSOAIS DIANTE DAS TECNOLOGIAS EMERGENTES

A expansão de tecnologias emergentes, como inteligência artificial, Big Data, aprendizagem de máquina, sistemas automatizados de decisão e infraestruturas digitais de alta conectividade, impõe à proteção de dados pessoais um horizonte de reformulação contínua. Nesse cenário, a perspectiva central já não consiste apenas em afirmar a necessidade de tutela da privacidade, mas em redefinir os próprios instrumentos jurídicos, institucionais e técnicos capazes de sustentar essa tutela em ambientes marcados por processamento intensivo,

inferência automatizada e circulação transnacional de informações. Salomão e Leonarde (2026) observam que a LGPD constitui o principal marco normativo brasileiro para equilibrar inovação tecnológica e salvaguarda dos indivíduos, mas que sua aplicação às novas arquiteturas digitais exige “interpretação e adaptação contínuas” para acompanhar o ritmo da inovação. Essa afirmação projeta uma primeira perspectiva relevante: a proteção de dados tende a se consolidar menos como um sistema fechado de regras estáticas e mais como um campo dinâmico de atualização normativa e hermenêutica.

Sob essa ótica, uma das perspectivas mais importantes é a passagem de um modelo reativo de regulação para um paradigma preventivo e prospectivo. Em ecossistemas digitais baseados em decisões algorítmicas, personalização em larga escala e cruzamento constante de bases de dados, a mera resposta posterior ao dano já se mostra insuficiente. A tendência é que a proteção de dados se articule cada vez mais com mecanismos de antecipação de risco, incorporando avaliações de impacto, modelagem prudencial de sistemas e revisão contínua de fluxos informacionais. A avaliação de risco e os relatórios de impacto em proteção de dados devem se tornar instrumentos centrais de decisão, especialmente diante da opacidade algorítmica e da dificuldade de auditabilidade dos arranjos sociotécnicos contemporâneos. Com isso, a perspectiva futura da proteção de dados desloca-se da simples conformidade formal para uma lógica de governança preditiva, capaz de identificar vulnerabilidades antes que elas se convertam em violações concretas.

Outra perspectiva decisiva diz respeito à consolidação do *privacy by design* e do *privacy by default* como critérios estruturantes do desenvolvimento tecnológico. Em vez de tratar a proteção de dados como etapa posterior ao lançamento de produtos, serviços ou sistemas automatizados, a literatura recente aponta para sua incorporação desde a origem da arquitetura técnica. Na leitura de Bioni (2019), a necessidade de projetar sistemas com privacidade “desde a origem” e “por padrão”, registrando finalidade, base legal, prazo de retenção e descarte ao longo de todo o ciclo de vida do dado.

Na mesma linha, Salomão e Leonarde (2026) sustentam que a LGPD deve ser elevada “de um mero instrumento de conformidade a um *framework* de design”, promovendo o *privacy by design* e o *security by design* como elementos fundamentais das fases iniciais de desenvolvimento de sistemas de IA. Essa mudança é especialmente relevante porque transforma a proteção de dados em critério de engenharia institucional e tecnológica, e não apenas em exigência documental.

A emergência da inteligência artificial também projeta uma perspectiva de fortalecimento do debate sobre explicabilidade, auditabilidade e revisão de decisões automatizadas. Em ambientes digitais complexos, a proteção de dados pessoais tende a convergir com a exigência de inteligibilidade dos sistemas que processam informações e produzem efeitos sobre a vida dos indivíduos.

Salomão e Leonarde (2026) observam que um dos pontos mais críticos da relação entre LGPD e IA está no “direito à explicação” e no direito à revisão das decisões automatizadas. Mais do que simples transparência abstrata, a perspectiva que se desenha é a de uma IA explicável, apta a fornecer justificativas compreensíveis e auditáveis sobre os critérios gerais de decisão. Isso significa que, futuramente, a proteção de dados não poderá ser dissociada de uma governança algorítmica orientada pela prestação de contas, pela possibilidade de contestação e pela limitação dos efeitos invisíveis da automação sobre os titulares.

Entre os principais fundamentos da LGPD, destacam-se os princípios da específica e necessidade, que limitam o tratamento de dados pessoais a propósitos específicos e legítimos, e o direito à transparência, que garantem aos titulares acesso claro às informações que estão sendo utilizadas. Assim, a LGPD não apenas reforça a segurança jurídica num ambiente cada vez mais digitalizado, mas também introduz um novo patamar de responsabilidade e transparência nas operações empresariais e governamentais (Salomão e Leonarde, p.16, 2026).

Em complemento, a proteção de dados pessoais diante das tecnologias emergentes aponta para uma valorização crescente de técnicas de anonimização, pseudonimização e minimização de dados. Se, no passado, a proteção da privacidade esteve fortemente associada ao consentimento e ao sigilo, as novas condições tecnológicas indicam que ela dependerá cada vez mais de escolhas estruturais sobre o volume, a qualidade e o grau de identificabilidade das informações tratadas.

A importância dessas técnicas reside no fato de que elas ampliam as possibilidades de uso legítimo de dados sem eliminar completamente as salvaguardas de privacidade. A perspectiva futura, portanto, não é a paralisação da inovação orientada por dados, mas o seu redirecionamento para modelos tecnicamente mais prudentes, que reduzam exposição indevida, limitem riscos de reidentificação e operem com maior aderência ao princípio da necessidade (Menolli *et al.*, 2025).

Souza (2025) assinala que a evolução da LGPD dependerá, em grande medida, de sua capacidade de acompanhar as mudanças tecnológicas e sociais, bem como de dialogar com regulamentações internacionais, especialmente o GDPR. Segundo o autor, essa harmonização

é essencial para facilitar a transferência segura de dados entre jurisdições e promover padrões globais de privacidade. Mais do que um alinhamento formal, essa convergência tende a ser estratégica num contexto em que plataformas, serviços em nuvem, modelos de IA e cadeias de processamento de dados operam para além das fronteiras nacionais.

Assim, uma das perspectivas mais consistentes para a proteção de dados pessoais no Brasil é sua inserção em uma governança transnacional da privacidade, na qual interoperabilidade normativa, critérios comuns de segurança e reconhecimento mútuo de padrões se tornem instrumentos de fortalecimento dos direitos dos titulares.

Nascimento, Barros e Pinto (2024) observam que a LGPD, embora represente um marco

regulatório relevante, ainda se projeta sobre um país em que a cultura de proteção de dados permanece em desenvolvimento. Essa constatação é particularmente importante para a análise prospectiva, pois indica que o futuro da proteção de dados no Brasil dependerá, em larga medida, da capacidade de transformar a privacidade em valor social compartilhado e em prática cotidiana de indivíduos, organizações e instituições públicas.

Nessa perspectiva, a educação digital assume papel central. A efetividade futura da proteção de dados não será garantida apenas pela existência de regras mais detalhadas ou por avanços tecnológicos de segurança, mas também pela formação de sujeitos capazes de compreender o significado da circulação de seus dados, os riscos associados ao ambiente digital e os mecanismos disponíveis para exercer controle sobre as informações que lhes dizem respeito. Nascimento Barros e Pinto (2024) reforçam essa necessidade ao destacar que a eficácia da LGPD depende de um esforço conjunto de governo, empresas e sociedade, com investimentos contínuos em educação e na construção de infraestrutura de suporte à proteção de dados

A formação dessa cultura de privacidade também exige revisão do modo como o consentimento é socialmente compreendido. Em ecossistemas digitais altamente dinâmicos, o aceite automático de termos extensos e pouco acessíveis demonstra que a simples formalização do consentimento não assegura, por si só, proteção real. Na leitura de Bioni (2019), é bastante preciso ao sustentar que, em serviços digitais cotidianos, as pessoas raramente leem ou compreendem plenamente os termos a que aderem, razão pela qual o consentimento precisa ser acompanhado de avisos em camadas, opções reais de recusa e redução da coleta ao estritamente necessário.

Essa formulação projeta uma perspectiva importante: a proteção de dados no futuro próximo tenderá a se apoiar menos em manifestações abstratas de vontade e mais em arquiteturas informacionais desenhadas para facilitar compreensão, escolha e controle. Em outras palavras, a cultura de privacidade não se forma apenas por discursos educativos, mas por

práticas comunicacionais e interfaces que respeitem a vulnerabilidade informacional do titular. Nesse ponto, a atuação educativa da Autoridade Nacional de Proteção de Dados torna-

se especialmente relevante. Nascimento, Barros e Pinto (2024) destacam que a ANPD não possui apenas papel sancionatório, mas também função pedagógica na disseminação de diretrizes e campanhas de conscientização. Em passagem expressiva, o texto registra que “a ANPD é a guardiã da LGPD, encarregada de garantir a eficácia da lei”, atuando tanto na fiscalização quanto na educação dos agentes de tratamento e da população (Santos, 2020, p. 120). A citação é valiosa porque permite compreender que o futuro da proteção de dados no Brasil não depende exclusivamente da intensificação de sanções, mas também da consolidação de uma regulação orientadora, capaz de fomentar aprendizado institucional e social. Assim, a cultura de privacidade projeta-se como construção coletiva, sustentada por campanhas públicas, guias técnicos, formação profissional e fortalecimento do repertório cidadão sobre direitos digitais.

A necessidade de educação e cultura de privacidade não pode ser dissociada da emergência de uma nova ética do uso de dados. Ainda de acordo com Nascimento, Barros e Pinto (2024) o Brasil ainda precisa superar barreiras de conscientização, infraestrutura e qualificação profissional para promover uma cultura de respeito à privacidade e à segurança no ambiente digital.

Já Salomão e Leonarde (2026) demonstram que a rápida expansão da IA exige não apenas conformidade jurídica, mas desenvolvimento ético e legalmente responsável da tecnologia. A articulação entre essas duas perspectivas revela um ponto fundamental: a proteção de dados pessoais, diante das tecnologias emergentes, tenderá a ser cada vez menos um tema exclusivamente jurídico e cada vez mais uma questão de formação social, desenho institucional e responsabilidade tecnológica.

3. METODOLOGIA

Para este estudo sobre os desafios da proteção de dados pessoais na era digital, a pesquisa tem como objetivo principal compreender criticamente as complexidades envolvidas

na aplicação da legislação vigente, especialmente a Lei Geral de Proteção de Dados (LGPD). Para alcançar este propósito, adotaremos uma abordagem qualitativa, concentrada na revisão bibliográfica e na análise documental.

O método hipotético-dedutivo será utilizado, permitindo formular hipóteses a partir da revisão da literatura e dos documentos analisados. Essas hipóteses serão verificadas através de dados disponíveis em relatórios de entidades públicas, dissertações, teses e outras produções científicas, conforme recomendado por Marconi e Lakatos (2021).

A natureza qualitativa da pesquisa, conforme sugerido por Gil (2010), facilitará a investigação aprofundada das questões jurídicas relacionadas à proteção de dados pessoais na era digital. Valorizaremos o contato direto com a legislação e as práticas observadas, buscando compreender tanto os aspectos comuns quanto as particularidades e significados múltiplos envolvidos.

Os procedimentos de coleta de dados serão predominantemente bibliográficos e documentais. Realizaremos uma revisão sistemática da literatura acadêmica, incluindo livros, artigos científicos, relatórios técnicos e documentos normativos relacionados à proteção de dados pessoais. Além disso, analisaremos documentos oficiais, políticas públicas, decisões judiciais e outras fontes relevantes para a pesquisa (Fonseca, 2002, p. 32).

Por meio desses procedimentos metodológicos, espera-se reunir um conjunto abrangente de informações e análises críticas que proporcionem uma compreensão embasada e aprofundada dos desafios enfrentados pelo Direito na proteção de dados pessoais na era digital.

4. ANÁLISE E DISCUSSÃO

A análise desenvolvida demonstra que a LGPD representa um avanço significativo na proteção dos dados pessoais no Brasil, mas sua efetividade ainda depende de mudanças práticas nas organizações. Para Doneda (2021), a proteção de dados está diretamente relacionada à autodeterminação informativa, pois assegura ao titular maior controle sobre suas informações pessoais. Assim, a lei não deve ser compreendida apenas como uma obrigação formal, mas como instrumento de proteção da privacidade, da dignidade humana e dos direitos fundamentais no ambiente digital.

Entretanto, observa-se que muitas instituições ainda enfrentam dificuldades para transformar as exigências legais em práticas concretas de governança, segurança e transparência. Nesse sentido, Bioni (2019) destaca que o consentimento, por si só, não é

suficiente para garantir a proteção efetiva dos dados pessoais, sendo necessário observar critérios como finalidade, necessidade e minimização. Dessa forma, a efetivação da LGPD exige planejamento institucional, capacitação profissional e adoção de mecanismos permanentes de controle.

Diante das tecnologias emergentes, como inteligência artificial e Big Data, os desafios tornam-se ainda mais complexos, pois o tratamento automatizado amplia os riscos de uso indevido, discriminação algorítmica e falta de transparência. Com base em Doneda (2021) e Bioni (2019), compreende-se que a proteção de dados deve acompanhar a inovação tecnológica, impondo limites éticos e jurídicos ao seu uso. Portanto, a consolidação da LGPD depende da articulação entre legislação, cultura de privacidade, responsabilidade organizacional e educação digital dos titulares.

5. CONSIDERAÇÕES FINAIS

O presente artigo demonstrou que a Lei Geral de Proteção de Dados Pessoais constitui

importante marco jurídico para a proteção da privacidade e dos direitos fundamentais no Brasil. Contudo, sua efetividade ainda depende de mais do que a simples existência de previsão legal, exigindo mudanças concretas nas práticas de tratamento de dados por organizações públicas e privadas.

No decorrer do estudo, verificou-se que a aplicação da LGPD enfrenta dificuldades relacionadas à governança de dados, à capacitação de profissionais, à adoção de medidas de segurança da informação e à consolidação de uma cultura institucional orientada pela responsabilidade e pela transparência. Também se observou que, diante de tecnologias emergentes como inteligência artificial e Big Data, a proteção de dados passa a demandar mecanismos mais sofisticados de controle, prevenção e acompanhamento, especialmente quanto à auditabilidade, à explicabilidade e à mitigação de riscos.

Além disso, a pesquisa evidenciou que a proteção de dados não deve ser compreendida apenas como obrigação regulatória, mas como elemento essencial para a confiança nas relações digitais. Nesse sentido, a educação digital dos titulares, o fortalecimento da atuação regulatória e a incorporação da privacidade desde a concepção dos sistemas mostram-se medidas relevantes para o aprimoramento da aplicação da LGPD.

Conclui-se, portanto, que a legislação representa avanço significativo, mas sua plena eficácia depende da articulação entre regulação, governança, tecnologia e conscientização

social. Assim, o fortalecimento da proteção de dados pessoais no Brasil requer não apenas conformidade formal, mas compromisso efetivo com a privacidade, a segurança da informação e o respeito à dignidade da pessoa humana.

REFERÊNCIAS

AMARAL, Fernando. **Introdução à ciência de dados**. Rio de Janeiro: Alta Books, 2016.

BEZERRA, Arthur Coelho; WALTZ, Igor. **Privacidade, neutralidade e inimizabilidade da**

internet no Brasil: avanços e deficiências no projeto do marco civil. Revista Eletrônica Internacional de Economia Política da Informação, da Comunicação e da Cultura –Revista Eptic Online, v. 16, n. 2, p.161-175, maio/ago. 2014. Disponível em:
<http://ridi.ibict.br/handle/123456789/858>.

BIONI, Bruno. **Proteção de dados pessoais:** a função e os limites do consentimento. São Paulo: Editora Revista dos Tribunais, 2019.

BOTELHO, Marcos César. A **proteção de dados pessoais enquanto direito fundamental:** considerações sobre a lei geral de proteção de dados pessoais. Revista Argumenta, n. 32, p. 191- 207, 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014.

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. Disponível em:
http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 2 set. 2025.

DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. São Paulo (SP):Editora **Revista dos Tribunais**. 2021. Disponível em: <https://www.jusbrasil.com.br/doutrina/da-privacidade-a-protecao-de-dados-pessoais/1394837157>.

FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (coords.). **Comentários à lei geral de proteção de dados:** Lei 13.709/2018. São Paulo: Editora Revista dos Tribunais, 2019.

FERREIRA, Daniela Assis Alves; PINHEIRO, Marta Macedo Kerr; MARQUES, Rodrigo Moreno. **Privacidade e proteção de dados pessoais:** perspectiva histórica. InCID: Revista de Ciência da Informação e Documentação, Ribeirão Preto, Brasil, v. 12, n. 2, p. 151-172,

2021. DOI: 10.11606/issn.2178-2075.v12i2p151172.

Disponível em: <https://www.revistas.usp.br/incid/article/view/179778>.

FONSECA, João José Saraiva. **Apostila de metodologia da pesquisa científica**. João José Saraiva da Fonseca, 2002.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2010.

NASCIMENTO, Francileuza Ferreira do; BARROS, Milena de Lourdes Carvalho; PINTO, Anderson de Sousa. A proteção de dados pessoais e a LGPD no Brasil: desafios e perspectivas. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 10, n. 12, dez. 2024. DOI: 10.51891/rease.v10i12.17628.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva, 2019.

SALOMÃO, Pedro Emílio Amador; LEONARDE, Geovana Silveira Soares. A convergência crítica entre a Lei Geral de Proteção de Dados (LGPD) e a Inteligência Artificial: desafios e perspectivas jurídicas no cenário brasileiro. **RJNM**, [S. l.], v. 7, n. 02, p. 1-19, 2026. DOI: [10.66104/rrekch68](https://doi.org/10.66104/rrekch68). Disponível em: <https://jrnrm.ojsbr.com/juridica/article/view/6012>. Acesso em: 7 abr. 2026.

SOUZA, Kadmiel Duarte. Lei Geral de Proteção de Dados (LGPD): impactos, desafios e perspectivas no cenário jurídico e empresarial do Brasil. **Revista Mato-grossense de Direito**, [S. l.], v. 3, n. 1, p. 15-25, 2025. Disponível em: <https://revistas.fasipe.com.br/index.php/REMAD/article/view/466>. Acesso em: 7 abr. 2026.

[1] Acadêmico do 10º Período do Curso de Direito da Faculdade Boas Novas – FBN, e-mail: walberfreire@hotmail.com.

[2] Doutorando em Educação (UFAM), Mestre em Educação (UFAM), Especialista em Direito Público (UEA), Bacharel em Direito (UNIP) e em Relações Internacionais (Faculdade La Salle).
E-mail: igor.camara@fbnovas.edu.br.