

O IMPACTO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NAS RELAÇÕES DE CONSUMO

The impact of the General Data Protection Law (LGPD) on consumer relations

Diana Vitória Guereschi Machado¹

Williane Tibúrcio Facundes²

MACHADO, Diana Vitória Guereschi; FACUNDES, Williane Tibúrcio. O impacto da Lei Geral de Proteção de Dados (LGPD) nas relações de consumo. 29 páginas. Trabalho de Conclusão de Curso de graduação em Direito – Centro Universitário UNINORTE, Rio Branco. 2026.

¹ Discente do curso de bacharelado em Direito pelo Centro Universitário UNINORTE.

² Docente do Centro Universitário Uninorte. Graduada em Direito pela U:VERSE. Especialista em Psicopedagogia, Direito Digital e Educação Especial e Inclusiva. Graduada em Letras Vernáculas pela Universidade Federal do Acre - UFAC.

RESUMO

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) representa um importante marco regulatório no ordenamento jurídico brasileiro, especialmente no contexto das relações de consumo, cada vez mais influenciadas pela economia digital e pelo uso intensivo de dados pessoais. O presente estudo analisa os impactos da LGPD nas relações entre consumidores e fornecedores, destacando as transformações promovidas na coleta, armazenamento, tratamento e compartilhamento de informações pessoais. A pesquisa aborda os fundamentos da legislação, seus princípios estruturantes e os direitos assegurados aos titulares dos dados, evidenciando a ampliação da proteção jurídica da privacidade e da autodeterminação informativa. Examina-se, ainda, a responsabilidade dos fornecedores quanto à adoção de medidas de segurança, transparência e governança de dados, bem como os reflexos da norma nas práticas de marketing, publicidade direcionada e personalização de ofertas. Também são analisadas as consequências jurídicas decorrentes do descumprimento da LGPD, incluindo sanções administrativas aplicadas pela Autoridade Nacional de Proteção de Dados e a responsabilização civil por danos causados aos titulares. O estudo demonstra que a proteção de dados passou a integrar a dinâmica das relações de consumo como elemento essencial para a construção da confiança entre consumidores e empresas. Conclui-se que a efetividade da LGPD depende da atuação conjunta do poder público, das organizações e dos próprios consumidores, exigindo investimentos contínuos em conformidade, educação digital e governança da informação. Nesse cenário, a legislação contribui para a promoção de um ambiente de consumo mais seguro, transparente, ético e compatível com os direitos fundamentais na sociedade da informação.

Palavras-chave: LGPD; relações de consumo; privacidade; consumidor; responsabilidade civil.

ABSTRACT

The General Data Protection Law (Law No. 13,709/2018) represents a significant regulatory milestone in the Brazilian legal system, particularly within consumer relations, which are increasingly shaped by the digital economy and the intensive use of personal data. This study analyzes the impacts of the LGPD on the relationship between consumers and suppliers, emphasizing the transformations introduced in the collection, storage, processing, and sharing of personal information. The research examines the foundations of the legislation, its guiding principles, and the rights granted to data subjects, highlighting the expansion of legal protection for privacy and

informational self-determination. Furthermore, it discusses the responsibilities of suppliers regarding the adoption of security measures, transparency practices, and data governance mechanisms, as well as the effects of the law on marketing strategies, targeted advertising, and personalized offers. The study also addresses the legal consequences arising from non-compliance with the LGPD, including administrative sanctions imposed by the National Data Protection Authority and civil liability for damages caused to data subjects. The findings demonstrate that data protection has become an essential component of consumer relations, strengthening trust between consumers and businesses. It is concluded that the effectiveness of the LGPD depends on the coordinated efforts of public authorities, organizations, and consumers themselves, requiring continuous investments in compliance, digital education, and information governance. In this context, the legislation contributes to the development of a safer, more transparent, ethical, and rights-oriented consumer environment in the information society.

Keywords: LGPD; consumer relations; privacy; consumer rights; civil liability.

INTRODUÇÃO

A expansão do ambiente digital modificou profundamente a forma como as informações pessoais são coletadas, compartilhadas e exploradas nas relações sociais e econômicas. No cotidiano do consumo, os dados deixaram de ter papel apenas cadastral e passaram a influenciar ofertas, publicidade, crédito, fidelização e o próprio acesso a produtos e serviços.

Nesse cenário, a proteção da privacidade e da autodeterminação informativa ganhou centralidade, pois o tratamento de dados pessoais passou a representar não apenas uma questão técnica, mas também jurídica, econômica e ética. A Lei Geral de Proteção de Dados Pessoais (Brasil, 2018) foi editada com o objetivo de estabelecer parâmetros de uso dessas informações legítimas, impondo limites ao poder de coleta e tratamento por parte de empresas, órgãos públicos e demais agentes envolvidos.

Assim, este trabalho analisa o impacto da LGPD nas relações de consumo, com foco nas mudanças produzidas pela lei na atuação dos fornecedores, na proteção dos direitos dos titulares e na reorganização das práticas empresariais, especialmente em matéria de coleta de dados, consentimento, transparência, publicidade direcionada e responsabilidade civil. A proposta é demonstrar que a

LGPD não se limita a um conjunto de critérios formais, mas redefine a forma como a confiança deve ser construída entre consumidor e fornecedor.

1 FUNDAMENTOS DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei n. 13.709/2018 instituiu, no ordenamento jurídico brasileiro, um regime geral de proteção de dados pessoais voltado à disciplina do tratamento de informações que identifiquem ou possam identificar uma pessoa natural. Seu propósito é garantir maior controle ao titular sobre seus dados, ao mesmo tempo em que estabelece deveres de conformidade aos agentes de tratamento e cria bases jurídicas para um uso mais responsável e transparente dessas informações (Brasil, 2018; Doneda; Mendes; Cueva, 2020).

1.1 HISTÓRICO E EVOLUÇÃO DA LEGISLAÇÃO

A proteção de dados pessoais, por estar diretamente relacionada à privacidade, à intimidade e à autodeterminação informativa, consolida-se ao longo do tempo como tema central no debate jurídico contemporâneo. Embora a preocupação com a preservação da vida privada acompanhe a história das relações sociais, foi sobretudo no contexto da expansão tecnológica e do aumento do fluxo de informações que a necessidade de uma disciplina normativa específica se tornou mais evidente. Nesse sentido, a proteção de dados deixou de ser um assunto periférico para posição estratégica na tutela dos direitos fundamentais.

No plano internacional, a Declaração Universal dos Direitos Humanos, de 1948, já indicava a relevância da proteção contra interferências arbitrárias na vida privada e nos assuntos pessoais, revelando a preocupação da comunidade internacional com a preservação da esfera individual (ONU, 1948). Nas décadas mais tarde, a partir dos anos 1970, o Conselho da Europa passou a desenvolver parâmetros iniciais à privacidade e à proteção de dados, incentivando os Estados a estruturarem normas próprias sobre o tema. Em seguida, em 1981, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) publicou diretrizes fundamentais sobre privacidade e fluxos transfronteiriços de informações pessoais, que contribuiu para o desenvolvimento de uma compreensão mais ampla acerca da proteção de dados pessoais na circulação entre diferentes jurisdições.

No Brasil, esse processo acompanhou a evolução constitucional e legislativa do país. A Constituição Federal de 1988 passou a tutelar de forma expressa a intimidade e a vida privada, conferindo base jurídica relevante à proteção da pessoa humana no ambiente social e informacional (BRASIL, 1988). Como observa Medeiros (2024, p. 2), a proteção de dados era tratada, naquele momento, de maneira reflexa, como desdobramento da tutela da intimidação, especialmente porque os dados pessoais se vinculam diretamente aos direitos da personalidade:

A evolução legislativa no Brasil também seguiu as tendências internacionais de proteção de dados. A Constituição Federal de 1988, em seu texto original, tutela o direito à intimidade e à vida privada. A proteção de dados era tratada de forma reflexa pela redação original do inciso X, do art. 5º da Constituição Federal, como consectário da intimidade, haja vista que os dados pessoais são direitos inatos à personalidade dos indivíduos e, portanto, são direitos fundamentais. O Código de Defesa do Consumidor, já em 1990, identificou a vulnerabilidade do Consumidor e previu a possibilidade de acesso de dados que estiverem em poder da empresa, ao destinar uma seção própria para tratar da temática do banco de dados e dos cadastros dos consumidores. Anos mais tarde, o Brasil edita o Marco Civil da Internet (Lei nº 12.965/2014), o qual buscou proteger os direitos à intimidade e à liberdade de expressão do cidadão na utilização da internet. Era necessário criar meios mais específicos de segurança e proteção para os dados pessoais, desde a sua coleta até o seu descarte, não apenas referente ao meio digital, mas relativos aos dados que são coletados e tratados fisicamente.

O Código de Defesa do Consumidor também contribuiu de forma importante para esse percurso ao considerar a vulnerabilidade do consumidor e disciplinar, na seção própria, os bancos de dados e cadastros de consumidores, antecipando preocupações que mais tarde seriam aprofundadas pela legislação específica (Brasil, 1990; Medeiros, 2024):

Posteriormente, o Marco Civil da Internet representou novo avanço ao fortalecer a proteção da privacidade, da intimidade e da liberdade de expressão no ambiente digital (Brasil, 2014). Ainda assim, o cenário normativo brasileiro permanece fragmentado, com regras dispersas em diplomas distintos, sem uma disciplina geral e sistemática capaz de organizar o tratamento de dados pessoais de maneira abrangente. Essa lacuna normativa contribuiu para a insegurança jurídica e dificultou a uniformização dos critérios aplicáveis ao tratamento de informações pessoais, tanto no meio digital quanto nas interações presenciais e comerciais.

Conforme destaca Doneda, Mendes e Cueva (2020), a LGPD é resultado de um amplo debate e representa a sistematização de uma matéria que, então até, era tratada de forma esparsa pelo ordenamento jurídico. A sua promulgação reflete, portanto, a necessidade de conferir maior coerência normativa à tutela dos dados pessoais e de alinhar o Brasil às tendências internacionais de proteção da privacidade.

Antes mesmo da LGPD, já se percebia no cenário nacional a preocupação com a orientação do tema. Conforme indicado no texto original, em 1997 houve uma iniciativa política voltada para a criação de uma lei de proteção dos cidadãos, o que demonstra que a discussão sobre o assunto antecedeu em muito a promulgação da norma de 2018. Até então, a proteção de informações sensíveis permaneceu associada ao sigilo profissional e às disposições já previstas no Código Penal e no Código de Processo Penal (Brasil, 1940; Brasil, 1941).

A sanção da LGPD, assim, não representa apenas a criação de uma nova lei, mas a consolidação de um novo paradigma regulatório. Como aponta Lilla (2023), uma norma alterou significativamente a forma como o Brasil passou a compreender privacidade e segurança da informação, ao instituir um regime geral de proteção de dados que complementa e organiza o arcabouço normativo existente. Na mesma linha, Cotta (2020, p. 68) destaca que a ausência de uma lei geral produz insegurança jurídica e descompasso com as tendências internacionais, ao passo que a LGPD unificou regras, fortaleceu os direitos dos titulares e ampliou a competitividade do país no cenário global, senão vejamos:

A ausência de uma lei geral de proteção de dados no Brasil, até a promulgação da LGPD, criava um cenário de insegurança jurídica e de descompasso com as tendências internacionais. A fragmentação da matéria em diversas leis setoriais, como o Código de Defesa do Consumidor e o Marco Civil da Internet, embora relevante, não era suficiente para garantir uma proteção integral e sistemática dos dados pessoais. A LGPD, ao unificar e consolidar as regras sobre o tratamento de dados, não apenas fortalece os direitos dos titulares, mas também posiciona o Brasil em um patamar de maior competitividade no cenário global, facilitando o fluxo internacional de dados e a atração de investimentos. (Cotta 2020, p. 68)

Dessa forma, a evolução legislativa da proteção de dados no Brasil evidencia uma passagem de tutela fragmentada e indireta para um regime jurídico próprio, mais coerente e abrangente. A LGPD, ao sistematizar a matéria, reafirma a

centralidade da privacidade, da dignidade da pessoa humana e da segurança jurídica, ao mesmo tempo em que estabelece disposições mais claras para a coleta, o uso e o compartilhamento de dados pessoais. Trata-se, portanto, de um avanço normativo que busca equilibrar a circulação de informações, o desenvolvimento tecnológico e a proteção dos direitos fundamentais dos titulares.

1.2 PRINCÍPIOS DA LGPD

A Lei Geral de Proteção de Dados Pessoais estabelece, em seu art. 6º, um conjunto de princípios que orienta toda atividade de tratamento de dados no Brasil. Esses princípios não possuem apenas função declaratória, eles definem os limites de atuação dos agentes de tratamento, indicam os parâmetros de legitimidade da coleta e do uso das informações e funcionam como critérios de interpretação da própria lei. Como observam Oliveira, Ferreira e Pires (2021), os princípios da LGPD estão expressamente incorporados ao texto legal e são essenciais para a proteção de dados pessoais. Doneda, Mendes e Cueva (2020) também destacam que o descumprimento desses princípios compromete a licitude do tratamento e pode ensejar responsabilização jurídica. No plano prático, isso significa que a conformidade com a LGPD não se resume à existência de políticas formais, mas exige postura efetiva de cuidado, controle e transparência por parte das organizações.

A relevância desses princípios decorre do fato de que a proteção de dados pessoais, na LGPD, está vinculada à tutela da dignidade da pessoa humana, da privacidade e da autodeterminação informativa. Nos termos concretos, Geraldo Leal (2021) aponta que a aplicação cotidiana desses comandos legais é necessária para a adequação das empresas e instituições, sobretudo porque a legislação impõe deveres objetivos de conduta, e não apenas recomendações genéricas.

Além disso, os princípios da LGPD têm forte conexão com os direitos dos titulares e com as obrigações dos agentes de tratamento. Quando desrespeitados, podem gerar consequências como eliminação de dados, bloqueio, comunicação de incidentes, responsabilização civil e sanções administrativas aplicadas pela Autoridade Nacional de Proteção de Dados. Por isso, sua função é dupla: ao mesmo tempo em que protegem o titular, orientam a conduta dos controladores e operadores. Em outras palavras, os princípios são o eixo normativo que permite

compreender quando o tratamento é legítimo e quando passa a representar violação à legislação.

1.2.1 PRINCÍPIO DA FINALIDADE

O princípio da finalidade, previsto no art. 6º, I, da LGPD, exige que o tratamento de dados pessoais seja realizado para fins legítimos, específicos, explícitos e informados ao titular. Esse comando é central porque impede que a coleta ocorra de forma aberta, vaga ou indefinida. Não basta dizer que os dados serão “utilizados para fins operacionais” ou “para melhorar a experiência do usuário”; é necessário indicar, de modo claro, qual será a finalidade específica do tratamento e como ela se relaciona com a relação jurídica estabelecida.

Na prática, a finalidade funciona como um limite de vinculação. Os dados devem ser tratados apenas dentro da finalidade comunicada, e qualquer desvio posterior exigirá nova base legal ou nova autorização compatível com situações concretas. Doneda, Mendes e Cueva (2020) destacam que a clareza na informação é indispensável para que o titular compreenda o destino de seus dados e possa exercer controle real sobre sua utilização. Por isso, a finalidade também se conecta à boa fé objetiva e à confiança, especialmente nas relações de consumo, nas quais o consumidor, em regra, não tem controle técnico sobre os sistemas que armazenam e processam suas informações.

Esse princípio é particularmente importante porque evita o chamado uso secundário indevido dos dados, isto é, a reaplicação das informações para objetivos diversos daqueles inicialmente apresentados. Sem esse limite, a coleta poderia se tornar ampla, abrindo espaço para perfilamento abusivo, compartilhamentos ocultos e práticas incompatíveis com a expectativa legítima do titular.

1.2.2 PRINCÍPIO DA NECESSIDADE

O princípio da necessidade determina que o tratamento deve ser para a realização da finalidade informada ao titular. Trata-se de uma das garantias mais relevantes da LGPD, porque combate diretamente a lógica da coleta excessiva, muito comum em ambientes digitais e em cadastros de consumo. Esse princípio dialoga com a ideia de minimização de dados, que busca reduzir riscos de vazamento, uso indevido e exposição desnecessária da esfera privada do titular.

Donda (2021), ao tratar da implementação da prática da LGPD, destaca justamente a importância de que as organizações revisem seus fluxos internos para evitar a retenção excessiva de informações e a coleta de dados sem pertinência real. Em termos empresariais, isso implica revisar formulários, contratos, cadastros e rotinas internacionais, de modo a excluir o que não seja efetivamente necessário.

A observância desse princípio é especialmente importante nas relações de consumo, porque muitas práticas comerciais tendem a solicitar dados em volume superior ao necessário para a prestação do serviço. Nesses casos, a necessidade atua como barreira contra excessos e como instrumento de contenção da assimetria entre consumidor e fornecedor. Em resumo, ela impede que a coleta de dados seja convertida em prática automática ou abusiva.

1.2.3 PRINCÍPIO DA TRANSPARÊNCIA

O princípio da transparência é um dos pilares da LGPD porque garante que o titular tenha acesso claro, preciso e acessível às informações sobre o tratamento de seus dados pessoais. Mais do que divulgar políticas genéricas, a lei exige uma comunicação funcional, eficaz e útil. Isso significa que o titular deve saber quais dados são coletados, para quais especificamente, com quem podem ser compartilhados, por quanto tempo serão mantidos e quais são seus direitos diante desse tratamento.

A transparência está diretamente ligada ao direito de acesso e ao exercício consciente da autodeterminação informativa. Sem informações adequadas, o titular não consegue avaliar se o tratamento é legítimo nem exercer, de forma real, os direitos garantidos pela LGPD. Doneda, Mendes e Cueva (2020) ressaltam que a transparência é condição essencial para a efetividade da legislação, pois o controle do titular depende da qualidade da informação que lhe é fornecida. Em outras palavras, não há proteção de dados eficaz quando o titular é mantido em ignorância sobre a forma como suas informações são usadas.

Esse princípio também possui grande relevância nas relações de consumo, porque a assimetria informacional é uma das marcas mais fortes desse tipo de relação. O consumidor normalmente não domina os mecanismos técnicos de coleta e seleção de dados. Por isso, a transparência funciona como instrumento de correção

dessa assimetria, fortalecendo a confiança e permitindo que a relação de consumo seja conduzida de maneira mais leal e equilibrada.

1.3 DIREITOS DOS TITULARES DE DADOS

A Lei Geral de Proteção de Dados Pessoais (Brasil, 2018) assegura ao titular uma série de direitos destinados a ampliar sua capacidade de controle sobre o tratamento de suas informações. Esses direitos são expressão direta da preocupação da LGPD com a proteção da privacidade, da transparência e da autodeterminação informativa, especialmente em um contexto no qual dados pessoais circulam com grande intensidade entre empresas, plataformas digitais e demais agentes de tratamento.

Cumpra destacar que parte desses direitos possui especial relevância por dialogar com os próprios princípios da lei, sobretudo os princípios do livre acesso, da transparência, da necessidade e da qualidade dos dados. O direito de acesso, por exemplo, permite que o titular conheça quais informações estão sendo protegidas, enquanto o direito de retificação garante a correção de dados incompletos, inexatos ou desatualizados. Já os direitos de anonimização, bloqueio e exclusão funcionam como mecanismos de contenção do tratamento indevido, permitindo que o titular reaja quando houver excesso, irregularidade ou ausência de fundamento jurídico adequado (Doneda; Mendes; Cueva, 2020).

Na prática, a efetividade desses direitos depende da postura dos agentes de tratamento e da existência de mecanismos acessíveis para o atendimento das solicitações dos titulares. Não basta que a lei preveja os direitos em abstrato; é necessário que as organizações disponham de canais adequados, procedimentos claros e respostas em tempo razoável. É justamente nesse ponto que a LGPD deixa de ser uma norma meramente programática e passa a exigir a condução de condutas concretas, capazes de transformar a proteção de dados na realidade cotidiana.

2 RELAÇÕES DE CONSUMO NO CONTEXTO DA LGPD

A Lei Geral de Proteção de Dados (LGPD) representa um marco regulatório significativo no Brasil, impactando profundamente as relações de consumo. A interação entre consumidores e fornecedores, que antes era regida principalmente pelo Código de Defesa do Consumidor (CDC), agora se vê

complementada e fortalecida pelas disposições da LGPD, onde visa garantir a privacidade e a proteção dos dados pessoais dos indivíduos. Essa nova camada de proteção é crucial em um cenário onde a coleta e o tratamento de dados se tornaram onipresentes nas transações comerciais e na personalização de serviços e produtos.

2.1 DEFINIÇÃO DE RELAÇÕES DE CONSUMO

As relações de consumo, nos termos do Código de Defesa do Consumidor, caracterizam-se pela presença de três elementos centrais: consumidor, fornecedor e produto ou serviço (BRASIL, 1990). Considera-se consumidora toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatária final, ao passo que fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, além dos entes despersonalizados, que desenvolve atividades de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos, bem como de prestação de serviços (Brasil, 1990).

Nesse contexto, a Lei Geral de Proteção de Dados Pessoais se insere como instrumento normativo fundamental para disciplinar o tratamento de dados pessoais, os quais são essenciais para a execução de inúmeras relações de consumo (BRASIL, 2018). Em razão do avanço tecnológico e da intensificação do uso de ferramentas digitais, as empresas passaram a empregar dados pessoais para fins de personalização de produtos, serviços e publicidade, o que torna o tema cada vez mais relevante no mercado de consumo.

Embora esse uso possa ampliar a oferta de bens e serviços mais ajustada ao perfil do consumidor, também pode gerar novas vulnerabilidades, especialmente quando o tratamento massificado de dados não é devidamente percebido ou compreendido pelos consumidores.

A conexão entre a defesa da(o) consumidora(consumidor) e a proteção de dados pessoais é cada dia mais presente na sociedade moderna em que vivemos, onde, graças ao avanço tecnológico, as empresas buscam ao máximo a personalização da produção, da comercialização e da publicidade. No mercado de consumo, os dados pessoais obtidos por meio da utilização de novas tecnologias da informação se transformam em um recurso essencial e valioso. O uso destas tecnologias que permitem o tratamento massificado de dados pessoais muitas vezes não são percebidas como nocivas pelas(os) consumidoras(es). Isso se observa em diversas situações que merecem reflexão. Se por um lado o aumento de informações pessoais disponíveis às(aos) fornecedoras(es) resulta em aumento de bens e serviços personalizados, por outro pode ocasionar também a discriminação da(o) consumidora(consumidor) no mercado. (Ministério Público do Estado do Espírito Santo, 2025, p. 6).

Portanto, a relação entre a tutela do consumidor e a proteção de dados pessoais tornou-se, portanto, cada vez mais evidente na sociedade contemporânea, marcada pela ampla circulação de informações e pela crescente dependência de tecnologias da informação. Deste modo, o aumento das informações disponíveis aos fornecedores pode favorecer a personalização de bens e serviços, mas também pode ocasionar discriminação no mercado de consumo.

2.2 RESPONSABILIDADES DOS FORNECEDORES E PRESTADORES DE SERVIÇOS

No âmbito das relações de consumo, os fornecedores e prestadores de serviços não respondem apenas pela qualidade e pela adequação dos bens e serviços disponibilizados, mas também pela observância dos deveres relacionados à proteção dos dados pessoais tratados em suas atividades. Nesse sentido, a conformidade com a Lei Geral de Proteção de Dados Pessoais e com o Código de Defesa do Consumidor exige a adoção de medidas efetivas de segurança, governança e transparência, voltadas à proteção das informações desde a coleta até o descarte, inclusive quanto ao compartilhamento, armazenamento e tratamento realizado por terceiros (Brasil, 1990; Brasil, 2018).

Para mitigar riscos e garantir o cumprimento das normas aplicáveis às empresas, é necessário que, ao implementarem políticas internas de segurança da informação, mecanismos de controle de acesso, registros de tratamento e procedimentos de resposta a incidentes. A omissão ou a inobservância dessas medidas pode acarretar consequências administrativas e civis, inclusive a

responsabilização por danos materiais ou morais decorrentes da violação da legislação de proteção de dados, nos termos do art. 42 da LGPD (Brasil, 2018).

O artigo 42 da LGPD estabelece que o controlador ou operador que causar dano material ou moral, individual ou coletivo, decorrente da violação da legislação de proteção de dados pessoais, fica obrigado a repará-lo. Essa responsabilidade é objetiva, ou seja, independe da comprovação de culpa, bastando a existência do dano e do nexo causal. Além disso, a lei prevê a inversão do ônus da prova em favor do titular dos dados, o que significa que a empresa terá que provar que não houve violação ou que o dano não foi causado por sua ação ou omissão. Essa disposição visa proteger o consumidor, que muitas vezes não possui os meios para comprovar a ocorrência de um vazamento ou uso indevido de seus dados (Hauer 2020, p. 1)

A jurisprudência brasileira vem consolidando o entendimento de que as empresas possuem dever objetivo de proteção dos dados pessoais dos consumidores, especialmente quando o tratamento dessas informações integra a atividade econômica desenvolvida. A jurisprudência já reconheceu que falhas na segurança de dados podem configurar defeito na prestação do serviço, atraindo a responsabilidade objetiva prevista no Código de Defesa do Consumidor, senão vejamos:

JUIZADO ESPECIAL CÍVEL. RECURSO INOMINADO. CONSUMIDOR. SERVIÇOS BANCÁRIOS. OPERAÇÕES REALIZADAS MEDIANTE FRAUDE. FALSO CONTATO. PRELIMINAR DE ILEGITIMIDADE PASSIVA. REJEITADA. DEVER DE SEGURANÇA. FALHA NA PRESTAÇÃO DO SERVIÇO. CONSUMIDORA IDOSA. HIPERVULNERABILIDADE. RESPONSABILIDADE OBJETIVA SÚMULA 479 DO STJ. VAZAMENTO DE DADOS. ARTS. 42 E 43 DA LGPD. DANOS MATERIAIS. COMPROVADOS. DANOS MORAIS. NÃO CONFIGURADOS. RECURSO CONHECIDO E NÃO PROVIDO. (TJDFT, 2025)

Portanto, a tutela do titular dos dados reforça a necessidade de interpretação das relações de consumo à luz dos princípios da transparência, da boa-fé e da confiança legítima, especialmente porque o consumidor, muitas vezes, não dispõe dos meios técnicos necessários para comprovar vazamentos, uso indevido ou tratamento irregular de suas informações (Hauer, 2020, p. 1).

Dessa forma, a proteção de dados pessoais nas relações de consumo ultrapassa o caráter meramente operacional da atividade empresarial, configurando verdadeiro dever jurídico integrado à própria dinâmica do mercado de consumo. Em

consonância com essa compreensão, a LGPD e o Código de Defesa do Consumidor reforçam a necessidade de práticas responsáveis e preventivas, de modo a promover não apenas os componentes de danos, mas também a prevenção de condutas lesivas e as declarações de uma cultura organizacional orientada pela conformidade, pela ética e pelo respeito aos direitos fundamentais do consumidor (Brasil, 1990; Brasil, 2018; Ministério Público Do Estado Do Espírito Santo, 2025).

2.3 IMPACTOS DA LGPD NA COLETA E TRATAMENTO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados Pessoais, instituída pela Lei nº 13.709/2018, promove mudanças significativas na forma como as empresas realizam a coleta e o tratamento de dados pessoais no Brasil (Brasil, 2018). Antes de sua vigência, era comum a obtenção e o uso de informações de forma ampla e, muitas vezes, sem a definição clara da finalidade do tratamento ou sem a devida transparência perante o titular. Com a entrada em vigor da LGPD, essa dinâmica passou a exigir observância rigorosa aos princípios legais aplicáveis, especialmente os da finalidade, adequação, necessidade, transparência, segurança e prevenção (Brasil, 2018).

Nesse novo cenário, as organizações devem justificar a pertinência dos dados coletados, informar de maneira clara e acessível especificamente de sua utilização e adotar medidas técnicas e administrativas aptas a proteger essas informações contra acessos não autorizados, vazamentos, perdas ou qualquer forma de tratamento irregular. A LGPD (Brasil, 2018), assim, não apenas disciplina o uso de dados pessoais, mas também reforça a necessidade de revisão dos processos internos, das políticas de privacidade e dos sistemas de segurança da informação, de modo a garantir maior controle ao titular e reduzir riscos jurídicos e reputacionais.

A Lei Geral de Proteção de Dados representa importante instrumento de proteção do consumidor na sociedade da informação, especialmente diante da intensificação do uso de tecnologias digitais e da crescente circulação de dados pessoais nas relações de consumo. Conforme observam Otero e Yaegashi (2024, p. 1), o ambiente digital ampliou significativamente a vulnerabilidade do consumidor, tornando necessária a criação de mecanismos jurídicos capazes de limitar o uso

indiscriminado de informações pessoais e assegurar maior controle do titular sobre seus dados.

Nesse contexto, a LGPD estabelece diretrizes claras sobre a coleta, o armazenamento, o processamento e a proteção de dados pessoais, solicitando consentimento explícito em determinadas hipóteses, indicação precisa da específica e mecanismos de segurança contra acessos indevidos ou vazamentos. Essa mudança de paradigma exige às empresas uma postura mais diligente e responsável, em consonância com os direitos fundamentais à privacidade e à autodeterminação informativa.

Dessa forma, a adequação à LGPD deixa de ser mera formalidade legal e passa a integrar a própria governança corporativa, a alternativa institucional e a sustentabilidade das atividades empresariais em uma sociedade cada vez mais orientada pelo uso intensivo de dados.

3 IMPACTOS DA LGPD NAS PRÁTICAS DE MARKETING E PUBLICIDADE

A promulgação da Lei Geral de Proteção de Dados representou um marco relevante para as práticas de marketing e publicidade no Brasil, especialmente porque deslocou o foco das empresas para a observância da transparência, da legalidade e da proteção dos direitos dos titulares dos dados (BRASIL, 2018). Nesse contexto, estratégias antes baseadas na ampla captação e no uso envolvido de informações passaram a exigir maior cautela, planejamento e justificativa jurídica. A personalização de campanhas, embora possível, deve agora ser compatível com os limites legais e com o respeito à privacidade do consumidor.

3.1 CONSENTIMENTO DO CONSUMIDOR

O consentimento passou a ocupar posição central na conformidade das práticas de marketing. Nos termos do art. 7º da LGPD, o tratamento de dados pessoais pode ocorrer mediante consentimento livre, informado e inequívoco do titular, ou que deve ser concedido para determinadas e pode ser revogado a qualquer momento (BRASIL, 2018). Nesse sentido, o consentimento não pode ser genérico nem obtido por meio de cláusulas amplas e pouco transparentes, devendo a empresa

explicar, de forma clara, como os dados serão utilizados em campanhas publicitárias, ações promocionais e processos de personalização.

Vasconcelos Camurça e Matias (2021, p. 1) destacam que o consentimento, nas práticas de publicidade direcionada, deve ser interpretado à luz da transparência e da autodeterminação informativa, evitando mecanismos obscuros de captação de dados que dificultem a compreensão do consumidor acerca do uso de suas informações pessoais.

A utilização de dados pessoais para direcionamento de publicidade exige transparência quanto às finalidades do tratamento e respeito à autodeterminação informativa do titular. O consentimento não pode ser obtido por mecanismos obscuros ou por estruturas que dificultem a compreensão do usuário sobre o efetivo uso de seus dados pessoais, sobretudo em ambientes digitais marcados pela assimetria informacional entre consumidores e fornecedores (VASCONCELOS CAMURÇA; MATIAS, 2021, p. 1).

O consentimento consolidou-se como elemento essencial para a legitimidade das práticas de marketing no contexto da LGPD, reforçando a necessidade de transparência, clareza e respeito à autonomia do titular dos dados. A exigência de consentimento livre, informado e revogável demonstra a preocupação do legislador em assegurar que o consumidor mantenha o controle sobre suas informações pessoais, prevenindo abusos decorrentes do uso indiscriminado de dados para fins comerciais.

Nesse sentido, as empresas que adotam práticas alinhadas às disposições legais não apenas reduzem riscos jurídicos e reputacionais, mas também fortalecem a confiança dos consumidores, estabelecendo relações comerciais mais éticas, seguras e compatíveis com os princípios da proteção de dados pessoais.

3.2 PUBLICIDADE DIRECIONADA E PERSONALIZAÇÃO

A publicidade direcionada e a personalização de ofertas sempre foram estratégias relevantes para aumentar a efetividade das campanhas e a conversão de vendas. Com a LGPD, no entanto, essas práticas passaram a ser submetidas a maior controle, especialmente quando envolve o uso de dados pessoais para segmentação de público, criação de perfis comportamentais e direcionamento de anúncios (Brasil,

2018). O tratamento nessas hipóteses deve observar base legal adequada, transparência informacional e possibilidade de oposição pelo titular, quando cabível.

A LGPD busca equilibrar os interesses empresariais e os direitos fundamentais dos titulares, de modo que o uso de dados para fins de marketing não pode ocorrer de forma indiscriminada. De acordo com Baptista Luz (2020, p. 1) legislação veda a utilização de dados para fins discriminatórios, o que impõe limites à personalização quando isso puder resultar em exclusão, manipulação ou tratamento desigual dos consumidores, vejamos:

A LGPD busca equilibrar esses interesses, estabelecendo que o tratamento de dados pessoais para fins de marketing direto deve respeitar os direitos e liberdades fundamentais dos titulares. Isso implica que as empresas não podem utilizar dados de forma indiscriminada para criar perfis comportamentais e direcionar anúncios sem a devida base legal, que pode ser o consentimento ou o legítimo interesse, desde que devidamente justificado e com a possibilidade de oposição do titular. A lei também proíbe a utilização de dados para fins discriminatórios, garantindo que a personalização não resulte em exclusão ou tratamento desigual dos consumidores (Baptista Luz, 2020, p. 1).

Essa abordagem regulatória visa evitar que a personalização, embora benéfica em muitos aspectos, se torne uma ferramenta para a manipulação ou discriminação do consumidor. As empresas são agora desafiadas a inovar em suas estratégias de marketing, buscando a relevância e a eficácia sem comprometer a privacidade e os direitos dos indivíduos. A conformidade com a LGPD nesse quesito não é apenas uma obrigação legal, mas uma oportunidade para construir relações de confiança mais sólidas e duradouras com os clientes.

3.3 DESAFIOS PARA AS EMPRESAS NA ADAPTAÇÃO ÀS NOVAS REGRAS

A adaptação empresarial às exigências da LGPD no campo do marketing e da publicidade constitui desafio complexo, pois exige revisão de processos internos, atualização de políticas de privacidade, adequação de formulários de coleta de dados e implementação de mecanismos eficazes para gestão de controles e solicitações dos usuários. Além disso, as empresas precisam estruturar procedimentos adequados para garantir o exercício dos direitos dos titulares, como

acesso, correção, eliminação e oposição ao tratamento de dados, bem como adotar medidas de prevenção e resposta a incidentes de segurança (Brasil, 2018).

Conforme Fidelis, Claro e Gonçalves (2025, p. 1), a adequação das práticas de marketing à LGPD exige das empresas maior transparência na utilização de dados pessoais em campanhas comerciais, especialmente quanto à definição das finalidades do tratamento e à obtenção de consentimento válido dos consumidores.

A utilização de dados pessoais em campanhas comerciais demanda transparência, definição clara das finalidades do tratamento e observância aos princípios estabelecidos pela LGPD. Nesse contexto, o consentimento do titular assume papel central na legitimidade das estratégias de marketing, exigindo das empresas maior responsabilidade no tratamento das informações pessoais utilizadas em ações promocionais e publicitárias (Fidelis; Claro; Gonçalves, 2025, p. 1).

Superar tais desafios não representa apenas uma forma de evitar sanções, mas também uma oportunidade de fortalecer a confiança do consumidor e consolidar uma imagem institucional pautada pela responsabilidade. Nesse sentido, a conformidade com a LGPD deve ser pensada como investimento estratégico, capaz de promover segurança jurídica, complementar no mercado e relações de consumo mais éticas e transparentes.

4 CONSEQUÊNCIAS JURÍDICAS PARA O DESCUMPRIMENTO DA LGPD

O descumprimento da Lei Geral de Proteção de Dados Pessoais não configura mera irregularidade formal, mas pode acarretar consequências jurídicas relevantes para empresas e organizações, inclusive sanções administrativas, responsabilização civil e impactos reputacionais (Brasil, 2018). Nesse contexto, a Autoridade Nacional de Proteção de Dados exerce papel central na fiscalização e aplicação das medidas previstas na lei, com a finalidade de garantir a efetividade do regime jurídico de proteção de dados e a tutela dos direitos fundamentais à privacidade e à autodeterminação informativa.

4.1 SANÇÕES ADMINISTRATIVAS, MULTAS

A LGPD prevê, em seus arts. 52 a 54, um conjunto de medidas administrativas aplicáveis pela ANPD em caso de descumprimento de suas

disposições, entre as quais se advertência inclui, multa simples, multa diária, divulgação da infração, bloqueio e eliminação dos dados pessoais relacionados à infração, além de outras medidas restritivas de maior gravidade, conforme a natureza e a extensão da irregularidade (Brasil, 2018).

A aplicação das sanções administrativas previstas na LGPD demonstra o fortalecimento da atuação fiscalizatória da Autoridade Nacional de Proteção de Dados e evidencia a importância da conformidade no tratamento de dados pessoais. A imposição das primeiras multas pela ANPD reforça o entendimento de que o tratamento irregular de dados pode gerar consequências econômicas e reputacionais relevantes para as empresas (Albuquerque; Lima; Magalhães, 2025, p. 1).

As sanções administrativas passaram a produzir efeitos a partir de 1º de agosto de 2021 e as características não são apenas repressivas, mas também preventivas e pedagógicas. A advertência vem acompanhada de prazo para adoção de medidas corretivas; a multa simples pode alcançar até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no último exercício, limitado a R\$ 50.000.000,00 por infração; O dia a dia pode ser utilizado para obrigar o cumprimento das determinações da ANPD (Brasil, 2018; Albuquerque; Lima; Magalhães, 2025).

Além disso, a lei admite medidas como a publicização da infração, o bloqueio e a eliminação dos dados, a suspensão parcial do funcionamento do banco de dados e, em hipóteses extremas, a exclusão parcial ou total do exercício de atividades relacionadas ao tratamento de dados. Em conjunto, essas melhorias reforçam a necessidade de governança, prevenção e conformidade contínua.

Carvalhaes Neto e Coutinho (2019) observam que as avaliações administrativas não possuem apenas função punitiva, mas também pedagógica, na medida em que buscam induzir mudança de comportamento nos agentes de tratamento e estimular a adoção de boas práticas e programas de governança em proteção de dados. Essa perspectiva é particularmente relevante porque desloca o debate da mera proteção para a prevenção estruturada de riscos.

4.2 RESPONSABILIDADE CIVIL POR DANOS

Além das sanções administrativas, o descumprimento da LGPD pode abranger a responsabilidade civil por danos materiais e morais causados aos

titulares dos dados. O art. 42 da lei estabelece que o controlador ou o operador que, em razão do exercício de suas atividades, causar dano patrimonial, moral, individual ou coletivo em violação à legislação de proteção de dados será obrigado a repará-lo (Brasil, 2018). Trata-se de mecanismo que amplia a proteção do consumidor e fortalece a tutela da personalidade em ambiente digital.

A responsabilização civil na LGPD dialoga com a lógica protetiva do Código de Defesa do Consumidor, especialmente porque o tratamento inadequado de dados pode produzir prejuízos concretos, inclusive em razão de vazamentos, uso indevido ou exposição indevida de informações pessoais, senão vejamos o entendimento de Mendes e Biondi (2021, p. 215):

A responsabilização civil no âmbito da LGPD dialoga com a lógica protetiva do Código de Defesa do Consumidor, uma vez que o tratamento inadequado de dados pessoais pode gerar danos relevantes, tanto de ordem material quanto moral. O regime jurídico adotado se aproxima da responsabilidade objetiva, na medida em que impõe ao controlador o dever de demonstrar que não houve violação à legislação, invertendo, em certa medida, o ônus probatório em favor do titular.

Na prática, o Superior Tribunal de Justiça reconheceu que o vazamento de dados pessoais pode configurar dano moral indenizável, especialmente quando envolve dados sensíveis ou quando há exposição indevida capaz de atingir a dignidade, a honra ou a segurança do titular, vejamos:

CIVIL, CONSUMIDOR E PROCESSUAL CIVIL. RECURSO ESPECIAL. AÇÃO DE OBRIGAÇÃO DE FAZER C/C INDENIZAÇÃO POR DANOS MORAIS. TEMA 710 E SUMULA 550 DO STJ. DISTINÇÃO. BANCO DE DADOS. DISPONIBILIZAÇÃO DOS DADOS DO CADASTRADO. HIPÓTESES PREVISTAS NA LEI Nº 12.414/2011. TERCEIROS CONSULENTES. RESTRIÇÃO LEGAL. DISPONIBILIZAÇÃO INDEVIDA.

DANO MORAL PRESUMIDO. RESPONSABILIDADE OBJETIVA DO GESTOR DE BANCO DE DADOS. CONFIGURAÇÃO. 1. Ação de obrigação de fazer c/c compensação de danos morais. 2. No particular, não se aplicam o Tema 710/STJ e a Súmula 550/STJ, que tratam especificamente do *credit scoring*, ficando expressamente consignado que essa prática "não constitui banco de dados", sendo este regulamentado pela Lei nº 12.414/2011. 3. O gestor de banco de dados regido pela Lei nº 12.414/2011 somente pode disponibilizar a terceiros consulentes o score de crédito, desnecessário o consentimento prévio; e o histórico de crédito, mediante previa autorização específica do cadastrado (art. 4º, IV). Por outro lado, as informações cadastrais e de adimplemento armazenadas somente podem ser compartilhadas com outros bancos de dados (art. 4º, III). Precedentes. 4. O gestor de banco de dados que disponibiliza para terceiros consulentes o acesso aos dados do cadastrado que somente poderiam ser compartilhados entre bancos de dados (como as informações cadastrais e de adimplemento) deve responder objetivamente pelos danos morais causados ao cadastrado, que são presumidos, diante da forte sensação de insegurança por ele experimentada. Precedentes. 5. Recurso especial conhecido e provido. (Brasil, 2025)

O vazamento de dados pessoais pode gerar responsabilidade civil das empresas quando houver violação da privacidade ou exposição indevida de informações dos titulares. Conforme Silva, Barbosa Silva e Leocádio (2025, p. 1), a proteção de dados passou a integrar a esfera dos direitos da personalidade, permitindo a responsabilização do agente de tratamento pelos danos materiais e morais decorrentes do uso inadequado das informações pessoais.

Desta forma, a responsabilidade civil prevista na LGPD reforça a necessidade de as empresas adotarem postura proativa na gestão de riscos, com políticas de privacidade, segurança da informação e resposta a incidentes devidamente estruturadas. A proteção de dados deixa, assim, de ser uma preocupação específica para posição central na estratégia e na sustentabilidade dos negócios.

4.3 EXEMPLOS DE CASOS DE INFRAÇÃO

As instituições brasileiras ainda estão em processo de consolidação sobre a aplicação da LGPD, mas já há exemplos relevantes que evidenciam a concretude das consequências do descumprimento da lei, especialmente nos setores de marketing digital, serviços financeiros e tratamento intensivo de dados pessoais.

No cenário global, casos emblemáticos como os envolvendo empresas de tecnologia e companhias aéreas, que resultaram em multas milionárias sob a GDPR (General Data Protection Regulation), a versão europeia da LGPD, servem de precedente e inspiração para a aplicação da lei no Brasil. No contexto nacional, a ANPD já aplicou suas primeiras sanções, como a multa a uma empresa por tratamento irregular de dados e a notificação de diversas outras por descumprimento de regras de proteção de dados. Além disso, o Poder Judiciário tem sido acionado por consumidores que buscam indenização por danos decorrentes de vazamentos ou uso indevido de suas informações pessoais, consolidando a compreensão de que a violação da LGPD acarreta responsabilidade civil. Esses exemplos reforçam a importância de as empresas investirem em conformidade e governança de dados para evitar prejuízos financeiros e reputacionais (Costa Fernandes 2023, p. 1).

Conforme elucidado por Costa Fernandes (2023), no plano internacional, casos envolvendo grandes empresas de tecnologia e companhias aéreas, com imposição de multas expressivas sob o Regulamento Geral de Proteção de Dados, demonstram o potencial sancionatório dos regimes de proteção de dados e funcionam como parâmetro comparativo para o contexto brasileiro. No âmbito nacional, a atuação inicial da ANPD e a crescente judicialização de conflitos por vazamento ou uso indevido de dados evidenciam que uma violação da LGPD pode gerar repercussões administrativas, civis e reputacionais.

Esses casos ilustram que o descumprimento da LGPD ultrapassa a esfera das multas e alcança a confiança do consumidor, a imagem institucional e a própria continuidade das atividades empresariais. Em um mercado cada vez mais orientado pela circulação de dados, a conformidade torna-se elemento de competitividade e não apenas de defesa jurídica.

4.4 OPINIÕES DE ESPECIALISTAS E CONSUMIDORES

A implementação da LGPD estimulou amplo debate entre especialistas em direito digital, privacidade e proteção de dados, bem como entre consumidores e agentes econômicos. Em geral, a lei é percebida como marco essencial para a

modernização da tutela de dados no Brasil e para a aproximação do país aos padrões internacionais de proteção, especialmente os adotados na Europa. APDADADOS (2024) ressalta que a LGPD fortalece a cultura de privacidade ao ampliar o controle do titular e exigir maior transparência das empresas.

Por outro lado, a percepção social sobre a lei ainda é desigual. Parte significativa da população brasileira desconhece os direitos assegurados pela LGPD ou não sabe como exercê-los de modo eficaz, o que limita a concretização de sua finalidade protetiva. Esse cenário reduz a capacidade de fiscalização social e dificulta o exercício do pleno da autodeterminação informativa (Brasil, 2018). À medida que as infrações e avaliações se tornem mais visíveis, espera-se maior conscientização pública e maior exigência de práticas responsáveis por parte das empresas.

Os especialistas também apontam desafios relacionados à aplicação prática da legislação, como a necessidade de maior uniformidade regulatória, o fortalecimento institucional da ANPD e a adaptação contínua das empresas, principalmente de menor porte. Ainda assim, prevalece o entendimento de que a LGPD constitui instrumento indispensável para a construção de um ambiente digital mais seguro, confiável e respeitoso à privacidade, vejamos:

Especialistas em proteção de dados e privacidade têm destacado que, apesar dos avanços trazidos pela LGPD, ainda existem desafios significativos para sua plena efetividade. A inércia regulatória em alguns aspectos e o rigor ainda incipiente na aplicação das sanções pela ANPD são pontos de preocupação, que podem levar a um 'descrédito e desvirtuamento da lei'. A complexidade da legislação e a necessidade de adaptação contínua das empresas, especialmente as de menor porte, também são frequentemente mencionadas como obstáculos. Contudo, há um consenso de que a LGPD é um instrumento essencial para a construção de um ambiente digital mais seguro e confiável, onde a privacidade do indivíduo é respeitada e valorizada. A educação e a conscientização tanto das empresas quanto dos consumidores são apontadas como fatores cruciais para o sucesso da lei a longo prazo (APDADADOS, 2024, p. 1).

Essa dualidade entre o reconhecimento técnico da importância da norma e o conhecimento ainda insuficiente por parte dos consumidores revela a necessidade de ações permanentes de informação, formação e esclarecimento. Sem esse esforço, a efetividade da LGPD tende à permanência parcial.

5 PROPOSTAS DE APRIMORAMENTO E FUTURO DA LGPD NAS RELAÇÕES DE CONSUMO

Embora represente avanço normativo relevante, a LGPD é uma legislação dinâmica, que precisa acompanhar as transformações tecnológicas e sociais para manter sua efetividade. O futuro da proteção de dados nas relações de consumo dependerá da capacidade de atualização normativa, do fortalecimento institucional da ANPD e da consolidação de uma cultura de conformidade entre consumidores, empresas e poder público (Brasil, 2018).

Entre os temas que frequentemente exigem aprimoramento estão o tratamento de dados de crianças e adolescentes, a regulação de transferências internacionais, a aplicação da lei a tecnologias emergentes, como inteligência artificial e blockchain, e o aprimoramento dos critérios de dosimetria e aplicação das sanções. Silva, Barbosa Silva e Leocádio (2025, p. 1) ressaltam que a evolução da LGPD exige constante aperfeiçoamento dos mecanismos de responsabilização civil e proteção dos titulares de dados, especialmente diante do aumento de incidentes envolvendo vazamentos e uso indevido de informações pessoais.

Além disso, a experiência internacional, especialmente a europeia, oferece opções úteis para o aperfeiçoamento do sistema brasileiro, especialmente no que se refere à governança, à fiscalização e à responsabilização dos agentes de tratamento. A elaboração institucional de uma legislação eficiente depende, portanto, de revisão contínua, diálogo e capacidade de adaptação às novas formas de tratamento de dados.

5.1 SUGESTÕES PARA A ATUALIZAÇÃO DA LEGISLAÇÃO

Para que a LGPD continue a cumprir seu papel de forma efetiva e se mantenha alinhada com as demandas de um mundo em constante digitalização, é fundamental que a legislação seja periodicamente revisada e atualizada. As sugestões de aprimoramento frequentemente abordam a necessidade de maior clareza e detalhamento em certos dispositivos legais, a adaptação a novas tecnologias emergentes, como a inteligência artificial e o blockchain, e o fortalecimento da atuação da Autoridade Nacional de Proteção de Dados (ANPD).

A experiência de outros países que possuem legislações similares e mais maduras, como a GDPR europeia, pode servir como um valioso referencial e fonte de inspiração para ajustes e melhorias no arcabouço legal brasileiro, vejamos:

O futuro da LGPD no Brasil está intrinsecamente ligado à sua capacidade de evoluir e se adaptar aos novos desafios impostos pelo avanço tecnológico e pela complexidade das relações digitais. Especialistas e a própria ANPD têm apontado a necessidade de aprimorar a legislação em temas como o tratamento de dados de crianças e adolescentes, a regulamentação de transferências internacionais de dados e a aplicação da lei a tecnologias emergentes, como a inteligência artificial e o blockchain. Além disso, há um clamor por maior clareza nas diretrizes para a aplicação das sanções e por um fortalecimento da estrutura da ANPD, garantindo-lhe os recursos necessários para fiscalizar e educar de forma eficaz. A colaboração entre o setor público, privado e a sociedade civil é vista como essencial para construir um arcabouço legal que seja robusto, flexível e capaz de proteger os direitos dos titulares de dados em um cenário em constante mutação (Migalhas, 2025, p. 1).

Essas considerações ressaltam que a LGPD não é um documento estático, mas um organismo vivo que deve ser nutrido e adaptado para enfrentar os desafios do presente e do futuro, garantindo que a proteção de dados pessoais permaneça como um direito fundamental inalienável na era digital.

5.2 IMPORTÂNCIA DA EDUCAÇÃO E CONSCIENTIZAÇÃO DO CONSUMIDOR

A educação digital e a conscientização do consumidor são elementos essenciais para a efetividade da LGPD. Para que a proteção de dados se traduza na prática social concreta, é necessário que os titulares conheçam seus direitos e compreendam os riscos associados ao compartilhamento de informações pessoais. A falta de conhecimento pode favorecer comportamentos inseguros e reduzir a capacidade de reação diante do uso indevido de dados.

Iniciativas de educação em privacidade, campanhas de esclarecimento e inclusão do tema nos espaços formativos são medidas indispensáveis para fortalecer a cidadania digital. Isso envolve a compreensão do conceito de dado pessoal, das bases legais de tratamento, das hipóteses de consentimento e dos mecanismos de acesso, correção, eliminação e oposição previstas na lei. Capital Digital (2024, p. 1)

destaca que a promoção de informação acessível é essencial para proteger a população contra abusos, fraudes e privacidade de direitos, vejamos:

A necessária promoção da educação em proteção de dados é um pilar fundamental para a construção de uma sociedade digital mais segura e justa. A falta de conhecimento sobre a LGPD e sobre a importância da proteção de dados deixa a população vulnerável a abusos e excessos, que podem resultar em fraudes, discriminação e violação de direitos fundamentais. É imperativo que sejam desenvolvidas e implementadas políticas públicas e iniciativas privadas que visem educar os cidadãos sobre seus direitos e responsabilidades no ambiente digital. Isso inclui a criação de materiais educativos acessíveis, a realização de campanhas informativas e a inclusão do tema da proteção de dados nos currículos escolares. Somente com uma população consciente e capacitada será possível garantir o pleno exercício da autodeterminação informativa e a efetiva proteção dos dados pessoais contra usos indevidos e maliciosos (Capital Digital, 2024, p. 1).

Investir em educação e conscientização não é apenas uma medida de conformidade, mas uma forma de consolidar uma cultura de privacidade e de ampliar o exercício efetivo da autodeterminação informativa.

5.3 O PAPEL DA TECNOLOGIA NA PROTEÇÃO DE DADOS

A tecnologia ocupa posição ambivalente na proteção de dados: ao mesmo tempo em que amplia riscos de vazamento, monitoramento excessivo e uso indevido de informações, também fornece instrumentos indispensáveis para a conformidade com a LGPD. A lei exige a adoção de medidas técnicas e administrativas adequadas para proteger os dados pessoais contra acessos não autorizados e incidentes de segurança, o que torna a tecnologia uma aliada fundamental da governança de dados.

Nesse sentido, soluções como criptografia, autenticação multifator, gestão de vulnerabilidades, registros de auditoria e monitoramento contínuo são instrumentos relevantes para reduzir riscos e garantir a integridade das informações. Machado, Cata Preta e Pungirum (2024, p. 1) ressaltam que a segurança da informação constitui elemento essencial para a conformidade das empresas com a LGPD, exigindo investimentos em mecanismos de prevenção, monitoramento e proteção contra incidentes envolvendo dados pessoais, vejamos:

A proteção de dados pessoais exige das organizações a adoção de medidas técnicas e administrativas voltadas à segurança da informação, incluindo mecanismos de controle de acesso, monitoramento contínuo, gestão de vulnerabilidades e prevenção de incidentes cibernéticos. Nesse contexto, a tecnologia assume papel estratégico para garantir a conformidade com a LGPD e reduzir riscos decorrentes do tratamento inadequado de dados pessoais (Machado; Cata Preta; Pungirum, 2024, p. 1).

Além de proteger dados, a tecnologia também viabiliza respostas mais eficientes às exigências regulatórias, como gestão de consentimento, atendimento a solicitações de titulares e controle de fluxos informacionais. Assim, a conformidade com a LGPD não depende apenas de adequação jurídica, mas também da incorporação de soluções tecnológicas capazes de preservar a confidencialidade, a integridade e a disponibilidade das informações tratadas.

CONSIDERAÇÕES FINAIS

Conclui-se que a Lei Geral de Proteção de Dados Pessoais representa um marco normativo de grande relevância para as relações de consumo, na medida em que consolida uma disciplina jurídica voltada à tutela da privacidade, da autodeterminação informativa e da segurança no tratamento de dados pessoais.

Em um contexto de intensificação do uso de tecnologias digitais e ampliação da coleta de informações por empresas e plataformas, a LGPD passou a desempenhar papel central na redefinição da relação entre consumidor e fornecedor, impondo limites de atuação econômica e fortalecendo a proteção da parte mais vulnerável da relação de consumo. Assim, sua relevância ultrapassa a dimensão formal da regulamentação, projetando-se como instrumento de reorganização das práticas empresariais e de afirmação de direitos fundamentais no ambiente digital.

Verificou-se, ao longo da análise, que a conformidade com a LGPD exige das organizações muito mais do que a mera adequação documental ou a elaboração de políticas genéricas de privacidade. Trata-se de um dever contínuo de governança, transparência e responsabilização, que abrange todas as etapas do ciclo de vida dos dados pessoais, desde a coleta até o descarte. Nesse sentido, fornecedores e os prestadores de serviços devem adotar medidas técnicas e administrativas adequadas para prevenir incidentes, reduzir vulnerabilidades e garantir o exercício eficaz dos direitos dos titulares.

Do mesmo modo, as práticas de marketing, publicidade e personalização de ofertas passaram a exigir maior cautela, uma vez que a utilização de dados pessoais deve observar bases legais específicas e respeito aos limites impostos pela legislação.

Por fim, demonstramos que o descumprimento da LGPD pode acarretar consequências administrativas e civis relevantes, evidenciando o caráter coercitivo e preventivo da norma. As medidas previstas buscam não apenas punir condutas irregulares, mas também induzir uma cultura organizacional voltada à conformidade e à proteção de dados como valor institucional. Nesse cenário, a efetividade da lei depende da atuação coordenada do poder público, da postura diligente das empresas e da conscientização dos consumidores quanto aos seus direitos. Portanto, a consolidação de uma cultura de proteção de dados nas relações de consumo é condição indispensável para a construção de um ambiente digital mais ético, seguro e equilibrado.

REFERÊNCIAS

ALBUQUERQUE, Cínthya Maria Caetano; LIMA, Renata Albuquerque; MAGALHÃES, Átila de Alencar Araripe. O mercado de dados pessoais no Brasil: análise jurídica da 1ª multa imposta pela Agência Nacional de Proteção de Dados. **Prisma Jurídico**, 2025. DOI: 10.5585/2025.25730. Disponível em: <https://periodicos.uninove.br/prisma/article/download/25730/11409> . Acesso em: 27 de maio de 2026.

ANPD. **Autoridade Nacional de Proteção de Dados**. Guias e Recomendações. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes>. Acesso em: 21 set. 2025.

APDADADOS. **Especialistas debatem desafios da LGPD e clamam por medidas rigorosas para assegurar a privacidade no Brasil**. 2024. Disponível em: <https://apdados.org/noticia/especialistas-debatem-desafios-da-lgpd-e-clamam-por-medidas-rigorosas-para-assegurar-a-privacidade-no-brasil-01-11-2024>. Acesso em: 23 set. 2025.

BAPTISTA LUZ. **Publicidade Digital e o Legítimo Interesse na LGPD: o Guia**. 2020. Disponível em: <https://baptistaluz.com.br/publicidade-digital-lgpd-guia/>. Acesso em: 23 set. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 de maio de 2026.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Rio de Janeiro, RJ: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 19 de maio de 2026.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. **Código de Processo Penal**. Rio de Janeiro, RJ: Presidência da República, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm . Acesso em: 19 de maio de 2026.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet**. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/12965.htm . Acesso em: 19 de maio de 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/13709.htm. Acesso em: 21 set. 2025.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 21 set. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial n. 2.201.694/SP**. Relator: Ministro Ricardo Villas Bôas Cueva. Relatora para o acórdão: Ministra Nancy Andrighi. Julgado em 05/08/2025. Superior Tribunal de Justiça, Brasília, DF, 2025 Disponível em:https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=5&documento_sequencial=329011149®istro_numero=202500811342&peticao_numero=202500811342 Acesso em: 27 mai. 2026.

CARVALHAES NETO, Eduardo Hayden; COUTINHO, Karen Mentzingen. Enforcement da Lei Geral de Proteção de Dados e sanções. In: BEPPU, Ana Claudia; BRANCHER, Paulo Marcos Rodrigues (coord.). **Proteção de Dados Pessoais no Brasil: Uma nova visão a partir da Lei nº 13.709/2018**. Belo Horizonte: Fórum, 2019. p. 305-326.

CETIC.br. **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros**: TIC Domicílios 2019. São Paulo: Comitê Gestor da Internet no Brasil, 2019. Disponível em: https://cetic.br/media/docs/publicacoes/2/tic_domicilios_2019_livro_eletronico.pdf. Acesso em: 21 set. 2025.

COSTA FERNANDES. **5 casos de empresas multadas por conta da LGPD**. 2023. Disponível em: <https://www.costafernandes.adv.br/5-empresas-multadas-pela-lgpd>. Acesso em: 23 set. 2025.

COTTA, Regina. A evolução da proteção de dados pessoais no Brasil: a implementação da LGPD e o novo marco legal. **Revista de Direito e Informática**, v. 14, n. 2, p. 65-85, 2020.

DISTRITO FEDERAL. Tribunal de Justiça do Distrito Federal e Territórios. **Acórdão n. 1994363, Recurso Inominado n. 0776228-18.2024.8.07.0016**. Relatora: Giselle Rocha Raposo. Segunda Turma Recursal. Julgado em: 04 maio 2025. Publicado no DJe em: 14 maio 2025. Disponível em: <https://jurisdf.tjdft.jus.br/acordaos/a09a09a5-b9a7-465e-844b-34335043e96e>. Acesso em: 27 mai. 2026.

DONDA, Daniel. **Guia Prático de Implementação da LGPD**. São Paulo: Donda Consultoria, 2021.

DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018): A caminho da efetividade: Contribuições para a implementação da LGPD**. São Paulo: Revista dos Tribunais, 2020.

FIDELIS, Francisco Adailton; CLARO, Luis Felipe de Araújo; GONÇALVES, Dimas Melo. LGPD e marketing cultural: o uso de dados pessoais em campanhas comerciais durante o Festival de Parintins. **ARACÊ**, 2025. DOI: 10.56238/arev7n10-230. Disponível em: <https://periodicos.newsciencepubl.com/arace/article/download/9202/11063>. Acesso em: 27 de maio de 2026.

HAUER, Ludmila. **O impacto da LGPD nas relações de consumo**. Conjur, 10 jul. 2020. Disponível em: <https://www.conjur.com.br/2020-jul-10/ludmila-hauer-impacto-lgpd-relacoes-consumo/>. Acesso em: 23 set. 2025.

LEAL, Geraldo. **Aspectos Gerais da LGPD na Prática**. 2. ed. São Paulo: Atlas, 2021.

LILLA, Paulo. **A evolução da LGPD no Brasil: cinco anos da LGPD**. *LinkedIn*, 2023. Disponível em: <https://pt.linkedin.com/pulse/evolu%C3%A7%C3%A3o-da-privacidade-brasil-cinco-anos-lgpd-roberta-nascimento>. Acesso em: 21 set. 2025.

MACHADO, Kalleb Ribeiro; CATA PRETA, Kaio Oliveira; PUNGIRUM, João César Mendel. Segurança da informação para empresas no Brasil. **Revista Multidisciplinar do Nordeste Mineiro**, 2024. DOI: 10.61164/rnm.v10i1.2985. Disponível em: <https://remunom.ojsbr.com/multidisciplinar/article/view/2985/3153>. Acesso em: 27 de maio de 2026.

MEDEIROS, Nîani Guimarães Lima de. A evolução da proteção de dados no Brasil: uma análise histórica e legislativa até o advento da LGPD. **Revista Jurídicas**, v. 11, n. 1, p. 11364,

2024. Disponível em: <https://revistajuridicas.pgsscogna.com.br/juridicas/article/view/11364>. Acesso em: 21 set. 2025.

MENDES, Laura Schertel; BIONDI, Bruno Ricardo (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. XXII, 741 p.

MINISTÉRIO PÚBLICO DO ESTADO DO ESPÍRITO SANTO. **A proteção de dados pessoais nas relações de consumo**. Vitória: MPES, 2025. Disponível em: https://mpes.mp.br/cadc/wp-content/uploads/sites/4/2025/04/Cartilha-UMAES-finalizado-em-01set_230717_141517-1.pdf. Acesso em: 23 set. 2025.

OLIVEIRA, Ana Carolina Rios; FERREIRA, Henrique da Cruz; PIRES, Fernanda Ivo. Princípios da Lei Geral de Proteção de Dados (LGPD). **Seara Jurídica**, v. 1, n. 1, 2021. Disponível em: <https://publicacoes.unijorge.com.br/searajuridica/article/view/431>. Acesso em: 21 set. 2025.

ONU. **Declaração Universal dos Direitos Humanos**. Paris, 1948. Disponível em: <https://www.un.org/pt/universal-declaration-human-rights/>. Acesso em: 19 de maio de 2026.

OTERO, C.; YATEGASHI, João Gabriel. A Lei Geral de Proteção de Dados e a proteção do consumidor na sociedade de informação. **Virtuajus**, 2024. Disponível em: <https://periodicos.pucminas.br/virtuajus/article/download/31973/22773>. Acesso em: 27 de maio de 2026.

SILVA, Anna Luiza; BARBOSA SILVA, Bruna Acosta; LEOCÁDIO, Luiza Cardozo. Responsabilidade civil no vazamento de dados. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, 2025. DOI: 10.51891/rease.v11i11.22167. Disponível em: <https://periodicorease.pro.br/rease/article/download/22167/13586>. Acesso em: 27 de maio de 2026.

VASCONCELOS CAMURÇA, Lia Carolina; MATIAS, João Luís Nogueira. Direito à privacidade e à proteção de dados pessoais: análise das práticas obscuras de direcionamento de publicidade consoante a Lei nº 13.709 de 14 de agosto de 2018. **Revista Direitos Fundamentais & Democracia**, 2021. DOI: 10.25192/ISSN.1982-0496.RDFD.V26I21590. Disponível em: <https://revistaeletronicardfd.unibrazil.com.br/index.php/rdfd/article/download/1590/692>. Acesso em: 27 de maio de 2026.

-
1. Discente do 9º período do Curso de Bacharelado em Direito pelo Centro Universitário UNINORTE.↵
 2. Docente do Centro Universitário Uninorte. Graduada em Direito pela U:VERSE. Especialista em Psicopedagogia pela Universidade Várzea-grandense e Direito Digital e Educação Especial e Inclusiva

pela Faculdade Metropolitana. Graduada em Letras Vernáculas pela Universidade Federal do Acre -

UFAC. Coordenadora do Núcleo de Acessibilidade e Apoio à Inclusão da Uninorte.↵