

ISABELLE LIMA BARROS PINHO
VITÓRIA ALESSANDRA SOARES

**A PROTEÇÃO DE DADOS DO CONSUMIDOR NAS COMPRAS REALIZADAS
POR MEIO DE PLATAFORMAS E DE E-COMMERCE**

Artigo científico apresentado a Afya Centro
Universitário de Ji-Paraná – Afya Ji-
Paraná, para obtenção de grau na
disciplina Trabalho de Conclusão de Curso
em Direito.

Prof. Orientador: Teófilo Lourenço de Lima

Ji-Paraná
2026

Dados Internacionais de Catalogação na Publicação - CIP

P654p

Pinho, Isabelle Lima Barros.

A proteção de dados do consumidor nas compras realizadas por meio de plataformas e de e-commerce. / Isabelle Lima Barros Pinho; Vitória Alessandra Soares. – Ji-Paraná, 2026.
23 p.; il.

Artigo Científico (Curso de Direito) – Afya Centro Universitário de Ji-Paraná, 2026.

Orientador: Prof. Esp. Teófilo Lourenço de Lima.

1. Proteção de dados. 2. Consumidor. 3. Comércio eletrônico. 4. LGPD. I. Soares, Vitória Alessandra. II. Lima, Teófilo Lourenço de. III. Título.

CDU 34:336.2

A PROTEÇÃO DE DADOS DO CONSUMIDOR NAS COMPRAS REALIZADAS POR MEIO DE PLATAFORMAS E DE E-COMMERCE

Isabelle Lima Barros Pinho¹

Vitória Alessandra Soares²

Teófilo Lourenço de Lima³

RESUMO: O avanço das tecnologias digitais e a ampliação do acesso à internet provocaram profundas transformações nas relações de consumo, especialmente com o crescimento do comércio eletrônico. Nesse contexto, a realização de compras por meio de plataformas digitais exige o fornecimento constante de dados pessoais pelos consumidores, o que gera preocupações relacionadas à privacidade, segurança da informação e uso indevido dessas informações. O presente artigo tem como objetivo analisar como ocorre a proteção dos dados pessoais dos consumidores nas compras realizadas por meio de plataformas de e-commerce no Brasil, considerando a legislação vigente e os desafios relacionados à sua aplicação. A pesquisa possui abordagem qualitativa e caracteriza-se como estudo bibliográfico e documental, fundamentado na análise de doutrinas, artigos científicos e legislação pertinente, especialmente a Lei Geral de Proteção de Dados Pessoais (LGPD). Os resultados demonstram que, embora a LGPD represente um importante avanço na regulamentação do tratamento de dados pessoais, ainda existem desafios relacionados à sua efetiva aplicação, à fiscalização por parte dos órgãos competentes e à conscientização dos próprios consumidores acerca de seus direitos. Conclui-se que a proteção adequada dos dados pessoais é essencial para garantir segurança nas relações de consumo digitais e fortalecer a confiança no comércio eletrônico.

Palavras-chave: Proteção de dados. Consumidor. Comércio eletrônico. LGPD.

ABSTRACT: The advancement of digital technologies and the expansion of internet access have brought about profound transformations in consumer relations, especially with the growth of e-commerce. In this context, making purchases through digital platforms requires the constant provision of personal data by consumers, which generates concerns related to privacy, information security, and the misuse of this information. This article aims to analyze how the protection of consumers' personal data occurs in purchases made through e-commerce platforms in Brazil, considering current legislation and the challenges related to its application. The research has a qualitative approach and is characterized as a bibliographic and documentary study, based on the analysis of doctrines, scientific articles, and relevant legislation, especially the General Data Protection Law (LGPD). The results demonstrate that,

¹ Acadêmica do 9º período do curso de Direito pelo Centro Universitário São Lucas Ji-Paraná. E-mail: isabellepinho25@gmail.com

² Acadêmica do 8º período do curso de Direito pelo Centro Universitário São Lucas Ji-Paraná. E-mail: vicanani@gmail.com

³ Pós-graduado em Administração e Planejamento para Docentes pela ULBRA, 1996; pós-graduado em Inovação, Gestão e Práticas Docentes no Ensino Superior pela Faculdade Santo Agostino, 2021. Licenciado em Pedagogia pela Universidade Federal de Rondônia, 1996; Bacharel em Direito pelo Centro Universitário São Lucas Ji-Paraná. Ji-Paraná, Rondônia, Brasil. E-mail: teofilolourencodelima@gmail.com

although the LGPD represents an important advance in the regulation of the processing of personal data, there are still challenges related to its effective application, oversight by competent bodies, and consumer awareness of their rights. It is concluded that adequate protection of personal data is essential to ensure security in digital consumer relations and to strengthen trust in e-commerce.

Keywords: Data protection. Consumer. E-commerce. LGPD (Brazilian General Data Protection Law).

1. INTRODUÇÃO

A expansão da internet no Brasil modificou de maneira profunda as formas de interação social, econômica e jurídica, incorporando novas dinâmicas ao cotidiano dos consumidores. Nesse cenário, o comércio eletrônico tornou-se uma das principais expressões da adaptação das relações de consumo ao ambiente digital, permitindo que bens e serviços sejam adquiridos por meio de plataformas virtuais que dependem intensamente da coleta, armazenamento e tratamento de dados pessoais. A utilização dessas informações, embora necessária para viabilizar as transações, coloca o consumidor em uma posição de vulnerabilidade diante da possibilidade de usos inadequados, falhas de segurança ou práticas que afetem sua privacidade.

Inserido na área do Direito do Consumidor e relacionado diretamente à proteção de dados pessoais, o tema revela-se relevante porque envolve direitos fundamentais e impactos diretos na dinâmica das relações comerciais contemporâneas. A proteção da privacidade e da intimidade encontra fundamento na Constituição Federal de 1988 (BRASIL, 1988), especialmente no artigo 5º, inciso X, que assegura a inviolabilidade da vida privada, da honra e da imagem das pessoas. A crescente utilização de plataformas digitais ampliou a necessidade de compreender como os dados fornecidos pelos consumidores são tratados e quais mecanismos jurídicos existem para assegurar sua tutela.

A pesquisa busca responder de forma discursiva ao problema central: como se configura a proteção dos dados pessoais do consumidor nas compras realizadas em plataformas de comércio eletrônico no Brasil, considerando a evolução tecnológica e o atual cenário jurídico? Para alcançar essa resposta, o estudo tem como objetivo geral analisar essa proteção dentro do contexto brasileiro, e como objetivos

específicos compreender a evolução do ambiente digital, identificar riscos e vulnerabilidades, descrever os mecanismos legais existentes e examinar os desafios envolvidos na sua efetivação.

A pesquisa foi desenvolvida por meio de levantamento bibliográfico e análise documental, tomando como base doutrinas, legislação e publicações que tratam da internet, do comércio eletrônico e da proteção de dados pessoais. Dessa forma, pretende-se construir uma visão clara sobre a importância do tema e sobre o papel do arcabouço jurídico na garantia da segurança e privacidade do consumidor no ambiente digital.

2. MATERIAL E MÉTODOS

O presente estudo caracteriza-se como uma pesquisa de natureza básica, com abordagem qualitativa e caráter bibliográfico e documental. A investigação fundamenta-se na análise de obras doutrinárias, artigos científicos, legislações e documentos institucionais relacionados à proteção de dados pessoais no comércio eletrônico.

O método adotado foi o dedutivo, partindo de conceitos gerais relacionados à internet, ao comércio eletrônico e à proteção de dados pessoais para, posteriormente, analisar sua aplicação específica nas relações de consumo no ambiente digital.

A pesquisa foi desenvolvida por meio de levantamento e análise de materiais publicados em livros, artigos científicos, plataformas acadêmicas e documentos oficiais. Entre os principais referenciais utilizados estão autores que discutem a proteção de dados e a regulação do ambiente digital, bem como a legislação vigente, especialmente a Lei Geral de Proteção de Dados Pessoais (LGPD).

3. O COMÉRCIO ELETRÔNICO E A COLETA DE DADOS DO CONSUMIDOR

O desenvolvimento das tecnologias digitais e a ampliação do acesso à internet possibilitaram o crescimento significativo do comércio eletrônico nas últimas décadas.

Essa modalidade de consumo caracteriza-se pela realização de transações comerciais por meio de plataformas digitais, permitindo que consumidores adquiram produtos e serviços sem a necessidade de deslocamento físico. Nesse cenário, o ambiente virtual passou a desempenhar papel relevante na dinâmica econômica contemporânea, ampliando as possibilidades de acesso ao mercado e transformando as relações tradicionais de consumo.

Entretanto, o funcionamento dessas plataformas depende diretamente da coleta e do processamento de dados pessoais dos consumidores, que se tornam elementos essenciais para a realização das transações. Informações como nome, endereço, número de telefone, e-mail e dados bancários são frequentemente solicitadas para viabilizar etapas como cadastro, pagamento e entrega dos produtos. De acordo com Bioni (2019), os dados pessoais passaram a representar um importante recurso na economia digital, sendo utilizados não apenas para permitir a execução das atividades comerciais, mas também para a criação de estratégias de mercado baseadas no comportamento dos usuários.

Desde a sociedade industrial, já se reconhecia a informação como um fator determinante para a geração de riquezas. Contudo, é apenas com a mencionada evolução de ordem quantitativa e qualitativa no processamento das informações que é selado o processo de transição da sociedade pré-informacional para a sociedade informacional. Os dados passam, então, a ocupar posição central nas relações econômicas e sociais. (Bioni, 2019, p. 28)

Além disso, a utilização de ferramentas tecnológicas que permitem o monitoramento de hábitos de navegação e consumo possibilita às empresas desenvolver perfis comportamentais detalhados dos usuários, prática conhecida como perfilização. Tal procedimento, embora contribua para a personalização de ofertas e para o aprimoramento das estratégias comerciais, também levanta questionamentos relacionados à transparência e aos limites do tratamento de dados pessoais no ambiente digital.

Dessa forma, o crescimento do comércio eletrônico evidencia a necessidade de conciliar o desenvolvimento tecnológico com a proteção dos direitos fundamentais

dos consumidores, especialmente no que se refere à privacidade e à proteção de seus dados pessoais.

3.1 Evolução histórica do comércio eletrônico

O comércio eletrônico, embora seja frequentemente associado ao avanço da internet, possui suas origens em práticas comerciais mais antigas, relacionadas à realização de transações à distância. Desde os primeiros modelos de comércio por correspondência, já se observava a necessidade de estabelecer meios de comunicação entre fornecedores e consumidores sem a presença física das partes.

Com o avanço das tecnologias de comunicação, essas práticas evoluíram, permitindo maior agilidade nas transações e ampliando o alcance das atividades comerciais. Assim, o comércio eletrônico pode ser compreendido como resultado de um processo histórico de transformação das relações de consumo, impulsionado pela inovação tecnológica e pela crescente digitalização da sociedade.

Os primeiros registros de comércio à distância estão relacionados ao uso do correio postal como meio de intermediação entre comerciantes e consumidores. Um exemplo relevante nesse contexto é o sistema conhecido como HERMES, que possibilitava a venda de produtos por meio de catálogos enviados aos consumidores.

Figura 1 – comércio por correspondência (Capa do Catálogo Hermes de 1966)



Fonte: ANOS DOURADOS. *Imagens – Velharia: Catálogo Hermes*. Disponível em: <https://www.anosdourados.blog.br/2010/06/imagens-velharia-catalogo-hermes.html>.

Acesso em: 6 março. 2026.

Nesse modelo, os clientes realizavam seus pedidos por correspondência, e os produtos eram posteriormente enviados pelo correio. Esse sistema representou um marco importante na evolução das relações de consumo, pois demonstrou a viabilidade de transações comerciais sem a necessidade de contato presencial.

Ainda que inicial, esse modelo já evidenciava a necessidade de coleta de dados dos consumidores, demonstrando a antiga relação entre consumo e tratamento de informações pessoais (Doneda, 2006).

Com o surgimento da internet nas últimas décadas do século XX, o comércio eletrônico passou por uma transformação significativa. A digitalização das relações comerciais possibilitou a criação de plataformas online, nas quais consumidores podem acessar produtos e serviços de forma rápida e prática.

A partir desse momento, a coleta e o tratamento de dados pessoais tornaram-se ainda mais intensos, uma vez que as plataformas digitais passaram a registrar não apenas informações básicas, mas também hábitos de navegação e preferências de

consumo dos usuários. O crescimento das atividades comerciais no ambiente digital ampliou significativamente a circulação de informações pessoais, tornando necessária a adoção de mecanismos jurídicos voltados à proteção da privacidade e à garantia da segurança dos dados dos consumidores.

3.2 Plataformas digitais e intermediação de consumo

No contexto do comércio eletrônico contemporâneo, destaca-se o papel das plataformas digitais como intermediadoras das relações de consumo, especialmente por meio dos chamados marketplaces. Essas plataformas funcionam como ambientes virtuais que conectam vendedores e consumidores, permitindo a realização de transações comerciais de forma rápida e acessível, sem que haja, necessariamente, contato direto entre as partes envolvidas.

As plataformas digitais que operam sob o modelo de marketplace atuam como facilitadoras das relações de consumo, oferecendo infraestrutura tecnológica, sistemas de pagamento, logística e mecanismos de avaliação de fornecedores. Nesse modelo, a plataforma não atua, em regra, como fornecedora direta do produto ou serviço, mas como intermediadora da relação, circunstância que suscita importantes debates jurídicos acerca de sua responsabilidade perante os consumidores.

Nos termos do Código de Defesa do Consumidor (BRASIL, 1990), os participantes da cadeia de fornecimento podem ser responsabilizados pelos danos causados ao consumidor, especialmente quando sua atuação contribui para a concretização da relação de consumo.

Segundo Cláudia Lima Marques (2021), a vulnerabilidade do consumidor constitui elemento central das relações de consumo, devendo orientar a interpretação e aplicação das normas previstas no Código de Defesa do Consumidor, inclusive nas contratações realizadas por meios digitais.

Nesse sentido, a doutrina e a jurisprudência vêm reconhecendo que as plataformas digitais podem ser responsabilizadas por eventuais danos causados aos

consumidores, especialmente quando há falhas na prestação do serviço, como ausência de controle sobre vendedores, publicidade enganosa ou deficiência nos mecanismos de segurança. Tal entendimento fundamenta-se na ideia de que, ao intermediar a relação de consumo e obter vantagens econômicas com essa atividade, as plataformas assumem deveres de cuidado e segurança em relação aos usuários.

Além disso, no contexto da proteção de dados pessoais, as plataformas digitais desempenham papel ainda mais relevante, uma vez que são responsáveis pela coleta, armazenamento e tratamento de uma grande quantidade de informações dos consumidores. Nesse cenário, tais empresas passam a atuar como agentes de tratamento de dados, estando sujeitas às disposições da Lei Geral de Proteção de Dados Pessoais (LGPD), devendo garantir a segurança das informações e o respeito aos direitos dos titulares.

Dessa forma, as plataformas digitais assumem um papel central nas relações de consumo contemporâneas, não apenas como intermediadoras, mas como agentes relevantes na estrutura do comércio eletrônico. Tal posição exige a adoção de práticas responsáveis e o cumprimento de deveres legais, tanto no âmbito do Direito do Consumidor quanto da proteção de dados pessoais, a fim de garantir maior segurança, equilíbrio e confiança nas relações estabelecidas no ambiente digital.

4. RISCOS E VULNERABILIDADES NO TRATAMENTO DE DADOS

Apesar das facilidades proporcionadas pelo comércio eletrônico, o ambiente digital instaura um cenário de riscos multifacetados que desafiam a segurança jurídica e a privacidade. Entre os problemas estruturais, destacam-se o vazamento de informações sensíveis, o desvio de finalidade no uso dos dados e a persistente opacidade quanto aos processos de coleta e armazenamento. Nesse contexto, a crescente dependência de sistemas tecnológicos para a realização de transações cotidianas não apenas facilita o consumo, mas amplia exponencialmente a exposição dos indivíduos a falhas sistêmicas e práticas abusivas que operam nos bastidores das plataformas digitais.

A vulnerabilidade do consumidor no ambiente digital é um conceito que transborda a hipossuficiência econômica tradicional, sendo agravada por uma severa assimetria informacional. Segundo Laura Schertel Mendes (2014), a proteção de dados pessoais constitui importante instrumento de tutela da personalidade e da privacidade do indivíduo, especialmente diante da crescente circulação e tratamento de informações no ambiente digital. No e-commerce, o consumidor raramente possui o conhecimento técnico necessário para compreender o fluxo real de seus dados após o clique inicial. As plataformas utilizam políticas de privacidade que, embora juridicamente válidas, são frequentemente extensas e redigidas em linguagem hermética, criando o que a doutrina chama de "fadiga do consentimento".

Diante da complexidade que envolve o fluxo informacional e a própria representação da identidade do usuário no e-commerce, Danilo Doneda adverte sobre o risco de uma proteção jurídica defasada:

A leitura das garantias constitucionais para os dados somente sob o prisma de sua comunicação e de sua eventual interceptação lastreia-se em uma interpretação que não chega a abranger a complexidade do fenômeno da informação ao qual fizemos referência. Há um hiato que segrega a tutela da privacidade, esta constitucionalmente protegida, da tutela das informações pessoais em si – que, para a corrente mencionada, gozariam de uma proteção mais tênue. E esse hiato possibilita a perigosa interpretação que pode eximir o aplicador de levar em conta os casos nos quais uma pessoa é ofendida em sua privacidade – ou tem outros direitos fundamentais desrespeitados – não de forma direta, porém por meio da utilização abusiva de suas informações pessoais em bancos de dados. Não é necessário ressaltar, novamente, o quanto hoje em dia as pessoas são reconhecidas em diversos relacionamentos somente de forma indireta, pela representação de sua personalidade que é fornecida pelos seus dados pessoais, ressaltando, ainda mais, a importância da proteção de tais dados para a proteção da identidade e personalidade de cada um de nós. (Doneda, 2011, p. 106-122)

Além da questão do consentimento, o avanço de tecnologias disruptivas como o Big Data e a inteligência artificial permite que as empresas transcendam a simples coleta de dados cadastrais. Através da perfilização (profiling), as organizações processam grandes volumes de metadados para decodificar hábitos de navegação, padrões de clique e até o tempo de exposição a determinados conteúdos.

A perfilização de consumidores levanta importantes discussões éticas e jurídicas relacionadas à autonomia privada e à liberdade de escolha. A utilização de algoritmos capazes de prever comportamentos de consumo pode gerar assimetrias

ainda mais profundas entre fornecedores e consumidores, sobretudo quando tais informações são utilizadas para direcionamento de publicidade personalizada ou diferenciação de ofertas comerciais.

Embora tais práticas visem, em teoria, o aprimoramento da experiência do usuário, elas levantam sérias preocupações quanto à autonomia e à liberdade de escolha. A análise massiva de dados permite a criação de "arquiteturas de escolha" ou dark patterns — interfaces desenhadas propositalmente para induzir o consumidor a decisões que ele talvez não tomasse em condições de total transparência. Esse monitoramento constante pode mitigar a liberdade do indivíduo, que passa a ser cercado por uma "bolha de consumo" baseada em suas vulnerabilidades previamente mapeadas. Isso reforça a necessidade premente de mecanismos legais que estabeleçam limites éticos claros, impedindo que o poder informacional das empresas se converta em uma ferramenta de manipulação comportamental.

Por fim, os riscos inerentes ao tratamento de dados evidenciam que a segurança da informação não é apenas um requisito técnico, mas um dever jurídico e ético. A fragilidade dos sistemas de segurança pode resultar em danos extrapatrimoniais severos, como o roubo de identidade e a exposição da vida privada. Portanto, a análise das vulnerabilidades presentes no ambiente digital demonstra que o desenvolvimento sustentável do comércio eletrônico é indissociável da proteção dos direitos fundamentais.

É imperativo que as normas jurídicas não apenas acompanhem a evolução tecnológica, mas antecipem cenários de risco, garantindo que a inovação não ocorra à custa da dignidade do consumidor.

4.1 Vazamento de dados e incidentes de segurança

O vazamento de dados pessoais configura um dos principais riscos no âmbito do comércio eletrônico, representando ameaça concreta à privacidade e à segurança dos consumidores. Tais incidentes podem ocorrer em razão de falhas nos sistemas de segurança das empresas, ataques cibernéticos praticados por hackers ou até mesmo por condutas internas inadequadas no tratamento das informações.

No contexto digital, a grande quantidade de dados armazenados por plataformas de e-commerce torna-se um alvo atrativo para práticas ilícitas, como invasões de sistemas e roubo de informações sensíveis. Dados como números de documentos, endereços, informações bancárias e históricos de compras podem ser expostos, gerando consequências graves para os consumidores, como fraudes, golpes financeiros e utilização indevida de sua identidade.

Conforme Patrícia Peck Pinheiro (2021), a proteção de dados pessoais exige a adoção de medidas de segurança, boas práticas e mecanismos de governança capazes de reduzir riscos e assegurar a conformidade com as disposições da Lei Geral de Proteção de Dados.

De acordo com Doneda (2006), a segurança da informação deve ser compreendida como elemento essencial da atividade econômica digital, não se tratando apenas de um requisito técnico, mas de um dever jurídico das empresas que realizam o tratamento de dados pessoais. Nesse sentido, a Lei Geral de Proteção de Dados estabelece a obrigação de adoção de medidas técnicas e administrativas aptas a proteger as informações contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração ou divulgação (Brasil, 2018).

A circulação de informações pessoais passou a integrar o próprio funcionamento da sociedade contemporânea, tornando indispensável a adoção de mecanismos de segurança aptos a impedir acessos indevidos, desvios de finalidade e violações à privacidade. A proteção dessas informações deixa de ser apenas questão técnica para assumir natureza jurídica relevante. (Doneda, 2006, p. 17).

Além dos prejuízos materiais, o vazamento de dados pode ocasionar danos de natureza moral, uma vez que a exposição indevida de informações pessoais atinge diretamente a esfera privada do indivíduo. Assim, a ocorrência de incidentes de segurança evidencia a necessidade de fortalecimento de mecanismos de proteção e de responsabilização das empresas que atuam no ambiente digital.

A ocorrência de vazamento de dados pessoais no comércio eletrônico levanta importantes discussões acerca da responsabilidade civil das empresas envolvidas no

tratamento dessas informações. No ordenamento jurídico brasileiro, a responsabilidade pelos danos causados ao consumidor encontra fundamento tanto no Código de Defesa do Consumidor quanto na Lei Geral de Proteção de Dados.

O Código de Defesa do Consumidor adota, como regra, a responsabilidade objetiva dos fornecedores, baseada na teoria do risco da atividade. Isso significa que as empresas respondem pelos danos causados aos consumidores independentemente da comprovação de culpa, bastando a demonstração do dano e do nexo de causalidade entre a conduta e o prejuízo sofrido.

No contexto da proteção de dados pessoais, essa lógica é reforçada pela LGPD, que também prevê a responsabilização dos agentes de tratamento que, em razão de falhas na segurança ou no cumprimento das normas legais, causem danos aos titulares dos dados. Dessa forma, empresas que não adotam medidas adequadas de proteção ou que permitem o acesso indevido às informações podem ser responsabilizadas judicialmente.

Entre os danos decorrentes do vazamento de dados, destaca-se o dano moral, que decorre da violação à privacidade e à intimidade do indivíduo. A jurisprudência brasileira tem reconhecido que a exposição indevida de dados pessoais pode gerar abalo à esfera psíquica do consumidor, sendo cabível a indenização nesses casos.

Além disso, a responsabilidade civil no ambiente digital deve ser analisada à luz da complexidade das relações de consumo, especialmente quando envolve múltiplos agentes, como plataformas digitais, fornecedores e intermediadores. Nesses casos, pode haver responsabilidade solidária entre os envolvidos, garantindo maior proteção ao consumidor, que não precisa identificar individualmente o responsável pelo dano.

A responsabilidade civil das plataformas digitais tem sido objeto de crescente debate doutrinário e jurisprudencial. Embora muitas empresas sustentem atuar apenas como intermediadoras das transações realizadas em marketplaces, parte da doutrina entende que sua participação na cadeia de fornecimento justifica a incidência

das normas protetivas do Código de Defesa do Consumidor. Nesse contexto, a vulnerabilidade do consumidor constitui princípio fundamental das relações de consumo, exigindo interpretação das normas consumeristas voltada à sua efetiva proteção (MARQUES, 2021).

Dessa forma, a responsabilização das empresas constitui instrumento fundamental para assegurar a efetividade da proteção de dados pessoais, incentivando a adoção de práticas mais seguras e responsáveis no tratamento das informações dos consumidores.

4.2 Educação digital do consumidor

A proteção efetiva dos dados pessoais no comércio eletrônico não depende apenas da atuação das empresas e da existência de normas jurídicas, sendo também essencial a participação ativa dos próprios consumidores. Nesse contexto, a educação digital surge como elemento fundamental para a construção de um ambiente virtual mais seguro e equilibrado.

Grande parte dos usuários da internet ainda possui conhecimento limitado sobre o funcionamento das plataformas digitais e sobre os riscos envolvidos no compartilhamento de informações pessoais. É comum que consumidores aceitem termos de uso e políticas de privacidade de forma automática, sem realizar a leitura ou a devida compreensão do conteúdo apresentado.

Essa prática contribui para o agravamento da vulnerabilidade informacional, uma vez que o consumidor passa a fornecer dados pessoais sem ter plena ciência das finalidades de seu uso. Conforme aponta Doneda (2006), a assimetria informacional entre empresas e consumidores constitui um dos principais desafios nas relações de consumo digitais, exigindo medidas que promovam maior transparência e compreensão.

O cidadão perde progressivamente o controle sobre as próprias informações, especialmente diante da crescente automatização do tratamento de dados e da concentração informacional nas mãos de grandes organizações. Tal

cenário amplia a vulnerabilidade do indivíduo perante estruturas econômicas baseadas na circulação massiva de dados. (Doneda, 2006, p. 42).

Nesse contexto, a conscientização dos consumidores acerca de seus direitos e deveres no ambiente digital torna-se indispensável. A educação digital deve envolver a orientação quanto à importância da proteção de dados pessoais, ao uso consciente da internet e à adoção de práticas seguras, como a verificação de sites confiáveis, o cuidado com compartilhamento de informações e a utilização de senhas seguras.

Além disso, o fortalecimento da cultura de proteção de dados no Brasil depende da atuação conjunta de instituições públicas, empresas e da sociedade civil, promovendo campanhas educativas e incentivando o desenvolvimento de uma postura mais crítica e informada por parte dos usuários.

Nesse contexto, a vulnerabilidade do consumidor no ambiente digital pode ser compreendida como uma forma de hipervulnerabilidade, tendo em vista que, além das limitações econômicas e técnicas já reconhecidas nas relações de consumo, há também a dificuldade de compreensão dos mecanismos tecnológicos envolvidos no tratamento de dados. Tal cenário amplia o desequilíbrio entre as partes, exigindo uma atuação mais incisiva do Direito na proteção dos consumidores. Conforme destaca Bioni (2019), o ambiente digital potencializa o poder informacional das empresas, tornando ainda mais necessária a criação de mecanismos que garantam a efetiva autonomia dos titulares de dados.

Dessa forma, a educação digital deve ser compreendida como um pilar essencial da proteção de dados pessoais, atuando de forma complementar às normas jurídicas. A construção de um ambiente digital seguro depende não apenas da regulação estatal, mas também da formação de consumidores conscientes, capazes de exercer seus direitos e adotar comportamentos preventivos. Somente com essa combinação será possível reduzir as vulnerabilidades existentes e promover relações de consumo mais equilibradas no comércio eletrônico.

5. A LEI GERAL DE PROTEÇÃO DE DADOS E A TUTELA DO CONSUMIDOR

Diante dos desafios relacionados à proteção de dados no ambiente digital e do crescimento do uso de informações pessoais nas relações econômicas, foi criada no Brasil a Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018. A legislação representa um marco regulatório importante no ordenamento jurídico brasileiro (Bioni, 2019), pois estabelece regras específicas para o tratamento de dados pessoais por pessoas físicas e jurídicas, tanto no setor público quanto no privado.

Segundo Monteiro (2018), a LGPD representa um avanço significativo ao estabelecer diretrizes específicas para o tratamento de dados pessoais no Brasil, tendo como objetivo principal garantir maior proteção aos direitos fundamentais de liberdade, privacidade e ao livre desenvolvimento da personalidade da pessoa natural, estabelecendo limites e responsabilidades para as organizações que realizam o tratamento de dados. Conforme destaca Bioni (2019), a lei surge como resposta à crescente utilização de dados pessoais como elemento central da economia digital, buscando equilibrar a inovação tecnológica com a proteção dos direitos individuais.

Nesse sentido, a legislação estabelece princípios e diretrizes que devem orientar o tratamento de dados pessoais pelas empresas. Entre os princípios previstos pela lei destacam-se a finalidade, que determina que os dados devem ser coletados para propósitos legítimos e específicos; a adequação, que exige compatibilidade entre o tratamento realizado e a finalidade informada ao titular; a necessidade, que limita a coleta ao mínimo de dados indispensáveis; “[...] e a segurança, que impõe a adoção de medidas técnicas e administrativas capazes de proteger as informações contra acessos não autorizados ou situações de vazamento”. (Brasil, 2018)

Um ponto de extrema relevância prática no comércio eletrônico são as bases legais para o tratamento de dados (Art. 7º). Diferente do que muitos consumidores acreditam, o consentimento não é a única forma de coletar dados. No e-commerce, o tratamento é frequentemente legitimado pela execução de contrato (para entrega do produto), pelo cumprimento de obrigação legal (emissão de nota fiscal) e, o mais polêmico, pelo legítimo interesse do controlador. Este último permite que empresas realizem marketing direto, desde que respeitem as legítimas expectativas do

consumidor e não firmam seus direitos fundamentais, exigindo um teste de proporcionalidade rigoroso por meio dos chamados LIAs – Legitimate Interest Assessments (Bioni, 2019).

Além disso, a LGPD prevê uma série de direitos aos titulares dos dados, permitindo que os indivíduos exerçam maior controle sobre suas próprias informações. Entre esses direitos estão o acesso aos dados coletados, a correção de informações incompletas ou desatualizadas, a portabilidade dos dados, bem como a possibilidade de solicitar a anonimização ou exclusão das informações pessoais quando estas deixarem de ser necessárias para a finalidade para a qual foram coletadas.

Entretanto, embora a legislação represente um avanço significativo na proteção da privacidade no Brasil, sua efetividade depende da correta implementação de suas normas pelas empresas e da atuação eficiente dos órgãos responsáveis pela fiscalização, especialmente a Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL, 2019). Dessa forma, a consolidação de uma cultura de proteção de dados no país exige não apenas a existência de normas jurídicas, mas também a conscientização dos consumidores e a adoção de práticas responsáveis por parte das organizações que realizam o tratamento de informações pessoais.

Nesse sentido, a atuação da Autoridade Nacional de Proteção de Dados revela-se essencial para a concretização da LGPD, não apenas no exercício de sua função fiscalizatória, mas também na edição de normas complementares e orientações técnicas que auxiliem na interpretação e aplicação da lei no contexto das constantes inovações tecnológicas.

Apesar de representar um avanço significativo na proteção dos dados pessoais no Brasil, a efetividade da Lei Geral de Proteção de Dados ainda enfrenta diversos desafios em sua aplicação prática. A existência de uma legislação estruturada, por si só, não é suficiente para garantir a plena proteção dos direitos dos titulares, sendo necessária a atuação conjunta de órgãos fiscalizadores, empresas e da própria sociedade.

Um dos principais obstáculos refere-se à dificuldade de fiscalização do cumprimento da lei. A Autoridade Nacional de Proteção de Dados (ANPD), responsável por regulamentar e supervisionar a aplicação da LGPD, ainda enfrenta limitações estruturais e operacionais, o que pode comprometer a efetividade de suas ações. A grande quantidade de empresas que realizam tratamento de dados no país, aliada à complexidade das atividades digitais, torna o processo de fiscalização desafiador, exigindo constante aprimoramento institucional.

Outro ponto relevante diz respeito à resistência ou dificuldade de adaptação por parte das empresas. Muitas organizações, especialmente de pequeno e médio porte, ainda não implementaram integralmente as medidas exigidas pela LGPD, seja por falta de conhecimento técnico, seja pelos custos envolvidos na adequação. Isso resulta em práticas inadequadas de tratamento de dados, aumentando os riscos de violação à privacidade dos consumidores.

Além disso, observa-se um significativo nível de desconhecimento por parte da população acerca dos direitos garantidos pela LGPD. Muitos consumidores não têm ciência de que podem solicitar acesso, correção ou exclusão de seus dados pessoais, o que dificulta o exercício efetivo desses direitos. “A proteção de dados pessoais está diretamente relacionada à autonomia informacional do indivíduo, garantindo-lhe maior controle sobre a circulação e utilização de suas informações pessoais.” (Doneda, 2006, p. 38)

Outro desafio importante está relacionado à rápida evolução tecnológica, que frequentemente supera a capacidade de atualização das normas jurídicas. Novas tecnologias, como inteligência artificial e análise massiva de dados, ampliam as possibilidades de tratamento de informações pessoais, criando situações que nem sempre estão claramente previstas na legislação. Isso exige uma interpretação dinâmica da LGPD e uma atuação proativa dos órgãos reguladores.

Dessa forma, verifica-se que a consolidação da proteção de dados no Brasil não se limita à existência de um marco legal, mas depende de uma transformação

estrutural que envolva a atuação eficiente do Estado, a responsabilidade das empresas e o fortalecimento da consciência dos consumidores. Somente a partir dessa integração será possível assegurar a efetividade da LGPD e garantir a proteção dos direitos fundamentais no ambiente digital contemporâneo.

Dentre os mecanismos institucionais criados para assegurar a efetividade da Lei Geral de Proteção de Dados, destaca-se a atuação da Autoridade Nacional de Proteção de Dados (ANPD), responsável pela regulamentação, fiscalização e promoção da cultura de proteção de dados no país.

5.1 O papel da Autoridade Nacional de Proteção de Dados na fiscalização das plataformas digitais

A efetividade da Lei Geral de Proteção de Dados Pessoais não depende exclusivamente da existência de normas jurídicas que regulamentem o tratamento de dados, mas também da atuação de órgãos responsáveis por sua fiscalização e aplicação. Nesse contexto, destaca-se a Autoridade Nacional de Proteção de Dados (ANPD), criada pela Lei nº 13.853/2019, com a finalidade de zelar pela proteção dos dados pessoais, fiscalizar o cumprimento da LGPD e promover a difusão da cultura de proteção de dados no Brasil.

A ANPD desempenha papel fundamental na consolidação do sistema brasileiro de proteção de dados, atuando na elaboração de regulamentos, orientações técnicas e diretrizes voltadas à interpretação e aplicação da legislação. Além da função normativa, a autoridade possui competência para fiscalizar agentes de tratamento de dados, instaurar processos administrativos e aplicar sanções em casos de descumprimento das disposições previstas na LGPD.

No âmbito das plataformas digitais e do comércio eletrônico, a atuação da ANPD revela-se especialmente relevante, considerando o elevado volume de dados pessoais coletados, armazenados e processados por essas empresas. As plataformas de e-commerce utilizam informações relacionadas à identificação dos consumidores, hábitos de navegação, preferências de consumo e histórico de compras, o que exige

a adoção de medidas rigorosas de segurança e transparência no tratamento dessas informações.

A fiscalização exercida pela ANPD busca assegurar que as empresas observem os princípios estabelecidos pela LGPD, especialmente aqueles relacionados à finalidade, adequação, necessidade, transparência e segurança. Além disso, a autoridade também atua na orientação dos agentes de tratamento quanto à adoção de boas práticas de governança e à implementação de mecanismos capazes de reduzir riscos de vazamentos e acessos indevidos aos dados pessoais.

Outro aspecto relevante refere-se à função educativa desempenhada pela ANPD. Por meio da publicação de guias, recomendações e materiais informativos, a autoridade contribui para o fortalecimento da conscientização social acerca da proteção de dados pessoais, auxiliando consumidores e organizações na compreensão de seus direitos e deveres. Tal atuação é essencial diante da crescente complexidade das relações digitais e da rápida evolução das tecnologias utilizadas pelas plataformas eletrônicas.

Dessa forma, verifica-se que a Autoridade Nacional de Proteção de Dados constitui elemento indispensável para a efetivação da proteção dos dados pessoais no Brasil. Sua atuação regulatória, fiscalizatória e educativa contribui para a construção de um ambiente digital mais seguro, transparente e equilibrado, fortalecendo a confiança dos consumidores nas relações estabelecidas por meio das plataformas de comércio eletrônico.

Nesse contexto, o tratamento de dados pelo poder público e pelas autoridades reguladoras exige a observância de um regime jurídico estrito que equilibre as prerrogativas estatais e os direitos dos cidadãos (WIMMER, 2021).

6. CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo do presente estudo permitiu compreender que o avanço das tecnologias digitais e a expansão do comércio eletrônico transformaram

significativamente as relações de consumo, tornando o tratamento de dados pessoais elemento essencial para o funcionamento das plataformas digitais. Nesse cenário, os consumidores passam a compartilhar uma grande quantidade de informações pessoais, o que aumenta sua exposição a riscos relacionados à privacidade e à segurança dos dados.

Verificou-se que a Lei Geral de Proteção de Dados representa um marco importante no ordenamento jurídico brasileiro, ao estabelecer princípios, direitos e responsabilidades voltados à proteção das informações pessoais. A legislação contribui para a construção de um ambiente digital mais seguro, reforçando a necessidade de transparência e responsabilidade no tratamento de dados por parte das empresas.

Entretanto, também se observou que a efetividade da LGPD depende não apenas da existência da norma, mas da sua aplicação prática. Nesse sentido, a atuação da Autoridade Nacional de Proteção de Dados, o cumprimento das obrigações legais pelas organizações e a conscientização dos consumidores sobre seus direitos são fatores essenciais para a consolidação de uma cultura de proteção de dados no Brasil.

Assim, conclui-se que a proteção adequada dos dados pessoais constitui elemento indispensável para o fortalecimento das relações de consumo no ambiente digital, contribuindo para garantir maior segurança jurídica, transparência e confiança nas transações realizadas por meio do comércio eletrônico.

7. REFERÊNCIAS

ANOS DOURADOS. **Imagens – Velharia: Catálogo Hermes**. 2010. Disponível em: <https://www.anosdourados.blog.br/2010/06/imagens-velharia-catalogo-hermes.html>. Acesso em: 16 jun. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Brasília: ANPD, 2021. Disponível em: <https://www.gov.br/anpd>. Acesso em: 11 mar. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Regulamento de Dosimetria e Aplicação de Sanções Administrativas**. Brasília: ANPD, 2023. Disponível em: <https://www.gov.br/anpd>. Acesso em: 11 mar. 2026.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. São Paulo: Forense, 2019. Acesso em: 07 jun. 2026.

BRASIL. Agência Senado. **Lei que cria Autoridade Nacional de Proteção de Dados é sancionada com vetos**. Senado Notícias, Brasília, DF, 9 jul. 2019. Disponível em: <https://www12.senado.leg.br/noticias/materias/2019/07/09/lei-que-cria-autoridadenacional-de-protecao-de-dados-e-sancionada-com-vetos>. Acesso em: 09 set. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União: seção 1, Brasília, DF, p. 59, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 09 set. 2025.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: <https://www.planalto.gov.br>. Acesso em: 11 mar. 2026.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Diário Oficial da União: Brasília, DF, 12 set. 1990. Disponível em: <https://www.planalto.gov.br>. Acesso em: 11 mar. 2026.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law, Joaçaba, v. 12, n. 1, p. 106-122, jan./jun. 2011. Disponível em: <https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315/658>. Acesso em: 07 jun. 2026.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. Acesso em: 07 jun. 2026.

MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais**. 9. ed. São Paulo: Revista dos Tribunais, 2021. Acesso em: 07 jun. 2026.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. Acesso em: 07 jun. 2026.

MONTEIRO, Renato Leite. **Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada**. Jota, [S.l.], 14 jul. 2018. Opinião e Análise. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analisedetalhada-14072018>. Acesso em: 09 set. 2025.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: Comentários à Lei nº 13.709/2018 (LGPD)**. São Paulo: Saraiva, 2021. Acesso em: 07 jun. 2026.

WIMMER, Miriam. **O regime jurídico do tratamento de dados pessoais pelo poder público**. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno (org.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 271-288. Acesso em: 07 jun. 2026.