Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v12i5.26786

A LGPD E O COMÉRCIO ELETRÔNICO: COMO A LEI INFLUENCIA AS PRÁTICAS DE E-COMMERCE E A PROTEÇÃO DOS DADOS DOS CONSUMIDORES

Tainá Alana Castro Santos[1]
Ihgor Jean Rego[2]

RESUMO: O comércio eletrônico consolidou-se como um setor estratégico da economia, intensificado pela digitalização e pelo aumento do consumo online, especialmente durante a pandemia da Covid-19. Apesar de oferecer conveniência e diversidade de opções, o e-commerce apresenta desafios relacionados à proteção de dados pessoais e à privacidade dos consumidores, que frequentemente se encontram em situação de hipervulnerabilidade. Nesse contexto, a informação torna-se um ativo econômico valioso, utilizado pelas empresas para marketing, análise de perfil e personalização de ofertas, acentuando a assimetria entre fornecedores e consumidores.A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) representa um marco jurídico no Brasil, estabelecendo parâmetros claros para o tratamento de dados e inspirando-se em legislações internacionais, como o GDPR europeu. A LGPD impõe requisitos como consentimento expresso, transparência, segurança da informação e comunicação de incidentes, além de conferir à Autoridade Nacional de Proteção de Dados (ANPD) papel fiscalizador e orientador.No comércio eletrônico, a lei provoca mudanças significativas nas práticas empresariais, promovendo maior transparência, responsabilidade e fortalecimento da confiança do consumidor. Entretanto, desafios persistem, como a adequação de micro e pequenas empresas, a conscientização limitada dos consumidores e a capacidade restrita de fiscalização da ANPD. A pesquisa qualitativa, baseada em revisão bibliográfica, documental e jurisprudencial, evidencia que a LGPD fortalece a proteção jurídica dos consumidores e contribui para equilibrar inovação tecnológica e direitos fundamentais. Para sua plena efetividade, são necessárias ações complementares de educação digital, fortalecimento institucional e integração regulatória internacional, promovendo um ambiente digital seguro, transparente e democrático.

Palavras-chave: Comércio eletrônico. Proteção de dados pessoais. LGPD. Consumidor hipervulnerável. Privacidade digital. Direitos fundamentais. Transparência.

[1]Discente do curso de Direito, Centro Universitário São Lucas – Afya.
[2]Orientador do curso de Direito, Centro Universitário São Lucas – Afya.

ABSTRACT: E-commerce has established itself as a strategic sector of the economy, intensified by digitalization and the rise of online consumption, especially during the COVID -19 pandemic. Despite offering convenience and a variety of options, e-commerce presents challenges related to the protection of personal data and the privacy of consumers, who are often in a situation of hypervulnerability. In this context, information becomes a valuable economic asset, used by companies for marketing, profile analysis, and personalization of offers, accentuating the asymmetry between suppliers and consumers.The General Personal Data Protection Law (LGPD – Law No. 13,709/2018) represents a legal milestone in Brazil, establishing clear parameters for data processing and drawing inspiration from international legislation, such as the European GDPR. The LGPD imposes requirements such as express consent, transparency, information security, and incident reporting, in addition to granting the National Data Protection Authority (ANPD) an oversight and guidance role. In e-commerce, the law brings about significant changes in business practices, promoting greater transparency, accountability, and strengthening consumer trust. However, challenges persist, such as the compliance of micro and small businesses, limited consumer awareness, and the ANPD's limited oversight capacity. Qualitative research, based on a review of literature, documents, and case law, shows that the LGPD strengthens consumer legal protection and helps balance technological innovation and fundamental rights. For its full effectiveness, complementary digital education, institutional strengthening, and international regulatory integration are necessary, promoting a safe, transparent, and democratic digital environment.

Keywords: E-commerce. Personal data protection. LGPD. Hypervulnerable consumers. Digital privacy. Fundamental rights. Transparency.

1. INTRODUÇÃO

O comércio eletrônico consolidou-se como um dos setores mais dinâmicos e estratégicos da economia global. No Brasil, o crescimento exponencial do e-commerce foi intensificado pela massificação da internet e pela transformação digital das relações de consumo, processo que se acelerou ainda mais com a pandemia da Covid-19. Nesse novo cenário, consumidores passaram a recorrer com maior frequência às plataformas virtuais para aquisição de bens e serviços, estabelecendo uma dependência cada vez mais significativa de ambientes digitais.

Se, por um lado, esse modelo oferece conveniência, diversidade de opções e eficiência nas transações, por outro, traz consigo desafios relacionados à segurança informacional, à proteção da privacidade e ao tratamento de dados pessoais. A informação, no contexto digital, transformou-se em um ativo econômico de alto valor, utilizado pelas empresas para a formulação de estratégias de marketing, análise de perfil de consumo e personalização de ofertas. Assim, o consumidor passou a ser visto não apenas como

destinatário final de produtos e serviços, mas também como fornecedor involuntário de dados.

Nesse ambiente de hiperconectividade, a assimetria entre fornecedores e consumidores é acentuada. Os primeiros detêm tecnologia e meios sofisticados para coletar e manipular dados, enquanto os segundos, em regra, não compreendem a extensão do uso de suas informações. Esse cenário intensifica a vulnerabilidade do consumidor, especialmente em contratações eletrônicas, nas quais muitas vezes a aceitação de cláusulas ocorre de forma automática, sem efetiva leitura ou compreensão.

A promulgação da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) representou um marco jurídico no Brasil, ao estabelecer parâmetros claros para o tratamento de dados pessoais, aplicáveis tanto ao setor público quanto ao privado. Inspirada em modelos internacionais, como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a LGPD busca equilibrar o desenvolvimento econômico com a preservação dos direitos fundamentais à privacidade e à autodeterminação informacional.

No comércio eletrônico, a influência da LGPD é direta e profunda. A lei obriga plataformas digitais a reverem práticas consolidadas de coleta e uso de informações, impondo requisitos como: obtenção de consentimento válido, dever de transparência, adoção de medidas de segurança e comunicação de incidentes. Além disso, atribui papel central à Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar e orientar a aplicação da norma.

A relevância do tema justifica-se pela necessidade de compreender de que forma a LGPD transforma as práticas empresariais no e-commerce e fortalece a proteção jurídica dos consumidores. A análise é pertinente não apenas do ponto de vista teórico, mas também prático, pois envolve desafios enfrentados por empresas de diferentes portes, consumidores hipervulneráveis e o próprio Estado enquanto regulador.

O objetivo geral deste artigo é analisar como a LGPD influencia as práticas de comércio eletrônico e em que medida contribui para a proteção dos dados pessoais dos consumidores. Como objetivos específicos, pretende- se examinar a relação entre direitos fundamentais, vulnerabilidade do consumidor e proteção de dados, identificar os principais impactos da LGPD nas operações de e-commerce e discutir desafios e perspectivas futuras para a efetividade da norma.

A metodologia utilizada será de natureza qualitativa, com base em pesquisa

bibliográfica, documental e jurisprudencial. O trabalho se estrutura em seis capítulos além desta introdução: no segundo capítulo, aborda-se a relação entre direitos fundamentais e proteção do consumidor digital; no terceiro, analisam-se as peculiaridades jurídicas do comércio eletrônico; no quarto, examina-se a LGPD e suas disposições aplicáveis ao e-commerce; no quinto, discutem-se os impactos concretos da lei sobre as práticas digitais; no sexto, apresentam-se desafios e perspectivas futuras; e, por fim, apresentam-se as conclusões do estudo.

Portanto, o presente artigo pretende contribuir para o debate sobre a efetividade da LGPD no ambiente digital, especialmente no contexto do comércio eletrônico, onde se evidencia a tensão entre inovação tecnológica e a proteção de direitos fundamentais do consumidor.

2. DIREITO FUNDAMENTAIS, RELAÇÕES DE CONSUMO E PROTEÇÃO DE DADOS

A proteção de dados pessoais é um dos temas mais relevantes da contemporaneidade, especialmente diante do avanço das tecnologias de informação e comunicação. A Constituição Federal de 1988, ao estabelecer a dignidade da pessoa humana como um dos fundamentos da República (art. 1º, III), deu base normativa para a construção de uma cultura de respeito à privacidade e à intimidade, valores estes reafirmados no art. 5º, incisos X e XII.

Com a Emenda Constitucional nº 115/2022, a proteção de dados pessoais foi elevada expressamente à condição de direito fundamental autônomo, conforme o art. 5º, inciso LXXIX, que dispõe: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais." Essa inovação demonstra o reconhecimento, pelo legislador constituinte, da centralidade da informação na vida contemporânea e da necessidade de resguardar o indivíduo frente aos riscos decorrentes do uso indevido de seus dados.

Como observa Sarlet (2015, p. 37):

> A proteção da pessoa humana no Estado Constitucional contemporâneo não se limita à salvaguarda da vida física, mas se estende à sua esfera informacional, reconhecendo-se que o controle sobre os próprios dados é elemento essencial da liberdade e da autodeterminação.

Nesse sentido, a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), representa o marco normativo brasileiro sobre o tratamento de dados pessoais, criando um regime jurídico específico para garantir transparência, segurança e finalidade

legítima na coleta e uso de informações. A norma é inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), adotando princípios semelhantes, como finalidade, necessidade, adequação e transparência.

Segundo Doneda (2006, p. 51):

> A proteção de dados deve ser compreendida como um instrumento de concretização da dignidade da pessoa humana, pois assegura ao indivíduo o poder de decidir sobre o uso e a circulação de suas informações pessoais, evitando que seja transformado em mero objeto das dinâmicas informacionais do mercado.

A proteção de dados, portanto, é expressão concreta da liberdade informacional, princípio que permite ao titular de dados controlar como suas informações são coletadas, utilizadas e compartilhadas. Esse controle está diretamente relacionado à autonomia privada, conceito essencial nas relações contratuais e, especialmente, nas relações de consumo.

O Código de Defesa do Consumidor (Lei nº 8.078/1990) já havia antecipado parte dessa preocupação ao consagrar o direito à informação (art. 6º, III) e à segurança contra riscos (art. 8º), além de reconhecer a vulnerabilidade do consumidor (art. 4º, I). Essa vulnerabilidade se acentua no contexto do comércio eletrônico, onde o consumidor, diante da assimetria técnica e informacional, é considerado hipervulnerável.

Como destacam Benjamin, Marques e Bessa (2016, p. 147):

> No ambiente digital, a vulnerabilidade do consumidor atinge níveis sem precedentes, pois os mecanismos de coleta e tratamento de dados são invisíveis, automáticos e contínuos, tornando o consumidor sujeito a decisões que o afetam sem que sequer tenha consciência do processo.

A proteção de dados pessoais no âmbito das relações de consumo, portanto, não é apenas um dever ético, mas um imperativo jurídico. O tratamento indevido de informações configura violação à boa-fé objetiva, aos princípios da transparência e da confiança legítima, pilares estruturantes do sistema protetivo do consumidor.

Blum (2018, p. 69) complementa:

> A proteção de dados pessoais transcende a mera preocupação com a privacidade, constituindo-se como elemento essencial da proteção do consumidor moderno, uma vez que a economia digital é sustentada pela informação como principal ativo econômico.

Assim, o reconhecimento da proteção de dados como direito fundamental e sua aplicação no contexto das relações de consumo revelam o esforço do Estado e da doutrina em assegurar um equilíbrio entre inovação tecnológica e proteção dos direitos da personalidade, reafirmando o compromisso constitucional com a dignidade humana.

3. O COMÉRCIO ELETRÔNICO E SEUS DESAFIOS JURÍDICOS

O comércio eletrônico transformou profundamente as relações de consumo, ampliando o acesso a produtos e serviços, mas também introduzindo novos desafios jurídicos relacionados à proteção do consumidor e à segurança dos dados pessoais. No Brasil, o Decreto nº 7.962/2013 regulamenta o Código de Defesa do Consumidor (Lei nº 8.078/1990) no ambiente digital, estabelecendo diretrizes sobre informação adequada, atendimento facilitado e respeito ao direito de arrependimento.

No entanto, a mera existência de normas legais não garante a efetividade dos direitos consumeristas. O ambiente digital é caracterizado por uma forte assimetria informacional, na qual o consumidor muitas vezes não tem plena consciência da forma como seus dados são coletados, armazenados e compartilhados. Essa realidade exige uma interpretação ampliada dos princípios da boa-fé objetiva, da transparência e da confiança legítima, pilares que sustentam a proteção do consumidor também nas transações virtuais.

Como observa Marques (2003, p. 89):

> A regulação jurídica do comércio eletrônico deve ir além da formalidade normativa, exigindo-se políticas de fiscalização, educação digital e responsabilização efetiva dos agentes econômicos para que os princípios do CDC se concretizem no ambiente virtual.

Entre os principais problemas enfrentados no e-commerce estão as fraudes digitais, os contratos eletrônicos de adesão e o tratamento indevido de dados pessoais. O direito de arrependimento, previsto no art. 49 do CDC, muitas vezes é dificultado por procedimentos burocráticos e resistência das plataformas, evidenciando uma lacuna entre a norma e a prática.

Além disso, o compartilhamento não autorizado de informações pessoais representa uma violação direta à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), que determina que o tratamento de dados deve se basear em finalidade legítima, consentimento expresso e transparência. Nesse contexto, o Superior Tribunal de Justiça (STJ) tem consolidado o entendimento de que as plataformas de comércio eletrônico devem garantir segurança e confidencialidade no tratamento de dados.

O Recurso Especial nº 1.737.428/SC é um exemplo emblemático desse posicionamento, tendo reconhecido a responsabilidade objetiva das plataformas digitais

por fraudes decorrentes de falhas de segurança.

> EMENTA: Direito do consumidor. Comércio eletrônico. Fraude em transação digital. Responsabilidade objetiva. Dano moral e material. Art. 14 do CDC. O fornecedor de comércio eletrônico responde objetivamente pelos danos causados por falhas de segurança que resultem em prejuízos ao consumidor, sendo irrelevante a comprovação de culpa. (STJ, REsp 1.737.428/SC, Rel. Min. Nancy Andrighi, 3ª Turma, DJe 2017).

A referida decisão representa um importante avanço na consolidação da responsabilidade das plataformas digitais no âmbito das relações de consumo. Ao reconhecer a responsabilidade objetiva dos fornecedores de e-commerce, o Superior Tribunal de Justiça reforçou que a segurança da informação constitui um dever jurídico essencial, e não apenas uma prática recomendável. Isso significa que as empresas devem adotar medidas preventivas e corretivas eficazes para evitar o vazamento, o uso indevido ou o acesso não autorizado aos dados pessoais de seus consumidores.

A responsabilização objetiva, prevista no art. 14 do Código de Defesa do Consumidor, tem como finalidade assegurar que o consumidor, parte mais vulnerável na relação, não seja onerado pela necessidade de comprovar culpa do fornecedor. Tal entendimento se coaduna com o princípio da boa-fé objetiva e com a teoria do risco do empreendimento, segundo a qual aquele que aufere lucro com determinada atividade deve suportar os riscos dela decorrentes.

No ambiente virtual, essa responsabilidade assume contornos ainda mais relevantes, uma vez que as transações ocorrem de forma automatizada e dependem de sistemas digitais interconectados. Qualquer falha de segurança pode expor milhares de consumidores simultaneamente, gerando danos de grande proporção, tanto de natureza material quanto moral.

Como ressalta Pinheiro (2020, p. 104):

> A economia digital se apoia na exploração de dados pessoais como recurso estratégico, mas essa lógica não pode se sobrepor aos direitos fundamentais. O desafio jurídico está em conciliar a inovação tecnológica com o respeito à privacidade e à autodeterminação informativa.

Assim, verifica-se que o comércio eletrônico, embora essencial ao desenvolvimento econômico contemporâneo, exige um arcabouço jurídico sólido e a responsabilidade proativa das empresas quanto à segurança da informação. A LGPD, em conjunto com o CDC, constitui um sistema protetivo integrado, cuja finalidade é equilibrar o poder nas relações digitais e garantir a efetividade dos direitos fundamentais do consumidor.

4. A LEI GERAL DE PROTEÇÃO DE DADOS E O E-COMMERCE

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) representa um marco regulatório essencial para a proteção dos direitos fundamentais de liberdade e privacidade no contexto digital. No comércio eletrônico, a LGPD se aplica de forma direta, uma vez que as operações de compra e venda realizadas por meio da internet envolvem o tratamento massivo de dados pessoais, desde o cadastro do consumidor até o processamento de pagamentos e o envio de produtos.

De acordo com o art. 1º da LGPD, a lei "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou

privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". Assim, o tratamento de dados em plataformas digitais deve observar princípios como finalidade, necessidade, transparência, segurança e prevenção, garantindo que o consumidor mantenha o controle sobre suas informações.

Conforme explica Doneda (2021, p. 57):

> A LGPD não se limita a impor regras técnicas, mas institui uma nova cultura jurídica baseada na responsabilidade e na ética digital. Trata-se de um instrumento que busca equilibrar a assimetria de poder entre titulares e controladores de dados, estabelecendo deveres de transparência e segurança como pilares da confiança nas relações digitais."

No comércio eletrônico, a aplicação desses princípios exige uma revisão das práticas empresariais, desde a coleta de dados até o descarte das informações, impondo maior rigor na proteção da privacidade do consumidor.

4.1 Princípios Aplicáveis ao Tratamento de Dados no E-commerce

O art. 6º da LGPD estabelece os princípios que norteiam o tratamento de dados pessoais, destacando-se: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção e responsabilização. No comércio eletrônico, tais princípios ganham relevância prática, pois o compartilhamento de dados é constante e envolve diversos agentes, plataformas, intermediadores de pagamento, transportadoras e serviços de marketing digital.

A aplicação desses princípios garante que o consumidor tenha ciência de como suas informações são utilizadas e que as empresas adotem práticas compatíveis com o mínimo necessário para a execução da relação contratual. A transparência e a prevenção são

fundamentais para reduzir riscos de incidentes de segurança, vazamentos e fraudes digitais.

Segundo Bioni (2019, p. 132):

> A concretização da proteção de dados pessoais no comércio eletrônico depende da implementação efetiva dos princípios previstos na LGPD. Esses princípios devem orientar toda a cadeia de tratamento de dados, desde a concepção do serviço até sua execução, sob pena de comprometer a confiança do consumidor e a legitimidade da atividade econômica digital.

Assim, o respeito aos princípios da LGPD se apresenta como elemento central para a construção de uma relação de consumo digital ética e segura.

4.2 Bases Legais para o Tratamento de Dados no Comércio Eletrônico

A LGPD, em seu art. 7º, prevê diversas bases legais que autorizam o tratamento de dados pessoais. No comércio eletrônico, as mais comuns são:

a) o consentimento do titular;

b) o cumprimento de obrigação legal ou regulatória;

c) a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular;

d) o legítimo interesse do controlador, desde que respeitados os direitos e liberdades fundamentais do consumidor.

O consentimento deve ser livre, informado e inequívoco, sendo indispensável que o consumidor tenha acesso claro e objetivo às finalidades do tratamento. Ademais, as plataformas digitais devem disponibilizar políticas de privacidade compreensíveis, conforme o art. 9º da LGPD, garantindo ao consumidor o direito de saber quais dados são coletados, por quanto tempo são armazenados e se há compartilhamento com terceiros.

Como destaca Mendonça (2020, p. 88):

> O tratamento de dados pessoais baseado no consentimento do consumidor demanda não apenas a obtenção formal de autorização, mas a efetiva compreensão do titular sobre o alcance e as consequências de sua decisão. O consentimento deve ser uma manifestação autêntica de vontade, e não um mero clique em caixas de seleção.

Portanto, a observância das bases legais previstas na LGPD assegura maior legitimidade e confiabilidade às práticas de e-commerce, fortalecendo a proteção dos consumidores e reduzindo riscos de responsabilização jurídica para as empresas.

4.3 Responsabilidade e Sanções no Tratamento Indevido de Dados

O descumprimento das normas da LGPD sujeita o infrator a sanções administrativas e civis. De acordo com o art. 52, a Autoridade Nacional de Proteção de Dados (ANPD) pode aplicar penalidades como advertência, multa simples ou diária, publicização da infração, bloqueio ou eliminação dos dados pessoais relacionados à infração.

Além disso, o art. 42 da LGPD prevê a responsabilidade solidária entre o controlador e o operador de dados, quando houver violação às normas de tratamento. Essa responsabilidade civil se soma à responsabilidade objetiva prevista no art. 14 do Código de Defesa do Consumidor, aplicável às plataformas de comércio eletrônico que não garantirem a segurança das informações de seus usuários.

Segundo Santos (2022, p. 76):

> A LGPD reforça o dever de cuidado das empresas digitais, que passam a responder não apenas pelos danos materiais, mas também pelos danos morais decorrentes do tratamento indevido de dados. O consumidor deve ser protegido de práticas abusivas e de falhas que comprometam sua privacidade, em consonância com os princípios da dignidade da pessoa humana e da boa-fé objetiva.

Assim, a conjugação entre a LGPD e o CDC consolida um regime de dupla proteção jurídica ao consumidor digital, promovendo maior equilíbrio nas relações de consumo e incentivando as empresas a adotar políticas de compliance em proteção de dados.

4.4 A Atuação da ANPD no Comércio Eletrônico

A Autoridade Nacional de Proteção de Dados (ANPD) foi criada pela Lei nº 13.853/2019, que alterou a LGPD, com o objetivo de zelar pela proteção dos dados pessoais e pela aplicação da legislação de forma uniforme em todo o território nacional. No contexto do comércio eletrônico, a ANPD desempenha um papel estratégico na fiscalização, regulamentação e orientação das empresas que realizam o tratamento de dados de consumidores.

O art. 55-J da LGPD define as competências da ANPD, entre as quais destacam-se:

I – zelar pela proteção dos dados pessoais;

II – elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;

III – fiscalizar e aplicar sanções em caso de tratamento de dados realizado em

desconformidade com a legislação;

IV – promover o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança.

A presença da ANPD reforça a necessidade de que as plataformas de e-commerce adotem políticas de governança em privacidade, relatórios de impacto à proteção de dados e programas de compliance digital, a fim de demonstrar responsabilidade proativa no tratamento das informações.

Como explica Monteiro (2021, p. 142):

> A ANPD é o principal instrumento de concretização da LGPD, atuando não apenas de forma repressiva, mas também orientadora. Seu papel educativo é essencial para que empresas e consumidores compreendam o valor jurídico e ético dos dados pessoais, promovendo uma cultura de respeito à privacidade e à transparência.

Além do aspecto regulatório, a ANPD possui função pedagógica, buscando conscientizar o setor empresarial sobre a importância da conformidade legal. Em muitos casos, a autoridade opta por medidas de orientação e advertência antes da aplicação de multas, conforme previsto no art. 52, §1º, inciso I, da LGPD, priorizando o ajuste das condutas empresariais.

Para Ferreira (2022, p. 95):

> A atuação da ANPD deve ser compreendida como um elemento de equilíbrio entre o poder público e o setor privado. No comércio eletrônico, sua intervenção é decisiva para garantir que a inovação tecnológica ocorra dentro dos limites da legalidade e da ética, preservando os direitos dos consumidores.

A ANPD também se destaca pela elaboração de guias orientativos e notas técnicas, como o Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte (2021), que fornece diretrizes específicas para micro e pequenas empresas. Esse tipo de documento tem impacto direto no e-commerce, uma vez que grande parte das lojas virtuais no Brasil pertence a pequenos empreendedores que precisam de orientações práticas para adequação à LGPD.

A consolidação da ANPD como órgão autônomo – alcançada em 2022 com sua transformação em autarquia de natureza especial – reforça sua legitimidade institucional e capacidade de fiscalização. Isso demonstra o fortalecimento da governança regulatória no Brasil e o compromisso do Estado com a efetiva proteção de dados no ambiente digital.

Dessa forma, a atuação da ANPD no comércio eletrônico não se limita à imposição de sanções, mas se projeta como um mecanismo de garantia de direitos fundamentais. Ao promover o equilíbrio entre inovação, consumo e privacidade, a autoridade contribui para

a construção de um ecossistema digital mais seguro, transparente e confiável para os consumidores brasileiros.

5. IMPACTOS DA LGPD NAS PRÁTICAS COMERCIAIS DIGITAIS

A entrada em vigor da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) representou um marco regulatório de grande relevância para o comércio eletrônico no Brasil, gerando transformações profundas nas práticas empresariais, nos processos internos das plataformas digitais e na relação entre consumidores e fornecedores. Entre as mudanças mais significativas destaca-se a necessidade de reformulação das políticas de privacidade das empresas, que passaram a ser estruturadas de acordo com os princípios e diretrizes da LGPD, garantindo maior clareza, transparência e objetividade na apresentação das informações relacionadas à coleta, armazenamento, uso e compartilhamento de dados pessoais (BENJAMIN; MARQUES; BESSA, 2016, p. 135).

Essa reformulação não apenas assegura a conformidade legal, mas também contribui para a construção de um ambiente digital mais seguro, capaz de reduzir riscos de incidentes de segurança e fortalecer a confiança do consumidor. Outro ponto crucial é a exigência de consentimento expresso do titular para atividades como o envio de publicidade e a transferência de dados a terceiros. Diferentemente de práticas anteriores, em que o consentimento era muitas vezes tácito ou obtido de forma genérica, a LGPD impõe que o consumidor tenha conhecimento claro e inequívoco sobre a finalidade do tratamento de seus dados, podendo exercer controle efetivo sobre suas informações. Essa obrigação legal fortalece a autonomia do consumidor e limita o uso abusivo de dados para fins comerciais, evitando que a informação pessoal seja utilizada como instrumento de manipulação ou exploração mercadológica.

A lei também trouxe impactos na transparência contratual, exigindo que os contratos e termos de uso explicitem detalhadamente as finalidades da coleta e do tratamento de dados pessoais. Tal medida reforça a compreensão das relações digitais e contribui para equilibrar a relação entre consumidores e fornecedores, mitigando a assimetria de informações que historicamente caracteriza o comércio eletrônico. Como consequência dessas medidas, observa-se um fortalecimento da confiança do consumidor, elemento essencial para a expansão sustentável do e-commerce, pois a segurança e a transparência nas transações digitais são fatores determinantes para a fidelização do

público e para a consolidação da reputação das empresas no mercado digital. Por outro lado, a implementação da LGPD também revelou desafios significativos, especialmente para micro e pequenas empresas, que frequentemente enfrentam limitações técnicas, financeiras e estruturais para adequar seus sistemas, processos e políticas de governança à nova legislação LGPD (BIONI, 2019, p. 82).

A necessidade de investimentos em tecnologias de segurança da informação, auditorias periódicas, programas de compliance digital e capacitação de colaboradores representa um obstáculo considerável para empresas de menor porte, podendo gerar disparidades na forma como a lei é efetivamente aplicada em diferentes segmentos do mercado. Além disso, muitos consumidores ainda apresentam baixo nível de compreensão sobre seus direitos e sobre os mecanismos de controle e proteção de seus dados, o que compromete a efetividade plena da norma. A Autoridade Nacional de Proteção de Dados (ANPD), por sua vez, enfrenta desafios relacionados à capacidade de fiscalização, à cobertura territorial e à complexidade das transações digitais, limitando sua atuação e exigindo aprimoramento estrutural e operacional.

Em síntese, embora a LGPD represente um avanço regulatório essencial, que promove maior equilíbrio, segurança e transparência nas relações digitais, sua efetividade depende de um esforço conjunto entre empresas, consumidores e Estado. Ponticelli (2018, p. 52) observa que a implementação plena da lei exige não apenas a adaptação de processos internos e políticas corporativas, mas também educação digital, conscientização sobre direitos e deveres, fortalecimento da fiscalização e cultura de proteção de dados, de modo a consolidar um ambiente de comércio eletrônico mais seguro, ético e confiável, capaz de aliar inovação tecnológica à preservação de direitos fundamentais dos consumidores.

6. DESAFIOS E PERSPECTIVAS FUTURAS

O futuro da proteção de dados no comércio eletrônico brasileiro está intrinsicamente ligado a três fatores centrais que demandam atenção de empresas, consumidores e do Estado. Primeiramente, a educação digital dos consumidores se mostra essencial, pois apenas cidadãos conscientes de seus direitos e da forma como suas informações pessoais são coletadas, armazenadas e utilizadas conseguem exercer controle efetivo sobre seus dados. A compreensão de conceitos como consentimento, finalidade, minimização de dados e direito de acesso permite que os usuários tomem decisões mais

seguras e informadas, evitando situações de hipervulnerabilidade e práticas abusivas por parte de fornecedores (PINHEIRO, 2020, p. 123).

Em segundo lugar, destaca-se o fortalecimento da atuação da Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável pela fiscalização e orientação quanto à aplicação da LGPD. Para garantir a efetividade da lei, é necessário ampliar sua estrutura, investir em capacitação técnica e em ferramentas que permitam monitorar e auditar o cumprimento das normas por empresas de diferentes portes e setores. Somente com uma fiscalização efetiva e abrangente será possível reduzir irregularidades, prevenir incidentes de segurança e responsabilizar de forma adequada os agentes que descumprirem a legislação.

Por fim, a integração internacional da regulação de proteção de dados representa um fator estratégico para o comércio eletrônico em um contexto globalizado. A aproximação da LGPD com legislações internacionais, como o Regulamento Geral de Proteção de Dados (GDPR) europeu, é fundamental para garantir segurança jurídica em transações internacionais, permitir a cooperação regulatória e assegurar que empresas brasileiras possam competir de forma transparente e confiável no mercado global.

A efetividade da LGPD, portanto, vai além da mera formalidade normativa; exige também uma mudança cultural profunda. As empresas devem internalizar a proteção de dados como um valor estratégico, incorporando princípios de transparência, segurança e ética em todas as suas operações digitais. Sampaio (2019, p. 41) enfatiza que os consumidores precisam reconhecer a importância de sua privacidade como direito fundamental inalienável, assumindo papel ativo na defesa de suas informações pessoais. Somente por meio dessa combinação de educação, fiscalização robusta e alinhamento internacional será possível consolidar um ambiente digital seguro, equilibrado e confiável, no qual o desenvolvimento econômico caminhe em harmonia com a proteção dos direitos fundamentais dos cidadãos.

7. CONCLUSÃO

Em conclusão, a Lei Geral de Proteção de Dados Pessoais (LGPD) representa um marco regulatório de grande relevância para a proteção dos direitos fundamentais no Brasil, destacando-se especialmente no contexto do comércio eletrônico e das relações digitais, que se expandem de forma acelerada na sociedade contemporânea. Ao estabelecer

princípios claros, como finalidade, necessidade, transparência e responsabilização, a LGPD cria parâmetros seguros para o tratamento de dados pessoais, reforçando a confiança dos consumidores e promovendo maior equilíbrio nas relações entre indivíduos e empresas no ambiente digital. Nesse sentido, a lei não apenas protege os titulares de dados, mas também proporciona segurança jurídica às organizações que operam no espaço online, incentivando práticas responsáveis e éticas na coleta, armazenamento e compartilhamento de informações.

Contudo, apesar dos avanços normativos, a efetividade da LGPD ainda enfrenta desafios significativos. Pequenas e médias empresas encontram dificuldades para se adequar às exigências legais devido a limitações financeiras, estruturais e tecnológicas, o que pode comprometer sua plena implementação. Paralelamente, observa-se uma lacuna de conscientização por parte dos consumidores, que muitas vezes desconhecem seus direitos de acesso, correção, exclusão e portabilidade de dados, limitando o exercício efetivo da proteção prevista pela lei. Além disso, a Autoridade Nacional de Proteção de Dados (ANPD), órgão. responsável pela fiscalização e orientação quanto ao cumprimento da norma, enfrenta restrições operacionais e de recursos, o que exige esforços adicionais para assegurar a uniformidade e a efetividade da legislação.

Superar essas dificuldades demanda um esforço coordenado entre Estado, iniciativa privada e sociedade civil, envolvendo a implementação de políticas de educação digital, campanhas de conscientização, capacitação de empresas e o fortalecimento institucional da ANPD. Somente com a articulação desses atores será possível garantir que a LGPD cumpra plenamente seu papel de tutelar os direitos fundamentais dos indivíduos, promovendo um ambiente digital seguro, transparente e confiável.

Dessa forma, a LGPD não deve ser compreendida como um obstáculo à inovação ou ao crescimento econômico, mas como um instrumento de equilíbrio entre desenvolvimento digital e proteção de direitos, capaz de consolidar uma cultura de responsabilidade no tratamento de dados pessoais. Ao proporcionar segurança jurídica e ética nas relações digitais, a lei contribui para a construção de um ambiente mais democrático, em que empresas e consumidores possam interagir de maneira transparente e confiável, consolidando práticas de governança de dados que fortalecem tanto a competitividade econômica quanto a proteção dos direitos fundamentais no Brasil.

REFERÊNCIAS

BENJAMIN, Antônio Herman de Vasconcellos e. **Código brasileiro de defesa do consumidor: comentado pelos autores do anteprojeto.** Rio de Janeiro: Forense, 2011.

BENJAMIN, Antônio Herman; MARQUES, Cláudia Lima; BESSA, Leonardo Roscoe.

Manual de Direito do Consumidor. Revista dos Tribunais, 2016.

BLUM, Rita Peixoto Ferreira. **O direito à privacidade e à proteção de dados do consumidor.**São Paulo: Almedina, 2018.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.**São Paulo: Thomson Reuters Brasil, 2019.

BORELLI, Alessandra et al. **LGDP: Lei Geral de Proteção de Dados Comentada.** 2ª ed. São Paulo: Thomson Reuters Brasil, 2019.

BRASIL. **Constituição da República Federativa do Brasil de 1988.**

BRASIL. **Decreto nº 7.962, de 15 de março de 2013. Regulamenta a contratação no comércio eletrônico.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm. Acesso em: 24 set. 2025.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor.** Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 24 set. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 24 set. 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

G1. **Netshoes diz que dados de clientes podem ter sido vazados após incidente cibernético.** G1, 17 jul. 2024. Disponível em: https://g1.globo.com/tecnologia/noticia/2024/07/17/netshoes-diz-que-dados-de-clientes-podem-ter-sido-vazados-apos-incidente-cibernetico.ghtml. Acesso em: 24 set. 2025.

MARQUES, Cláudia Lima. **Comentários ao Código de Defesa do Consumidor.** São Paulo: Revista dos Tribunais, 2003.

PEZZI, Ana Paula Jacobus. **A necessidade proteção dos dados pessoais nos arquivos de consumo: em busca da concretização do direito á privacidade.** 2007. 215 f. Dissertação (Mestrado em Direito) – Curso de Pós-Graduação em Direito, Universidade do Vale do Rio dos Sinos, São Leopoldo, 2007. Disponível em:

http://www.dominiopublico.gov.br/download/teste/arqs/cp042824.pdf. Acesso em: 25 set. 2025.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD).** 2ª ed. São Paulo: Saraiva Jur, 2020.

PONTICELLI, Murilo Meneguel. **O direito fundamental à privacidade no âmbito da rede mundial de computadores com o advento da lei geral de proteção de dados.** 2018. 57 f. Monografia (Bacharelado em Direito) – Curso de Graduação em Direito, Universidade do Sul de Santa Catarina, Tubarão, 2018. Disponível em: http://www.riuni.unisul.br/handle/12345/6288. Acesso em: 25 set. 2025.

SAMPAIO, Carlos Eduardo Ferreira. **Privacidade virtual e divulgação de dados íntimos nas plataformas digitais.** 2019. Monografia (Graduação em Direito) – Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, 2019. Disponível em: https://repositorio.uniceub.br/jspui/handle/prefix/13547. Acesso em: 25 set. 2025.

SENADO. **Lei Geral de Proteção de Dados Pessoais entra em vigor.** Site do Senado Federal, 2020. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor. Acesso em: 25 set. 2025.

STJ. **REsp 1.737.428/SC.** Rel. Min. Nancy Andrighi. 3ª Turma. DJe 2017. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/busca?q=resp+1.737.428-rs. Acesso em: 25 set. 2025.

TARTUCE, Flávio. **Manual de direito civil: volume único.** Rio de Janeiro: Forense; São Paulo: Método, 2020.

TARTUCE, Flávio. **Manual de direito do consumidor: direito material e direito processual. 5ª ed. São Paulo: Método, 2016.**