

Impactos da Lei Geral de Proteção de Dados (LGPD) no Comércio Digital no Brasil

Daniel Silva Mendanha¹
Camila Valera Reis Henrique²
Ana Celia de Julio³
Laiana Delakis Recanello⁴
Camila Varanda Brizzi Trizzi⁵
Erli Henrique Garcia⁶

Resumo: A entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD) representou um marco regulatório para o comércio digital brasileiro. Este artigo analisou seus impactos sob a ótica das empresas, dos consumidores e do poder público. Foram abordados os fundamentos jurídicos da proteção de dados, os desafios de conformidade enfrentados pelas organizações, o fortalecimento dos direitos dos consumidores e o papel da Autoridade Nacional de Proteção de Dados (ANPD). Também foram examinadas experiências internacionais, em especial o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), e as perspectivas futuras para o Brasil diante de novas tecnologias como inteligência artificial e big data. Conclui-se que a LGPD, embora ainda em fase de consolidação, já promove avanços significativos na construção de um ambiente digital mais ético, seguro e confiável, sendo indispensável o fortalecimento da ANPD, a conscientização dos consumidores e o engajamento das empresas na implementação de políticas de compliance e segurança da informação.

Palavras-chave: LGPD; comércio digital; proteção de dados; direitos do consumidor; segurança da informação.

Abstract: The enactment of Brazil's General Data Protection Law (LGPD) represented a regulatory milestone for digital commerce. This article examined its impacts from the perspective of companies, consumers, and public authorities. It analyzed the legal foundations of data protection, compliance challenges faced by organizations, the strengthening of consumer rights, and the role of the National Data Protection Authority (ANPD).

¹Possui Especialização em Direito Civil e Docência pelo Centro Universitário Leonardo da Vinci, UNIASSELVI, Brasil (2020).

² Mestrado em Direito. Centro Universitário Eurípides de Marília, UNIVEM, Brasil.(2022)

³ Mestrado em Direito Negocial. Universidade Estadual de Londrina, UEL, Brasil.(2006)

⁴ Mestrado em Ciências Jurídicas. Universidade Estadual do Norte do Paraná, UENP, Brasil.(2013)

⁵ Graduação em Direito. União das Faculdades do Mato Grosso, UNIFAMA, Brasil.(2024)

⁶ Mestrado em Direito Criminal. Universidade Católica Portuguesa, UCP, Portugal.(2010)

International experiences, particularly the European Union's General Data Protection Regulation (GDPR), were also addressed, as well as future perspectives in light of emerging technologies such as artificial intelligence and big data. The study concludes that, although still in a consolidation phase, the LGPD has already significantly advanced the development of a more ethical, secure, and trustworthy digital environment. Strengthening ANPD, raising consumer awareness, and encouraging companies to adopt compliance and information security policies are essential steps for the law's effectiveness.

Keywords: LGPD; digital commerce; data protection; consumer rights; information security.

1. INTRODUÇÃO

O crescimento do comércio digital no Brasil, impulsionado pela expansão do acesso à internet e pelo desenvolvimento de plataformas de e-commerce, consolidou-se como um dos principais motores da economia nacional na última década. Segundo dados da Ebit Nielsen (2022), o comércio eletrônico brasileiro movimentou mais de R\$160 bilhões em 2021, demonstrando a centralidade desse setor na dinâmica econômica contemporânea.

Entretanto, a intensificação do uso de tecnologias digitais trouxe novos desafios relacionados à coleta, ao armazenamento e ao tratamento de dados pessoais. O ambiente digital tornou-se espaço privilegiado para práticas de mineração de dados (*data mining*) e de perfis de consumo (*consumer profiling*), levantando preocupações quanto à proteção da privacidade, à segurança da informação e à defesa dos direitos dos consumidores.

Nesse contexto, a promulgação da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) – representou um marco normativo no ordenamento jurídico brasileiro. Inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a LGPD estabeleceu princípios, direitos e obrigações destinados a disciplinar o tratamento de dados pessoais em qualquer atividade econômica, com especial impacto sobre o comércio digital (DONEDA, 2019; LEMOS, 2020).

A entrada em vigor da LGPD, em setembro de 2020, exigiu das empresas de comércio eletrônico profundas adequações organizacionais, incluindo a revisão de políticas de privacidade, a implementação de mecanismos de consentimento informado, o fortalecimento da segurança da informação e a criação de canais de atendimento ao titular de dados. Tais mudanças, embora custosas, são fundamentais para a construção de um ambiente digital mais confiável e ético (OLIVEIRA, 2021; PIMENTA, 2022).

Este trabalho tem como objetivo analisar os impactos da LGPD no comércio digital brasileiro, partindo dos fundamentos normativos da proteção de dados, discutindo os desafios de conformidade enfrentados pelas empresas, os reflexos para os direitos dos consumidores e as perspectivas futuras de regulamentação e fiscalização.

2. FUNDAMENTOS DA PROTEÇÃO DE DADOS NO COMÉRCIO DIGITAL

O comércio digital contemporâneo não se limita à mera transação de bens ou serviços, mas depende, em grande medida, da coleta e análise de dados pessoais dos consumidores. A economia digital é marcada pela chamada “economia de dados”, em que informações pessoais tornam-se ativos estratégicos para empresas, influenciando desde campanhas publicitárias personalizadas até decisões automatizadas de crédito (ZUBOFF, 2019).

No Brasil, o crescimento do setor de e-commerce foi acompanhado por práticas intensivas de coleta de dados, muitas vezes realizadas sem transparência adequada ou consentimento válido dos titulares. Esse cenário demandou a positivação de um marco legal que equilibrasse inovação tecnológica, desenvolvimento econômico e proteção de direitos fundamentais.

A LGPD define dados pessoais como “informação relacionada a pessoa natural identificada ou identificável” (art. 5º, I). Inclui ainda a categoria de dados pessoais sensíveis, que exigem proteção reforçada, abrangendo informações sobre origem racial, convicção religiosa, opinião política, saúde, vida sexual, dados genéticos ou biométricos (art. 5º, II).

O tratamento de dados deve observar princípios como finalidade, adequação, necessidade, transparência e segurança (art. 6º). Para que seja lícito, deve basear-se em uma das hipóteses previstas no art. 7º, destacando-se o consentimento do titular. Como destaca Doneda (2019), a lei positivou no Brasil a noção de autodeterminação informativa, reconhecendo ao indivíduo o poder de controlar o uso de seus dados pessoais.

No comércio eletrônico, os direitos dos titulares previstos na LGPD assumem relevância especial. Os consumidores têm direito a: a) confirmar a existência de tratamento de seus dados (art. 18, I); b) acessar os dados tratados (art. 18, II); c) corrigir informações incompletas, inexatas ou desatualizadas (art. 18, III); d) solicitar anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos (art. 18, IV); e) portabilidade dos dados (art. 18, V); f) eliminação dos dados tratados com consentimento (art. 18, VI).

Esses direitos visam corrigir a assimetria informacional típica das relações de consumo digitais, nas quais empresas detêm grande poder sobre os dados coletados. Como argumenta Ronaldo Lemos (2020), a efetividade da LGPD reside justamente na sua capacidade de devolver ao consumidor o controle sobre o fluxo de suas informações.

A ANPD, criada pela Lei nº 13.853/2019, é o órgão responsável por zelar pela aplicação da LGPD, editar normas complementares e fiscalizar o cumprimento da legislação. Seu papel é central para garantir a efetividade da proteção de dados no comércio digital.

A atuação da ANPD envolve tanto a função educativa, por meio da emissão de guias orientativos e recomendações, quanto a função sancionatória, mediante aplicação de advertências, multas e até a suspensão de atividades de tratamento de dados (ANPD, 2021).

No entanto, como observa Danilo Doneda (2020), a efetividade da ANPD depende de sua independência técnica e de recursos adequados para desempenhar suas atribuições, sob pena de se tornar um órgão meramente formal, incapaz de enfrentar as complexas práticas de tratamento de dados no comércio eletrônico.

3. FUNDAMENTOS DA PROTEÇÃO DE DADOS NO COMÉRCIO DIGITAL

A entrada em vigor da LGPD representou um marco disruptivo para as empresas que atuam no comércio eletrônico. A necessidade de revisão das práticas de coleta e tratamento de dados implicou custos financeiros, tecnológicos e organizacionais. Conforme destaca Oliveira (2021), muitas empresas tiveram que implementar novos sistemas de segurança, contratar especialistas em privacidade e investir em auditorias de conformidade.

Esses custos, embora mais onerosos para pequenas e médias empresas, não podem ser interpretados apenas como entraves econômicos. Como observa Pimenta (2022), a adequação à LGPD deve ser compreendida também como oportunidade estratégica: empresas que demonstram transparência no tratamento de dados conquistam vantagem competitiva, reforçando a confiança dos consumidores e a reputação da marca.

Um dos requisitos centrais da LGPD é a nomeação do encarregado pelo tratamento de dados pessoais (art. 41), popularmente denominado Data Protection Officer. Sua função é atuar como ponto de contato entre a empresa, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Segundo Doneda (2019), a figura do DPO representa uma inovação institucional relevante, pois insere no âmbito privado uma função de compliance jurídico que transcende a dimensão técnica da segurança da informação. No comércio eletrônico, o DPO assume papel central para assegurar que as práticas de marketing digital, análise de perfis de consumo e armazenamento de informações estejam em conformidade com a lei.

A LGPD estabelece, em seu art. 46, que os agentes de tratamento de dados devem adotar medidas técnicas e administrativas capazes de proteger os dados pessoais de acessos não autorizados, destruição, perda, alteração ou qualquer forma de tratamento inadequado. No contexto do e-commerce, isso significa a necessidade de políticas robustas de segurança da informação, como criptografia, autenticação multifatorial e monitoramento de acessos.

A segurança da informação, entretanto, não se reduz a aspectos técnicos. Como ressalta Bruce Schneier (2015), trata-se de uma prática organizacional contínua, que envolve treinamento de colaboradores, cultura de proteção de dados e auditorias regulares. Assim, o compliance com a LGPD no comércio eletrônico depende da conjugação de soluções tecnológicas e políticas de governança corporativa.

A LGPD prevê sanções administrativas relevantes em caso de descumprimento, que vão desde advertências até multas que podem atingir 2% do faturamento da empresa, limitadas a R\$ 50 milhões por infração (art. 52). Essas penalidades, aplicadas pela ANPD, têm caráter pedagógico e buscam induzir a adoção de práticas adequadas de proteção de dados.

Além das sanções administrativas, subsiste a responsabilidade civil da empresa pelos danos materiais e morais causados aos consumidores em razão de falhas no tratamento de dados. Como assinala Tartuce (2021), a responsabilidade civil por violação da LGPD deve ser compreendida em diálogo com o Código de Defesa do Consumidor, reforçando a tutela da parte hipossuficiente nas relações digitais.

4. PROTEÇÃO DOS DIREITOS DO CONSUMIDOR E CONFIANÇA NO AMBIENTE DIGITAL

A proteção de dados pessoais no comércio eletrônico relaciona-se diretamente ao direito à privacidade, consagrado no art. 5º, X, da Constituição Federal. Como observa Sarlet (2019), a privacidade integra o núcleo essencial da dignidade da pessoa humana e deve ser resguardada frente ao crescente poder econômico das empresas digitais.

No comércio digital, a privacidade do consumidor é elemento essencial para a formação de um ambiente de confiança. Empresas que violam esse direito, seja por práticas abusivas de coleta de dados, seja por incidentes de segurança, fragilizam não apenas sua reputação, mas o próprio desenvolvimento sustentável do mercado eletrônico.

O Código de Defesa do Consumidor (Lei nº 8.078/1990) estabelece, em seu art. 6º, III, o direito básico à informação adequada e clara. A LGPD reforça essa diretriz, exigindo que os consumidores sejam informados sobre quais dados estão sendo coletados, para quais finalidades e por quanto tempo serão armazenados.

Segundo Lemos (2020), a convergência entre a LGPD e o CDC fortalece o dever de informação como pilar das relações digitais, tornando-o um instrumento de empoderamento do consumidor. No comércio eletrônico, a clareza das políticas de privacidade e a acessibilidade dos canais de atendimento são determinantes para a efetividade desses direitos.

A LGPD confere ao consumidor uma série de instrumentos para o exercício de seus direitos, entre os quais se destacam o acesso facilitado às informações (art. 9º), o direito à revisão de decisões automatizadas (art. 20) e o direito à portabilidade de dados (art. 18, V). Esses instrumentos aproximam o consumidor do conceito de autodeterminação informativa, já reconhecido como direito fundamental em diversos países europeus (STERN, 2018).

Entretanto, como adverte Pimenta (2022), a efetividade desses instrumentos depende de mecanismos de fiscalização e de conscientização social. Ainda são comuns casos em que os consumidores desconhecem seus direitos ou enfrentam barreiras práticas para exercê-los no ambiente digital.

No cenário contemporâneo, a confiança tornou-se um ativo competitivo estratégico. Como observa Shoshana Zuboff (2019), em uma economia de vigilância, a proteção da privacidade pode funcionar como diferencial de mercado, atraindo consumidores mais conscientes e exigentes.

No Brasil, a implementação adequada da LGPD pode contribuir para a construção de um comércio digital mais ético, transparente e confiável. Empresas que incorporam a proteção de dados em sua cultura organizacional não apenas cumprem a legislação, mas também fortalecem sua posição no mercado, consolidando relações de longo prazo com seus consumidores.

5. EXPERIÊNCIA INTERNACIONAL E COMPARAÇÃO COM O BRASIL

A LGPD inspirou-se diretamente no Regulamento Geral de Proteção de Dados da União Europeia (GDPR – General Data Protection Regulation), em vigor desde 2018. O GDPR estabeleceu padrões globais para a proteção de dados pessoais, impondo às empresas europeias e estrangeiras que atuam no mercado europeu exigências rigorosas de transparência, consentimento e segurança (KUNER, 2020).

No contexto do comércio digital, o GDPR trouxe inovações como o direito à portabilidade dos dados (art. 20) e o direito à explicação em decisões automatizadas (art. 22). Essas disposições influenciaram diretamente a redação da LGPD, embora no Brasil a previsão do direito à revisão de decisões automatizadas (art. 20) ainda careça de regulamentação detalhada por parte da ANPD.

Diferentemente da União Europeia, os Estados Unidos não possuem uma lei federal unificada de proteção de dados pessoais. O modelo norte-americano é fragmentado, com legislações setoriais como a California Consumer Privacy Act (CCPA), que confere aos consumidores direitos semelhantes aos do GDPR, mas restritos ao território da Califórnia (SCHWARTZ; SOLOVE, 2011).

Na Ásia, países como Japão e Coreia do Sul adotaram legislações robustas de proteção de dados, buscando alinhar-se aos padrões internacionais da União Europeia. A Act on the Protection of Personal Information (APPI), no Japão, tem sido reconhecida pela Comissão Europeia como equivalente ao GDPR, permitindo a transferência internacional de dados entre os blocos (GREENLEAF, 2018).

A LGPD converge com o GDPR ao adotar princípios como finalidade, necessidade e transparência, além de reconhecer direitos como o acesso, a correção e a exclusão de dados. Contudo, diverge na estrutura institucional: enquanto o GDPR é supervisionado por autoridades independentes nos Estados-membros, a ANPD brasileira foi criada inicialmente como órgão vinculado ao Poder Executivo, o que gerou críticas sobre sua autonomia (DONEDA, 2020).

Outro ponto de divergência refere-se às sanções. O GDPR prevê multas que podem alcançar 4% do faturamento global da empresa, enquanto a LGPD limita as penalidades a 2%

do faturamento nacional, com teto de R\$ 50 milhões por infração. Essa diferença reduz o potencial dissuasório da lei brasileira em relação a grandes empresas multinacionais.

As experiências internacionais demonstram que a efetividade das leis de proteção de dados depende não apenas de normas bem elaboradas, mas de uma estrutura institucional sólida e de fiscalização eficiente. O Brasil pode se inspirar na independência das autoridades europeias e no dinamismo regulatório da CCPA para fortalecer a atuação da ANPD, garantindo maior credibilidade ao sistema de proteção de dados e ampliando a confiança dos consumidores no comércio digital.

6. PERSPECTIVAS FUTURAS E RECOMENDAÇÕES

A Autoridade Nacional de Proteção de Dados ocupa papel central na consolidação da cultura de privacidade no Brasil. Seu fortalecimento institucional, com autonomia administrativa e orçamentária, é essencial para que possa fiscalizar grandes corporações digitais e orientar pequenas e médias empresas (ANPD, 2021).

A plena efetividade da LGPD exige não apenas fiscalização rigorosa, mas também a conscientização da sociedade sobre os direitos previstos na lei. Como observa Lemos (2020), muitos consumidores ainda desconhecem a possibilidade de solicitar acesso, correção ou exclusão de seus dados. Campanhas educativas são fundamentais para democratizar o exercício da autodeterminação informativa.

A expansão de tecnologias emergentes como inteligência artificial, big data e blockchain traz novos desafios para a aplicação da LGPD. Como destaca Zuboff (2019), a chamada “economia de vigilância” depende da coleta massiva de dados, exigindo regulações ainda mais sofisticadas. No comércio eletrônico, algoritmos de recomendação e sistemas de precificação dinâmica devem ser compatibilizados com os direitos dos consumidores, evitando discriminações ocultas ou abusos informacionais.

A partir da análise realizada, é possível propor que as empresas invistam em programas de compliance em proteção de dados, capacitação de colaboradores e políticas de governança digital.

Os consumidores, por sua vez, devem exercer ativamente seus direitos de acesso, correção e eliminação de dados, exigindo transparência nas relações digitais.

Ao Poder público cabe fortalecer a ANPD, harmonizar a LGPD com legislações internacionais e adotar políticas públicas de incentivo à cultura de privacidade.

A conjugação desses esforços é indispensável para que o Brasil consolide um ambiente digital seguro, ético e competitivo, capaz de equilibrar inovação tecnológica, desenvolvimento econômico e proteção de direitos fundamentais.

CONCLUSÃO

A análise empreendida ao longo deste artigo permitiu constatar que a Lei Geral de Proteção de Dados Pessoais transformou profundamente o comércio digital brasileiro, estabelecendo um novo paradigma de equilíbrio entre inovação tecnológica, desenvolvimento econômico e proteção de direitos fundamentais.

No âmbito empresarial, verificou-se que a LGPD impôs desafios significativos de conformidade e custos de adequação, mas também abriu oportunidades para a construção de relações comerciais mais transparentes e baseadas na confiança. Para os consumidores, a lei representou um avanço na tutela da privacidade e no reconhecimento da autodeterminação informativa como direito fundamental, fortalecendo a posição do indivíduo diante do poder econômico das plataformas digitais.

Do ponto de vista institucional, destacou-se o papel essencial da ANPD na fiscalização e na educação sobre a proteção de dados. Todavia, a efetividade da lei depende de seu fortalecimento estrutural e da ampliação de sua autonomia, de modo a garantir maior credibilidade e alcance regulatório.

As experiências internacionais demonstraram que o Brasil ainda precisa avançar em pontos cruciais, como a autonomia da autoridade reguladora e a eficácia das sanções aplicáveis a grandes corporações digitais. Ademais, os novos desafios impostos por tecnologias emergentes, como inteligência artificial e big data, exigem atualização constante da regulação, sob pena de enfraquecer a proteção de direitos conquistada.

Conclui-se que a LGPD representa não apenas um marco jurídico, mas também uma oportunidade histórica de consolidar no Brasil uma cultura de proteção de dados e de confiança digital. Para tanto, será necessário o engajamento conjunto de empresas, consumidores e poder público, na busca por um comércio eletrônico mais ético, seguro e alinhado aos padrões internacionais de governança digital.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo para Adequação à LGPD. Brasília, 2021. Disponível em: <https://www.gov.br/anpd>. Acesso em: 5 jun. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br>. Acesso em: 5 jun. 2024.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. *Altera a LGPD para criar a Autoridade Nacional de Proteção de Dados (ANPD)*. Diário Oficial da União, Brasília, 9 jul. 2019.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 3. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. *A proteção de dados pessoais como direito fundamental*. Revista de Direito Administrativo, Rio de Janeiro, v. 280, n. 1, p. 259-278, 2020.

EBIT|NIELSEN. *Webshoppers 45ª edição*. São Paulo, 2022. Disponível em: <https://www.ebit.com.br>

LEMONS, Ronaldo. Privacidade e os Novos Desafios no Brasil. São Paulo: Companhia das Letras, 2020.

OLIVEIRA, Marina. Segurança da Informação e Compliance com a LGPD no Comércio Eletrônico. Revista de Direito Digital, São Paulo, v. 15, n. 3, p. 25-43, 2021.

PIMENTA, Fernanda. Impactos da LGPD no Mercado de E-commerce Brasileiro. Revista Brasileira de Direito do Consumidor, Brasília, v. 20, n. 2, p. 57-78, 2022.

SARLET, Ingo Wolfgang. Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988. 12. ed. Porto Alegre: Livraria do Advogado, 2019.

SCHWARTZ, Paul; SOLOVE, Daniel. The PII problem: Privacy and a new concept of personally identifiable information. *New York University Law Review*, v. 86, p. 1814-1894, 2011.

SCHNEIER, Bruce. Data and Goliath: The hidden battles to collect your data and control your world. New York: W. W. Norton, 2015.

STERN, Klaus. Das Staatsrecht der Bundesrepublik Deutschland. 3. ed. München: C. H. Beck, 2018.

TARTUCE, Flávio. Manual de direito civil. 11. ed. Rio de Janeiro: Forense, 2021.

UNIÃO EUROPEIA. *General Data Protection Regulation (GDPR)*. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Bruxelas, 2016.

ZUBOFF, Shoshana. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: PublicAffairs, 2019.