RESPONSABILIDADE CIVIL NO USO DE DADOS PARA FINS DE MARKETING: RISCOS E PREVENÇÃO A LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS

CIVIL LIABILITY IN THE USE OF DATA FOR MARKETING PURPOSES: RISKS AND PREVENTION IN LIGHT OF THE GENERAL DATA PROTECTION LAW

Emanuel Victor de Moura Oliveira Barros[1]
Gabriel Sperandio Milan[2]
Viviane Aprigio Prado e Silva[3]

V. 6 N. 2
2025

ISSN: 2177-1472

RESUMO

Este artigo aborda a responsabilidade civil no uso de dados pessoais para fins de marketing, com foco na Lei Geral de Proteção de Dados (LGPD). A questão de pesquisa que norteou o estudo é a seguinte: quais são os principais riscos e implicações jurídicas da responsabilidade civil no uso de dados pessoais para fins de marketing, e quais medidas preventivas podem ser adotadas para garantir a conformidade com a LGPD? O objetivo geral foi o de analisar a responsabilidade civil decorrente do uso de dados pessoais para fins de marketing, identificando os principais riscos e as medidas preventivas à luz da LGPD, com o intuito de compreender como as empresas podem adequar suas práticas e evitar sanções jurídicas. O método de pesquisa utilizado consistiu em uma revisão da literatura, que incluiu a análise de artigos científicos, livros e jurisprudências sobre a responsabilidade civil no uso de dados para fins de marketing. Este trabalho examina os riscos jurídicos relacionados ao tratamento inadequado de dados, tais como vazamentos e uso não autorizado de dados, e as implicações da responsabilidade objetiva e subjetiva das empresas. A pesquisa também analisa a necessidade de adoção de medidas preventivas, como políticas de privacidade transparentes, consentimento explícito dos titulares e segurança da informação, para garantir a conformidade com a LGPD e minimizar os riscos legais. Conclui-se que a responsabilidade civil, quando bem gerida, pode fortalecer a confiança dos consumidores e evitar sanções regulatórias para as empresas.

Palavras-chave: responsabilidade civil; proteção de dados pessoais; Lei Geral de Proteção de Dados (LGPD).

RECEBIDO: 10/03/2025
APROVADO: 20/04/2025

1 Mestre em Gestão e Négocios pela Universidade do Vale do Rio dos Sinos (Unisinos). Bolsista pesquisador da Fundação de Amparo e Pesquisa de Goiás (Fapeg) na Universidade de Rio Verde (UniRV). E-mail: emanuel@unirv.edu.br.
2 Pós-doutor em Administração e Doutor em Engenharia de Produção pela Universidade Federal do Rio Grande do Sul (UFGRS). Professor e pesquisador na Unisinos. E-mail: gsmilan@unisinos.br.
3 Doutora em Direito pela Unisinos. Professora titular da UniRV. E-mail: viviane@unirv.edu.br.

ABSTRACT

This article addresses civil liability in the use of personal data for marketing purposes, with a focus on the General Data Protection Law (LGPD). The research question that guided the study is as follows: What are the main risks and legal implications of civil liability in the use of personal data for marketing purposes, and what preventive measures can be adopted to ensure compliance with the LGPD? The general objective was to analyze the civil liability arising from the use of personal data for marketing purposes, identifying the main risks and preventive measures in light of the LGPD, with the aim of understanding how companies can adjust their practices and avoid legal sanctions. The research method used consisted of a literature review, which included the analysis of scientific articles, books, and case law on civil liability in the use of data for marketing purposes. This study examines the legal risks associated with improper data processing, such as data breaches and unauthorized use, as well as the implications of both objective and subjective liability for companies. The research also analyzes the need to adopt preventive measures, such as transparent privacy policies, explicit consent from data subjects, and information security, to ensure compliance with the LGPD and minimize legal risks. It is concluded that well-managed civil liability can strengthen consumer trust and prevent regulatory sanctions for companies.

Keywords: civil liability; personal data protection; General Data Protection Law (GDPL).

1 INTRODUÇÃO

A utilização de dados pessoais para fins de marketing envolve riscos no âmbito da responsabilidade civil, especialmente sob a égide da Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018). A legislação estabelece que os agentes de tratamento de dados devem adotar medidas de segurança para proteger as informações contra acessos não autorizados e eventos acidentais ou ilícitos, como destruição, perda, alteração, comunicação ou difusão indevida. O descumprimento dessas medidas pode resultar na responsabilização civil dos agentes, sobretudo quando há violação dos direitos dos titulares e falta de transparência nas práticas de tratamento e uso de dados (Santos; Pinheiro; Barbosa, 2022).

A responsabilidade civil dos agentes de tratamento pode ser classificada como objetiva ou subjetiva, a depender das circunstâncias específicas de cada caso. No entanto, a LGPD não define de maneira clara qual modalidade de responsabilidade deve ser aplicada a entes públicos e privados no tratamento de dados pessoais, o que gera debates doutrinários sobre a aplicação da responsabilidade objetiva ou subjetiva. Essa indefinição pode resultar em insegurança jurídica para as organizações que utilizam dados pessoais em suas estratégias e ações de marketing, aumentando os riscos de litígios e sanções regulatórias (Divino; Lima, 2021).

Para mitigar os riscos de responsabilização civil, as empresas devem adotar medidas preventivas robustas. Entre elas, destacam-se a implementação de políticas de privacidade transparentes, a obtenção de consentimento explícito dos titulares para o uso de seus dados em campanhas ou ações específicas de marketing e a garantia de que os dados e as informações coletadas sejam utilizados exclusivamente para os fins informados. Além disso, o investimento em segurança da informação é essencial para evitar violações e incidentes de proteção de dados. A adoção dessas práticas não apenas assegura a conformidade com a LGPD, mas também fortalece a confiança dos consumidores na marca (Santos; Pinheiro; Barbosa, 2022).

Em um cenário no qual os dados pessoais são frequentemente utilizados para segmentação de público, publicidade direcionada e outras estratégias comerciais, a proteção da privacidade dos indivíduos e a transparência nas práticas de tratamento de dados se tornam aspectos centrais. Nesse contexto, surgem dúvidas sobre os riscos legais que as empresas podem enfrentar em caso de descumprimento da LGPD, incluindo a responsabilidade civil dos agentes de tratamento. Além disso, a incerteza quanto à aplicação de responsabilidade objetiva ou subjetiva dificulta a previsão de consequências jurídicas, aumentando a vulnerabilidade das organizações a litígios e sanções. Assim sendo, a questão central desta pesquisa é: quais são os principais riscos e implicações jurídicas da responsabilidade civil no uso de dados pessoais para fins de marketing, e quais medidas preventivas podem ser adotadas para garantir a conformidade com a LGPD?

Diante disso, este estudo tem como objetivo geral analisar a responsabilidade civil decorrente do uso de dados pessoais para fins de marketing, identificando os principais riscos e medidas preventivas à luz da LGPD, a fim de compreender como as empresas podem adequar suas práticas e evitar sanções jurídicas.

Para atingir esse objetivo, foi realizada uma revisão bibliográfica abrangente, incluindo a análise de artigos científicos, livros e jurisprudências sobre a responsabilidade civil no uso de dados para fins de marketing. Essa abordagem permitiu a identificação dos principais riscos envolvidos, bem como das medidas preventivas recomendadas pela doutrina e aplicadas nos tribunais. A revisão considerou a LGPD como principal marco regulatório, a fim de compreender seu impacto na responsabilização das empresas e na proteção dos direitos dos titulares de dados.

2 FUNDAMENTOS DA RESPONSABILIDADE CIVIL

A responsabilidade civil é um instituto jurídico que impõe a obrigação de reparar danos causados a terceiros por meio de ações ou omissões, sejam elas voluntárias ou decorrentes de negligência. Seu fundamento principal está no princípio *neminem laedere*, que estabelece que ninguém deve causar dano a outrem. No direito brasileiro, a responsabilidade civil pode ser contratual, quando resulta do descumprimento de obrigações previstas em um contrato, ou extracontratual, quando decorre da violação de deveres gerais de conduta, conforme disposto no artigo 186 do Código Civil. O objetivo central é assegurar que a vítima seja devidamente indenizada, restabelecendo, na medida do possível e quando possível, a situação anterior ao dano (Santos; Silva, 2020).

Entre os princípios fundamentais da responsabilidade civil, destaca-se o princípio da reparação integral, que visa compensar todos os prejuízos sofridos pela vítima, abrangendo danos materiais e morais. Outro princípio essencial é o da causalidade, que exige a existência de um nexo causal entre a conduta do agente e o dano experimentado pela vítima. É necessário, então, que o prejuízo seja uma consequência direta da ação ou omissão do responsável (Pereira; Silva, 2018).

O princípio da culpa é outro pilar da responsabilidade civil, especialmente na modalidade subjetiva, na qual é imprescindível comprovar a culpa ou dolo do agente para que haja a obrigação de indenizar. Contudo, existem situações em que a responsabilidade independe de culpa, fundamentando-se no princípio do risco, que embasa a responsabilidade objetiva. Essa modalidade é aplicável em atividades que, por sua natureza, oferecem riscos elevados ou em casos específicos previstos em lei, como no Código de Defesa do Consumidor. Nessas hipóteses, basta demonstrar o dano e o nexo causal para que surja o dever de indenizar, dispensando-se a prova de culpa (Brasil, 1990; Divino; Lima, 2021).

Nesse sentido, Schreiber (2021, p. 328) elucida:

> Pode-se afirmar, em outras palavras, que não há uma resposta unívoca a indagação sobre a espécie de responsabilidade civil que vigora no âmbito da LGPD. Tal como ocorre no Código de Defesa do Consumidor e, também, no Código Civil, ambos os regimes de responsabilidade civil – subjetivo e objetivo – convivem na legislação de proteção de dados pessoais. Dentre as hipóteses de responsabilidade subjetiva, o legislador destacou, por meio do parágrafo único do art. 44, a hipótese de ausência de adoção das medidas protetivas indicadas no art. 46, mas isso não afasta outros casos de responsabilidade civil objetiva, decorrentes do tratamento de dados pessoais que não fornaça a segurança que pode esperar o titular dos referidos dados, à luz das circunstâncias indicadas nos incisos do art. 44 da LGPD. (…) Em suma, apesar da redação confusa, pode-se concluir que convivem na LGPD dois regimes distintos de responsabilidade civil: a responsabilidade subjetiva e responsabilidade objetiva. É, de resto, o que ocorre no Código Civil, no qual convivem as cláusulas gerais de responsabilidade subjetiva (art. 186 c/c art. 927, *caput*) e objetiva (art. 927, parágrafo único), bem como no Código de Defesa do Consumidor (responsabilidade objetiva nos arts. 12, *caput*, e 14, *caput*, por exemplo; e responsabilidade subjetiva no art. 14, § 4º), sendo certo que esses dois diplomas legislativos parecem ter guiado, acertadamente, as opções do legislador especial na disciplina de dados pessoais.

O princípio da equidade também desempenha um papel relevante na responsabilidade civil, permitindo que o julgador ajuste a indenização conforme as particularidades de cada caso concreto. Esse princípio possibilita a avaliação da extensão do dano e da capacidade econômica do responsável, visando fixar uma compensação justa e proporcional, evitando decisões que possam ser excessivamente onerosas ou insuficientes para reparar o prejuízo sofrido pela vítima (Teixeira, 2016).

Por fim, a responsabilidade civil exerce uma função social significativa ao incentivar comportamentos mais cautelosos e desencorajar condutas lesivas. Ao impor o dever de reparar danos, o ordenamento jurídico protege não apenas os interesses individuais, mas também os coletivos, promovendo a segurança jurídica e a justiça social. Por conseguinte, os princípios que norteiam a responsabilidade civil asseguram a reparação adequada das vítimas e atuam como mecanismos de prevenção a novos danos, contribuindo para a harmonia e o equilíbrio nas relações sociais (Cirne; Silva, 2021).

A responsabilidade civil está regulamentada na Seção III do Capítulo VI da LGPD, intitulada "Da Responsabilidade e do Ressarcimento de Danos". No entanto, tais normas não serão aplicáveis em todos os casos envolvendo responsabilidade civil, podendo, a depender da relação jurídica, ceder espaço a normas específicas, como o Código de Defesa do Consumidor, o que, inclusive, é expressamente reconhecido pela LGPD em seu art. 45: "Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente".

Perfunctoriamente, a responsabilidade surge do exercício da atividade de proteção de dados que viole a LGPD, embora a responsabilidade civil não decorra apenas da violação a referida legislação. Analisando sistematicamente o art. 42, caput, em consonância com o art. 44, parágrafo único, que prevê que o controlador ou o operador responde pelos danos decorrentes da violação da segurança de dados que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano. Por sua vez, o art. 46 estabelece que os agentes de tratamento deverão adotar medidas de segurança, técnicas e administrativas, visando à proteção de dados pessoais. Com efeito, é possível identificar duas situações de responsabilidade civil na LGPD: (i) violação de normas jurídicas, do microssistema de proteção de dados; e (ii) violação de normas técnicas, voltadas à segurança e proteção de dados pessoais. Evidentemente, somente será caracterizada a responsabilidade civil se a violação de norma jurídica ou técnica ocasionar dano material ou moral a um titular ou a uma coletividade.

A responsabilidade civil na proteção de dados pessoais também se entrelaça com o uso de dados para fins de marketing, um dos temas mais discutidos à luz da LGPD. A legislação brasileira impõe que o tratamento de dados pessoais, incluindo aqueles que são utilizados para estratégias e ações de marketing, só seja realizado mediante o consentimento expresso do titular ou em outras bases legais previstas, como a execução de contrato ou o legítimo interesse.

Nesse sentido, as empresas precisam garantir que os dados pessoais dos consumidores sejam coletados, armazenados e processados de maneira transparente, com objetivos claros e devidamente informados ao titular, sob pena de responsabilidade civil. A utilização de dados pessoais para fins de marketing deve estar em conformidade com os princípios da LGPD, respeitando a privacidade dos indivíduos e proporcionando um ambiente de confiança nas relações comerciais, o que configura um desafio significativo para as organizações que buscam equilibrar inovação e respeito à proteção de dados (Costa, 2021).

3 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E O USO DE DADOS PARA MARKETING

A LGPD, instituída pela Lei n.º 13.709/2018, estabelece os fundamentos e objetivos para o tratamento de dados pessoais no Brasil. Conforme o artigo 1º da LGPD, sua finalidade é proteger os direitos fundamentais de liberdade e privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural (Silva; Almeida, 2019) (Silva, 2019).

A LGPD define o titular[4] como protagonista das relações jurídicas que envolvam o tratamento de dados, não só porque regula a proteção de dados pessoais, mas, principalmente, elege como fundamento em seu art. 2º, inciso II, a "autodeterminação informativa", que consiste no direito de escolher quais dados serão usados, bem como os limites e o prazo dessa utilização. Prevista no Capítulo III da LGPD, especialmente no artigo 18, a autodeterminação é garantida pela previsão de vários direitos, tais como: o de informação, de acesso, de correção, de portabilidade, de eliminação, dentre outros.

Entre os princípios que norteiam o tratamento de dados pessoais, destacam-se a finalidade, a necessidade, a transparência e a segurança. Tais princípios asseguram que os dados sejam coletados e utilizados de forma adequada, limitada ao necessário para atingir os objetivos específicos informados ao titular, garantindo a transparência nas operações e a proteção contra acessos não autorizados (Ferreira, 2019).

A LGPD também define as bases legais para o tratamento de dados, incluindo o consentimento do titular, o cumprimento de obrigação legal ou regulatória, a execução de políticas públicas, a realização de estudos por órgãos de pesquisa, a execução de contrato, o exercício regular de direitos, a proteção da vida ou da saúde, o interesse legítimo do controlador ou de terceiro e a proteção de crédito. Essas bases estabelecem os fundamentos legais que autorizam o uso de dados pessoais em diferentes contextos (Santos; Pinheiro; Barbosa, 2022).

A lei assegura aos titulares de dados pessoais uma série de direitos, como a confirmação da existência de tratamento, o acesso, a correção de dados incompletos ou desatualizados, a anonimização, o bloqueio ou a eliminação de dados desnecessários ou excessivos, a portabilidade dos dados a outro fornecedor, a eliminação de dados tratados com consentimento, a informação sobre compartilhamento de dados e a revogação do consentimento. Esses direitos fortalecem o controle do indivíduo sobre suas informações pessoais (Costa, 2021).

Para garantir o cumprimento da LGPD, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), responsável pela fiscalização e aplicação de sanções administrativas em casos de descumprimento (Brasil, 2019). A ANPD também orienta organizações sobre as melhores práticas de proteção de dados, promovendo a cultura de privacidade e de segurança da informação no país (Almeida, 2021).

No contexto do marketing, a LGPD estabelece que o tratamento de dados pessoais deve estar amparado por bases legais específicas. Uma dessas bases é o consentimento explícito do titular, que deve ser

4 "Art. 5º: V – titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (Brasil, 2018).

obtido de forma livre, informada e inequívoca. Nesse caso, os indivíduos devem ser plenamente informados sobre as finalidades específicas para as quais seus dados serão utilizados, garantindo transparência e controle sobre suas informações pessoais. A revogação desse consentimento deve ser facilitada, permitindo que o titular possa retomar o controle dos dados a qualquer momento (Ferreira, 2019).

Outra base legal aplicável no marketing é o interesse legítimo do controlador. Desse modo, a empresa pode processar dados pessoais sem o consentimento do titular, desde que exista um interesse legítimo que justifique essa ação, como a personalização de ofertas ou a melhoria dos serviços prestados. Contudo, é essencial que o controlador realize uma avaliação criteriosa para assegurar que seus interesses não se sobreponham aos direitos e às liberdades fundamentais do titular, equilibrando os benefícios da empresa com a proteção dos dados pessoais (Santos; Pinheiro; Barbosa, 2022).

O cumprimento de obrigação legal também constitui uma base legal para o tratamento de dados no marketing. Por exemplo, empresas podem ser obrigadas a coletar e processar dados pessoais para atender a exigências fiscais ou regulatórias, como o envio de informações comerciais a clientes. Nessas situações, o tratamento é necessário para o cumprimento de obrigações legais e não depende do consentimento do titular (Almeida, 2021).

A execução de contrato é outra base que se aplica ao marketing, especialmente quando o tratamento de dados é necessário para a realização de um contrato entre a empresa e o cliente. Por exemplo, ao adquirir um serviço de assinatura, os dados do cliente são utilizados para fornecer o serviço contratado, realizar cobranças e comunicar promoções ou atualizações relacionadas ao contrato. Nessas circunstâncias, o tratamento de dados é essencial para a execução do acordo estabelecido (Costa, 2021).

Por fim, a proteção da vida ou da saúde pode justificar o tratamento de dados pessoais no marketing, especialmente em setores como o de saúde ou seguros. Nessas áreas, o uso de dados é necessário para garantir a segurança do consumidor, oferecer serviços adequados às suas necessidades de saúde ou cumprir obrigações legais relacionadas à proteção da vida e da saúde. É fundamental que o tratamento de dados nessas situações seja realizado com respeito aos direitos dos titulares e em conformidade com a LGPD (Pereira, 2021).

A LGPD garante uma série de direitos aos titulares de dados, os quais visam proporcionar maior controle sobre suas informações pessoais. Entre os principais direitos, destaca-se o direito de acesso, que permite ao titular saber quais dados estão sendo tratados pela empresa e para quais finalidades. Além disso, o titular tem o direito de corrigir dados incompletos, errados ou desatualizados, garantindo que suas informações sejam sempre precisas. Outro direito importante é o direito à eliminação de dados, o que significa que, em determinadas situações, o titular pode solicitar que seus dados sejam apagados quando não houver mais necessidade do tratamento, especialmente quando o consentimento for revogado (Marteleto; Tomaél, 2001).

Além dos direitos dos titulares, as empresas têm deveres significativos para garantir a conformidade com a LGPD. Elas devem adotar medidas para assegurar a segurança dos dados pessoais, implementando práticas e tecnologias que protejam as informações contra vazamentos ou acessos não autorizados. A transparência é outro dever essencial: as empresas devem informar claramente aos titulares sobre como seus dados serão coletados, utilizados e compartilhados, fornecendo informações acessíveis e compreensíveis. As

empresas também são obrigadas a respeitar os direitos dos titulares, garantindo que estes possam exercer suas opções sobre os dados pessoais de maneira simples e eficaz, como o direito de revogar o consentimento ou solicitar a exclusão de informações (Ferreira, 2019).

Em acréscimo, a LGPD impõe à empresa a responsabilidade de realizar a gestão de riscos associados ao tratamento de dados pessoais. Isso envolve a realização de avaliações de impacto à proteção de dados, especialmente quando o tratamento pode representar alto risco aos direitos e liberdades dos indivíduos. As empresas também devem nomear um encarregado de dados, que é o profissional responsável por supervisionar as práticas de privacidade e proteção de dados na organização, garantindo que todas as operações de tratamento estejam de acordo com a legislação. A obrigação de notificar incidentes de segurança que envolvem dados pessoais também é um dever da empresa, sendo necessário comunicar à ANPD e aos titulares quando ocorrer um vazamento de dados que possa acarretar riscos significativos (Costa; Souza, 2021).

4 RISCOS NO USO INDEVIDO DE DADOS PARA FINS DE MARKETING

A coleta e o tratamento indevido de dados pessoais representam sérios desafios no cenário atual, especialmente com a crescente digitalização das informações. A LGPD, sancionada em 2018 e em vigor desde 2020, estabelece diretrizes rigorosas para o tratamento de dados pessoais no Brasil, visando proteger a privacidade e a dignidade dos indivíduos (Silveira, 2021).

A LGPD introduz princípios fundamentais, como finalidade, necessidade, transparência e segurança, que devem ser observados por empresas, organizações e entidades públicas e privadas ao lidarem com dados pessoais. Uma das inovações mais significativas da lei é a exigência de consentimento explícito do titular para o tratamento de seus dados, garantindo maior controle e transparência sobre como suas informações são utilizadas (Moraes, 2020).

Entretanto, a implementação efetiva da LGPD enfrenta desafios, sobretudo no que se refere à adaptação de repositórios institucionais. Estudos apontam que muitas instituições precisam realizar ajustes importantes em seus processos e fluxos de trabalho para atender às exigências da lei, incluindo a revisão de documentos institucionais, a capacitação de pessoal e a adoção de ações de transparência. Essas adaptações são essenciais para garantir a conformidade com a legislação e evitar sanções administrativas (Barros; Silva; Almeida, 2020).

Além disso, a proteção de dados pessoais é intrinsecamente ligada à privacidade, um direito fundamental que requer equilíbrio entre a transparência das informações públicas e a confidencialidade dos dados pessoais. Mesmo quando a coleta e o uso de informações pessoais são autorizados por leis específicas, como as sanitárias, essas informações mantêm sua natureza confidencial, e seu acesso deve respeitar o consentimento do indivíduo, salvo exceções previstas em lei (Costa; Souza, 2021).

A atuação de profissionais da informação, como arquivistas, é crucial na implementação da LGPD. Estudos revelam que a participação ativa desses profissionais no planejamento e na discussão sobre a

proteção de dados pessoais nas universidades federais do Brasil é limitada. Isso destaca a necessidade de mais envolvimento e capacitação desses profissionais para assegurar que as instituições atendam às exigências legais e promovam a proteção adequada dos dados pessoais (Lima; Pereira, 2021).

Em síntese, a coleta e o tratamento indevido de dados pessoais constituem questões complexas que exigem a colaboração de diversos setores da sociedade. A conformidade com a LGPD é fundamental para a construção de uma cultura de respeito à privacidade e à proteção de dados, garantindo que os dados e as informações pessoais sejam tratados de forma ética, transparente e segura (Silveira, 2021).

O compartilhamento não autorizado de dados pessoais é uma violação grave da privacidade e segurança dos indivíduos. Esse tipo de prática ocorre quando dados pessoais são repassados a terceiros sem o devido consentimento ou fora das condições previamente acordadas pelo titular. Segundo especialistas, o compartilhamento indevido pode ocorrer tanto de forma intencional quanto acidental, sendo, muitas vezes, motivado pela falta de políticas claras de governança de dados dentro das organizações. A vulnerabilidade gerada por esses compartilhamentos compromete não apenas os direitos do titular, mas também a confiança do público nas instituições responsáveis pelo tratamento dos dados (Costa; Souza, 2021).

Cabe salientar que os vazamentos de dados pessoais representam uma das formas mais graves de comprometimento da segurança da informação. Vazamentos podem ocorrer em razão de falhas técnicas, como brechas de segurança em sistemas de armazenamento, ou por causa da negligência no manuseio de informações sensíveis. Esses incidentes, quando acontecem, expõem informações privadas dos indivíduos, como números de documentos, endereços e dados bancários, que podem ser usadas de forma maliciosa para causar danos aos afetados, como fraudes financeiras e roubo de identidade. De acordo com pesquisadores, a prevenção de vazamentos exige que as empresas adotem medidas rigorosas de segurança cibernética e treinem seus colaboradores para a gestão adequada de dados pessoais (Pereira, 2021).

Em relação aos vazamentos, a LGPD determina que as organizações devem notificar a ANPD e os titulares afetados caso ocorra um incidente de segurança que possa comprometer os dados pessoais. Tal obrigação de transparência visa mitigar os danos causados, permitindo que as vítimas do vazamento tomem as providências necessárias para se protegerem. Contudo, estudos indicam que muitas empresas ainda falham em cumprir essa obrigação, o que reforça a importância de uma fiscalização mais eficiente e de uma conscientização maior sobre os riscos associados ao tratamento indevido de dados (Lima; Pereira, 2021).

O compartilhamento não autorizado e os vazamentos de dados têm consequências significativas para a reputação das empresas e organizações envolvidas, além de resultar em sanções legais severas, como multas e ações judiciais. A conformidade com a LGPD é crucial para evitar esses riscos, pois a lei prevê penalidades específicas para casos de tratamento irregular de dados pessoais. A implementação de medidas eficazes de segurança da informação, a criação de políticas de privacidade claras e a promoção de uma cultura organizacional centrada na proteção de dados são fundamentais para garantir a integridade das informações pessoais e a confiança dos indivíduos (Silva; Almeida, 2019).

A LGPD estabelece um conjunto de penalidades e sanções para as organizações que descumprirem suas normas, com o objetivo de garantir a efetividade da proteção de dados pessoais e incentivar as empresas a adotarem boas práticas de segurança da informação. As penalidades variam de acordo com a gravidade da infração e podem ser aplicadas pela ANPD, que tem o papel de fiscalizar e assegurar o cumprimento

da lei. As sanções estão divididas em advertências, multas e, em casos mais graves, a suspensão ou proibição da atividade de tratamento de dados pessoais (Divino; Lima, 2021).

As advertências são as sanções mais brandas, geralmente aplicadas nas primeiras infrações, especialmente quando a organização demonstra boa-fé e cooperação para corrigir a irregularidade. No entanto, quando a infração envolve a violação de direitos fundamentais dos titulares, como a falta de consentimento para o tratamento de dados pessoais, a multa pode ser aplicada. A multa pode variar entre 2% do faturamento da empresa, limitada a R$ 50 milhões por infração, dependendo da gravidade do descumprimento. Além disso, a ANPD pode aplicar uma multa diária, caso a organização não tome as medidas necessárias para corrigir a infração em tempo hábil (Santos; Silva, 2020).

Em situações mais graves, como o compartilhamento não autorizado de dados pessoais ou a omissão de informações relevantes ao titular dos dados, a ANPD pode decidir pela suspensão ou proibição do tratamento de dados pessoais. Essa medida visa impedir que a empresa continue a infringir os direitos dos indivíduos e obrigar a organização a adotar uma postura mais responsável e em conformidade com a LGPD. A suspensão das atividades de tratamento de dados pode ser temporária ou permanente, dependendo da situação e da capacidade da organização de corrigir os problemas identificados (Carvalho, 2022).

Além das sanções administrativas impostas pela ANPD, as empresas podem ser alvo de ações judiciais por parte dos titulares de dados pessoais afetados por infrações à LGPD. Isso pode resultar em indenizações por danos materiais e morais, uma vez que o titular dos dados pode ser prejudicado pela exposição indevida de suas informações pessoais. A legislação também prevê a responsabilização dos agentes de tratamento, como controladores e operadores, podendo ambos serem responsabilizados em conjunto ou separadamente, conforme a responsabilidade de cada parte na infração (Antos; Silva, 2012).

Em resumo, as penalidades e sanções previstas na LGPD são um mecanismo crucial para garantir a conformidade com a proteção de dados pessoais no Brasil. Elas visam não apenas punir as infrações, mas também incentivar as empresas a implementar práticas adequadas de governança de dados e a promover a cultura de respeito à privacidade e à proteção dos dados dos indivíduos (Antos; Silva, 2012).

5 PREVENÇÃO E BOAS PRÁTICAS NO TRATAMENTO DE DADOS PARA MARKETING

A proteção de dados pessoais é um elemento essencial para a manutenção da privacidade e da confiança dos consumidores no ambiente digital. A LGPD enfatiza a necessidade de transparência no armazenamento, tratamento e disponibilização de dados pessoais por empresas e entidades públicas, garantindo aos titulares informações claras sobre o uso de suas informações (Mendes, 2021).

O consentimento informado é fundamental nesse contexto. De acordo com a LGPD, o consentimento deve ser uma manifestação livre, informada e inequívoca do titular, autorizando o tratamento de

seus dados pessoais para finalidades específicas. Essa abordagem assegura que os indivíduos tenham controle sobre suas informações, promovendo um ambiente de respeito à privacidade (Silva, 2020).

A transparência nas estratégias e ações de marketing é crucial para a construção de confiança. Estudos indicam que a clareza sobre o uso de cookies e a percepção de riscos e benefícios influenciam diretamente a intenção de compra on-line dos consumidores. Práticas transparentes, tais como a obtenção de consentimento explícito para o uso de dados, reforçam a ética no marketing digital praticado pelas empresas (Ferreira, 2019).

Em síntese, a adoção de boas práticas no tratamento de dados pessoais para marketing, incluindo consentimento informado e transparência, é vital para a construção de um ambiente digital ético e seguro. Essas práticas não apenas cumprem as exigências legais, mas também fortalecem a confiança e as preferências do consumidor, contribuindo para a integridade das relações comerciais no meio digital (Almeida, 2021).

A implementação de políticas de segurança da informação é uma etapa fundamental na proteção dos dados pessoais e no cumprimento das normas estabelecidas pela LGPD. Essas políticas envolvem um conjunto de diretrizes, normas e práticas destinadas a proteger os dados contra acessos não autorizados, alterações, divulgação indevida ou qualquer outro tipo de violação. A segurança da informação não se limita apenas à proteção de dados sensíveis, mas também à integridade e à disponibilidade das informações dentro das organizações (Lima, 2020).

A gestão de riscos é um dos principais pilares das políticas de segurança da informação, pois permite identificar, avaliar e mitigar as ameaças que podem comprometer a proteção dos dados. A implementação de controles adequados – como é o caso da criptografia, da autenticação de múltiplos fatores, do monitoramento constante e das auditorias periódicas – fortalece a infraestrutura de segurança. A criação de uma cultura organizacional de segurança também é essencial, com treinamentos e conscientização contínuos para todos os colaboradores, garantindo que os procedimentos e as políticas de segurança sejam seguidos de maneira eficaz (Costa; Souza, 2021).

Outra medida importante é a revisão constante das políticas de segurança da informação, adaptando-as às novas ameaças e tecnologias que surgem. À medida que o ambiente digital se torna mais dinâmico, com o crescimento de tecnologias emergentes, como inteligência artificial e Internet das Coisas (IoT – Internet of Things), as organizações devem ser proativas em atualizar suas estratégias de proteção de dados. A governança de dados, alinhada com a política de segurança da informação, garante que as ações sejam coordenadas e que os dados sejam tratados de maneira ética e legal (Costa; Souza, 2021).

A transparência e o monitoramento também são aspectos essenciais da implementação de políticas de segurança da informação. As empresas devem garantir que suas práticas de segurança estejam claramente documentadas e sejam acessíveis para auditoria, além de serem transparentes com os consumidores sobre os processos de proteção de seus dados pessoais. Dessa forma, a implementação de políticas de segurança robustas não só protege os dados, mas também constrói a confiança entre as empresas e seus consumidores, contribuindo para um ambiente digital mais seguro e ético (Pereira, 2021).

A adoção de medidas eficazes para evitar litígios e responsabilizações é uma parte essencial da gestão de dados pessoais no contexto empresarial. As organizações precisam estar atentas à conformidade com as leis de proteção de dados, como a LGPD, para prevenir violações que possam resultar em litígios judiciais

ou sanções administrativas. Por isso, a implementação de políticas claras e a documentação adequada das práticas de coleta, tratamento e armazenamento de dados são fundamentais para mitigar riscos legais. Além disso, as empresas devem garantir que seus processos sejam auditáveis, possibilitando a verificação do cumprimento das normas de proteção de dados (Antos; Silva, 2012).

Uma das principais medidas para evitar litígios é garantir a transparência nas práticas de tratamento de dados. Isso inclui informar claramente aos titulares sobre a finalidade do uso dos dados, o período de retenção das informações e os direitos dos titulares, como a possibilidade de retificação ou exclusão de dados. Empresas que oferecem um processo claro de consentimento, no qual os titulares saibam como seus dados serão usados e tenham o direito de revogá-lo a qualquer tempo, têm menos chances de enfrentar disputas legais. A criação de canais de comunicação eficientes para que os consumidores possam expressar suas preocupações ou questionamentos também é crucial para evitar litígios (Divino; Lima, 2021).

Outra estratégia importante é a educação e o treinamento contínuo dos funcionários sobre as normas e práticas relacionadas à proteção de dados. A conscientização interna dentro das organizações pode prevenir comportamentos inadequados e garantir que todos os colaboradores compreendam a importância do cumprimento das leis e da ética no tratamento de dados. Consoante a isso, as empresas devem estabelecer procedimentos claros para a gestão de incidentes de segurança, com planos de resposta a vazamentos de dados ou outras falhas que possam comprometer a privacidade dos consumidores. Ao adotar medidas de segurança adequadas e agir rapidamente diante de incidentes, as empresas demonstram comprometimento com a proteção de dados e podem reduzir os riscos de ações judiciais ou multas (Santos; Silva, 2020).

Por fim, a mediação e a resolução de disputas de forma extrajudicial também têm se mostrado eficazes para evitar litígios prolongados. Muitos casos envolvendo proteção de dados podem ser resolvidos por meio de mecanismos de mediação ou arbitragem, que oferecem soluções rápidas e menos onerosas do que os processos judiciais. As organizações que promovem estas alternativas de resolução de conflitos criam um ambiente de maior confiança, tanto para os consumidores quanto para os parceiros de negócios. A adoção de boas práticas neste sentido pode evitar a escalada de disputas e minimizar os impactos financeiros e reputacionais decorrentes de litígios (Costa; Souza, 2021).

A implementação de políticas de segurança da informação, a transparência no tratamento de dados e a adoção de práticas adequadas para evitar litígios e responsabilizações são fundamentais para a proteção de dados pessoais no ambiente digital. Ao adotar essas medidas, as organizações não apenas cumprem as exigências legais, mas também fortalecem a confiança dos consumidores, preservam sua reputação e garantem a conformidade com as regulamentações vigentes. A construção de um ambiente ético e seguro, com foco na privacidade e no respeito aos direitos dos titulares, é essencial para o sucesso sustentável das empresas no mercado digital atual.

6 CONSIDERAÇÕES FINAIS

A crescente importância da proteção de dados no cenário do marketing digital se intensifica especialmente diante da implementação da LGPD. A LGPD representa um marco significativo na forma como as empresas devem tratar e utilizar os dados pessoais de seus consumidores, impondo um regime de transparência, segurança e consentimento. Em um ambiente digital no qual os dados são a moeda de troca mais valiosa, a conformidade com essa legislação não se limita a ser uma exigência legal, mas também se configura como uma estratégia essencial para fortalecer a confiança e construir um relacionamento duradouro com o consumidor, além de proteger a reputação das empresas e garantir a segurança dos dados e das informações tratadas e utilizadas.

A responsabilidade civil, tanto objetiva quanto subjetiva, é um pilar fundamental no contexto da proteção de dados. Empresas que falham na proteção adequada dos dados e das informações pessoais ou no cumprimento das obrigações previstas pela LGPD podem enfrentar não apenas sanções administrativas, como multas significativas, mas também consequências de caráter civil, a exemplo das ações judiciais por danos materiais e morais. A violação dos direitos dos titulares dos dados pode resultar em danos irreparáveis à imagem das organizações, prejudicando sua competitividade e relação com o público-alvo. A aplicação rigorosa da responsabilidade civil, portanto, atua como um mecanismo crucial de proteção para os consumidores e como um incentivo para que as empresas adotem práticas mais éticas, responsáveis e seguras.

Os riscos relacionados ao uso indevido de dados pessoais para fins de marketing, como a coleta e o tratamento não autorizados, o compartilhamento inadequado de informações e o vazamento de dados são questões que precisam ser tratadas com extrema seriedade. A LGPD oferece diversos instrumentos para mitigar tais riscos, incluindo a exigência de bases legais para o tratamento de dados, o direito ao consentimento explícito dos titulares e a imposição de sanções severas para o descumprimento das normas. Todavia, a legislação, por si só, não é suficiente para garantir uma proteção efetiva. A implementação de medidas práticas e operacionais, como a adoção de políticas de segurança da informação, a realização de treinamentos periódicos para os colaboradores e a revisão constante dos processos de tratamento de dados e de informações são essenciais para garantir que os riscos sejam minimizados.

A prevenção e a adoção de boas práticas são a chave para um tratamento de dados ético e seguro no marketing digital. A obtenção de consentimento informado e a garantia de transparência nas práticas de coleta e uso de dados são etapas fundamentais para assegurar a confiança do consumidor. Além disso, a implementação de sistemas e políticas de segurança robustas, que protejam as informações contra acessos não autorizados e vazamentos, é indispensável para evitar danos que possam comprometer a integridade das organizações. Medidas preventivas, como a revisão regular dos processos de tratamento de dados e a criação de canais de comunicação eficazes para o esclarecimento de dúvidas dos titulares, são fundamentais para evitar litígios e responsabilizações.

Por fim, os desafios em torno da proteção de dados, por exemplo, no marketing digital, são complexos e demandam uma abordagem sistêmica, que envolva não apenas a conformidade das práticas empresariais com a LGPD, mas também um compromisso contínuo das organizações com a ética, a

transparência, a segurança dos dados e a responsabilidade social. A conformidade com a legislação deve ser encarada como uma oportunidade para as empresas se diferenciarem positivamente no mercado, construindo um ambiente de confiança mútua com seus consumidores. Dessa forma, a proteção de dados contribui tanto para o cumprimento de normas legais quanto para a criação de uma cultura corporativa que valorize a privacidade e a segurança da informação, elementos essenciais para o sucesso e a sustentabilidade das empresas a longo prazo.

7 REFERÊNCIAS

ALMEIDA, J. F. O impacto da Lei Geral de Proteção de Dados nas estratégias de marketing digital. *Revista de Direito e Tecnologia*, [*s. l.*], v. 9, n. 2, p. 25-37, 2021.

ANTOS, L. M.; SILVA, R. A. Responsabilidade civil do Estado por omissão estatal: uma análise sob a ótica do Princípio Responsabilidade de Hans Jonas. *Revista Direito GV*, São Paulo, v. 8, n. 1, p. 109-130, 2012. Disponível em: https://www.scielo.br/j/rdgv/a/kSXsWrfjj3rkDFcTZ4hgZbj/?lang=pt. Acesso em: 12 maio 2025

BARROS, R.; SILVA, J.; ALMEIDA, M. A adaptação das instituições à Lei Geral de Proteção de Dados. *Em Questão*, [*s. l.*], v. 26, n. 2, p. 54-70, 2020. Disponível em: https://www.scielo.br/j/emquestao/a/w3xQNy4bnytwK6MxzgyKgsy/?lang=pt. Acesso em: 12 maio 2025.

BRASIL. *Lei n.º 8.078, de 11 de setembro de 1990*. Código de Defesa do Consumidor (CDC). Brasília, DF: Presidência da República,1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 12 maio 2025.

BRASIL. *Lei n.º 10.406, de 10 de janeiro de 2002.* Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 12 maio 2025.

BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 maio 2025.

BRASIL. *Lei n.º 13.853, de 08 de julho de 2019*. Cria a Autoridade Nacional de Proteção de Dado. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 12 maio 2025.

CARVALHO, J. A hiperconectividade e a transformação do espaço urbano. *Cidades Inteligentes e Sociedade Digital*, [*s. l.*], v. 7, n. 1, p. 30-50, 2022.

CIRNE, M. L.; SILVA, R. P. A Responsabilização Civil Solidária no Licenciamento Ambiental - PL 2159/2021. *Revista de Direito Ambiental*, [*s. l.*], v. 25, n. 3, p. 225-240, 2021. Disponível em: https://doi.org/10.18623/rvd.v21.2664. Acesso em: 12 maio 2025.

COSTA, A. L. Proteção de dados e responsabilidade civil: aspectos normativos e jurisprudenciais. *Revista Brasileira de Direito Digital*, [*s. l.*], v. 14, n. 3, p. 56-72, 2021.

COSTA, F.; SOUZA, P. A proteção da privacidade no Brasil: A LGPD e suas implicações. *Cadernos de Pesquisa*, [*s. l.*], v. 51, n. 1, p. 115-130, 2021.

DIVINO, F.; LIMA, R. Responsabilidade civil no tratamento de dados pessoais: desafios e perspectivas à luz da LGPD. *Revista Argumenta*, [*s. l.*], v. 15, n. 2, p. 45-62, 2021.

FERREIRA, M. L. Transparência e ética no marketing digital: A relação com a proteção de dados pessoais. *Revista Brasileira de Marketing Digital*, [*s. l.*], v. 8, n. 3, p. 45-59, 2019.

LIMA, F. T. A gestão de riscos e a segurança da informação nas organizações. *Revista Brasileira de Tecnologia e Segurança*, [*s. l.*], v. 16, n. 3, p. 34-47, 2020.

LIMA, T.; PEREIRA, L. Arquivistas e a implementação da LGPD nas universidades federais. *Em Questão*, [*s. l.*], v. 28, n. 1, p. 34-45, 2021.

MENDES, L. G. A proteção de dados pessoais e sua implementação no Brasil. *Revista Brasileira de Direito Digital*, [*s. l.*], v. 14, n. 2, p. 48-63, 2021.

MORAES, M. A Lei Geral de Proteção de Dados e suas implicações no Brasil. *Estudos Jurídicos*, [*s. l.*], v. 34, n. 3, p. 213-228, 2020.

PEREIRA, M. F. S. Responsabilidade civil no contexto da Lei Geral de Proteção de Dados: riscos e reparação. *Revista de Direito e Tecnologia*, São Paulo, v. 11, n. 2, p. 98-112, 2021.

PEREIRA, L. M.; SILVA, T. R. Responsabilidade Civil e Sustentabilidade: normatividade em prol do Meio Ambiente. *Revista de Direito Ambiental*, São Paulo, v. 23, n. 1, p. 123-145, 2018.

SANTOS, M.; PINHEIRO, T.; BARBOSA, L. Agentes de tratamento de dados e a responsabilidade civil na LGPD: uma análise crítica. *Revista de Direito e Tecnologia*, [*s. l.*], v. 10, n. 1, p. 89-105, 2022.

SANTOS, L. M.; SILVA, R. A. A responsabilidade civil na era digital: implicações da LGPD. *Revista de Direito da Informática*, São Paulo, v. 9, n. 1, p. 33-47, 2020.

SCHREIBER, A. Responsabilidade civil na lei geral de proteção de dados pessoais. *In*: MENDES, L. S. *et al.* (coord.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 324-328.

SILVA, R. A. O consentimento no contexto da Lei Geral de Proteção de Dados (LGPD): Perspectivas e desafios. *Revista de Estudos Jurídicos e Digitais*, [*s. l.*], v. 5, n. 1, p. 10-22, 2020.

MARTELETO, R. M.; TOMAÉL, M. I. Análise de redes sociais: aplicação nos estudos de transferência da informação. *Ciência da Informação*, Brasília, v. 30, n. 1, p. 71-81, jan./abr. 2001. Disponível em: https://repositorio.ufba.br/bitstream/ri/32179/1/analise-de-redes-sociais-repositorio.pdf. Acesso em: 12 maio 2025.

SILVEIRA, P. Desafios e perspectivas da LGPD no Brasil. *Em Questão*, [*s. l.*], v. 29, n. 2, p. 99-115, 2021.

TEIXEIRA, A. C. M. Descumprimento do art. 229 da Constituição Federal e a responsabilidade civil dos pais. *Revista de Investigações Constitucionais*, São Paulo, v. 3, n. 2, p. 115-130, 2016.