LUMEN ET VIRTUS
ISSN: 2177-2789

RESPONSABILIDADE CÍVIL DAS EMPRESAS E O TRATAMENTO DE DADOS PESSOAIS: PROTEÇÃO DE DADOS PESSOAIS E RESPONSABILIDADE CIVIL DOS FORNECEDORES DE SERVIÇOS OU PRODUTOS EM CASO DE VAZAMENTO DE DADOS DE CONSUMIDORES[1]

https://doi.org/10.56238/levv16n47-062

Data de submissão: 18/03/2025 **Data de publicação:** 18/04/2025

Yan Lucas Silva Corrêa
Acadêmico do curso de Bacharelado em Direito do Instituto de Ensino Superior do Sul do Maranhão – IESMA/Unisulma.
E-mail: yannlsc255@gmail.com

Henry Guilherme Ferreira Andrade
Professor Orientador. Mestre em Sociologia (UFMA). Especialista em Direito Civil e Empresarial (Fundação Damásio de Jesus – FDDJ) Professor do Curso de Bacharelado em Direito do Instituto de Ensino Superior do Sul do Maranhão – IESMA/Unisulma.
E-mail: henry.andrade@unisulma.edu.br

RESUMO

O presente artigo analisa a responsabilidade civil das empresas no tratamento de dados pessoais, com foco na proteção dos consumidores e na prevenção de vazamentos de informações. A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece um marco jurídico para a segurança da informação, impondo às empresas o dever de adotar medidas técnicas e administrativas eficazes para proteger os dados pessoais contra acessos não autorizados e incidentes de segurança. Aborda os fundamentos da proteção de dados no ordenamento jurídico brasileiro, com base na Constituição Federal e na LGPD, destacando os direitos dos titulares e os deveres dos controladores e operadores de dados. Explora também a responsabilidade civil objetiva nas relações de consumo, conforme o Código de Defesa do Consumidor (CDC), que estabelece que os fornecedores de serviços e produtos devem reparar os danos causados por falhas no tratamento de dados, sem necessidade de comprovação de culpa. Discute o dever de segurança da informação, enfatizando as medidas preventivas que as empresas devem adotar, como criptografia, autenticação multifatorial e políticas de compliance. Por fim, o artigo aborda as consequências jurídicas dos vazamentos de dados, incluindo sanções administrativas previstas pela LGPD, a responsabilidade civil das empresas e as implicações reputacionais, financeiras e jurídicas, tanto para os danos materiais quanto morais causados aos consumidores. O método utilizado nesta pesquisa foi dialético e dedutivo, sendo através da leitura de artigos e livros, bem como a análise de várias legislações do ordenamento jurídico brasileiro.

Palavras-chave: Violação de Direitos. Proteção dos Dados. Responsabilidade Civil. Vazamento de Dados.

[1] Artigo apresentado ao Curso de Bacharelado em Direito do Instituto de Ensino Superior do Sul do Maranhão – IESMA/Unisulma.

1 INTRODUÇÃO

O avanço tecnológico e a crescente digitalização das relações comerciais e sociais trouxeram consigo uma série de benefícios, mas também desafios significativos, principalmente no que se refere à proteção da privacidade e à segurança dos dados pessoais (CAPANEMA, 2020).

Dados pessoais são informações relacionadas a uma pessoa natural identificada ou identificável, que, quando mal gerenciadas, podem causar danos irreparáveis à sua privacidade e à sua segurança. Com a crescente coleta, armazenamento e processamento de dados, especialmente em plataformas digitais e serviços de e-commerce, surge a necessidade urgente de um marco regulatório robusto que regule e proteja os direitos dos indivíduos (BLUM, 2018).

Nesse contexto, a Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, representou um avanço significativo na regulamentação do tratamento de dados no Brasil, alinhando-se a normativas internacionais, como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) (BIONI, 2018).

A LGPD visa proteger a privacidade dos indivíduos, estabelecer normas claras para o tratamento de dados pessoais e criar um sistema de responsabilização para as empresas que lidam com essas informações.

Com a vigência da LGPD, as organizações passaram a ter a responsabilidade de adotar medidas de segurança adequadas, informar seus consumidores sobre o uso de seus dados e garantir que os direitos dos titulares sejam respeitados. A violação desses direitos pode gerar consequências graves para as empresas, incluindo a responsabilidade civil, tanto para os danos patrimoniais quanto morais causados aos titulares de dados, especialmente em caso de vazamentos ou uso indevido de informações pessoais (BLUM, 2018).

A responsabilidade das empresas em caso de vazamento de dados pessoais é um dos aspectos mais relevantes da LGPD e se entrelaça diretamente com as relações de consumo. De acordo com o Código de Defesa do Consumidor (CDC), a responsabilidade civil das empresas nos casos de falhas na prestação de serviços, como é o caso do tratamento inadequado de dados, é objetiva. Isso significa que as empresas podem ser responsabilizadas pelos danos causados, independentemente de culpa, desde que se comprove o defeito ou falha no serviço oferecido (BIONI, 2018).

Nesse sentido, o CDC e a LGPD convergem, estabelecendo uma rede de proteção para o consumidor, que pode ser afetado de maneira significativa pela violação de sua privacidade.

Dessa forma, é necessária a proteção dos dados pessoais como um todo. Assim, nesse contexto, surgiu a Lei de nº 13.709/2018 ou, como é mais conhecida, a Lei Geral de Proteção de Dados (LGPD). Esta lei veio ao ordenamento jurídico brasileiro para dispor sobre o tratamento de dados pessoais, seja este por meio físico ou digital.

Além disso, a segurança da informação tornou-se um dever essencial para as empresas que lidam com dados pessoais. As organizações devem adotar uma série de medidas preventivas e corretivas para garantir que seus sistemas de segurança sejam adequados e que os dados pessoais estejam protegidos contra acessos não autorizados e incidentes de segurança, como o vazamento de informações. A falta de adoção dessas medidas pode resultar em danos diretos e indiretos aos titulares dos dados e comprometer a confiabilidade e a reputação das empresas, além de ensejar a aplicação de sanções pela Autoridade Nacional de Proteção de Dados (ANPD), que é o órgão responsável por fiscalizar a conformidade com a LGPD (CAPANEMA, 2020).

Este artigo tem como objetivo explorar a responsabilidade civil das empresas no tratamento de dados pessoais, com ênfase nas consequências jurídicas e reparação de danos decorrentes de vazamentos de dados.

Serão analisados os fundamentos da proteção de dados pessoais no ordenamento jurídico brasileiro, a responsabilidade objetiva das empresas no contexto das relações de consumo, o dever de segurança da informação e as sanções impostas pela LGPD e outras legislações pertinentes.

A discussão também abrange as boas práticas que as empresas devem adotar para evitar incidentes de segurança e mitigar os riscos de danos aos titulares de dados. Ao final, pretende-se destacar a importância da conformidade com as normas de proteção de dados e a adoção de uma cultura de segurança da informação, que não apenas evita consequências jurídicas, mas também reforça a confiança dos consumidores e a sustentabilidade das empresas no mercado.

Assim, com o avanço da digitalização das relações comerciais e a crescente dependência de dados pessoais no contexto das economias modernas, a responsabilidade civil das empresas por falhas na proteção desses dados assume um papel central no debate jurídico contemporâneo. A implementação de práticas adequadas de segurança, alinhadas aos princípios da LGPD, não apenas cumpre uma função legal, mas também preserva a confiança dos consumidores, assegurando que os direitos fundamentais à privacidade e à proteção dos dados sejam respeitados, mesmo em um ambiente de constantes transformações tecnológicas (BIONI, 2018).

Para isto, faz-se necessária a leitura da Lei Geral de Proteção de Dados, especialmente sobre os fundamentos, princípios, conceitos utilizados pela lei e os artigos que discorrem sobre o tratamento dos dados pessoais. Ainda, mostra-se fundamental a verificação do Código Civil, do Código de Defesa do Consumidor e da Constituição Federal, em especial os artigos que tratam de responsabilidade civil, principalmente sobre reponsabilidade subjetiva e objetiva, dos direitos do consumidor em face à Internet e dos direitos fundamentais garantidos neles.

Além disso, foi realizada a leitura de artigos científicos, monografias, dissertações e doutrinas sobre a responsabilidade civil do fornecedor, os direitos do consumidor na era da Internet e a Lei Geral de Proteção de Dados.

2 FUNDAMENTOS DA PROTEÇÃO DE DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO

Com o avanço das tecnologias de informação e a crescente digitalização das relações sociais, o tratamento de dados pessoais tornou-se um elemento central para o funcionamento das empresas, órgãos públicos e plataformas digitais. Diante desse cenário, cresceu também a preocupação com a proteção desses dados, especialmente quanto ao seu uso indevido, vazamentos e violações à privacidade. No Brasil, a proteção de dados pessoais passou a ser reconhecida expressamente como um direito fundamental, encontrando amparo na Constituição Federal e, mais recentemente, na Lei nº 13.709/2018 – a Lei Geral de Proteção de Dados Pessoais (LGPD) (CAPANEMA, 2020).

Atualmente, vive-se na era da tecnologia, em que uma das suas grandes características é a ausência de fronteiras. Isto foi possível, especialmente, com a invenção da Internet, tendo em vista que o acesso à informação ficou mais fácil, bem como a comunicação entre as pessoas (ARABI, 2017).

A Constituição Federal de 1988, em seu artigo 5º, incisos X e XII, já assegurava a inviolabilidade da intimidade, da vida privada e das comunicações dos indivíduos, prevendo o direito à indenização em caso de violação. No entanto, foi com o advento da LGPD que o ordenamento jurídico brasileiro passou a regulamentar de maneira sistematizada e específica o tratamento de dados pessoais, estabelecendo princípios, direitos e deveres para todas as partes envolvidas, incluindo empresas privadas, poder público e indivíduos. (CAPANEMA, 2020). A LGPD foi inspirada no Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), e representa um marco na consolidação do direito à proteção de dados como um direito autônomo, vinculado à dignidade da pessoa humana. A lei define como dado pessoal qualquer informação relacionada a pessoa natural identificada ou identificável, abrangendo desde nome e CPF até hábitos de consumo e localização. Além disso, introduz o conceito de dados sensíveis, que merecem um grau ainda maior de proteção, como origem racial, convicção religiosa, opinião política, dados de saúde e biometria (BIONI, 2018).

Um dos principais pilares da LGPD é o conjunto de princípios que orientam o tratamento de dados pessoais. Dentre eles, destacam-se: a finalidade, que exige o tratamento para propósitos legítimos, específicos e explícitos; a necessidade, que impõe a limitação do tratamento ao mínimo necessário; a transparência, que assegura ao titular o acesso claro e fácil às informações sobre seus dados; e a segurança, que determina a adoção de medidas técnicas e administrativas para proteger os dados contra acessos não autorizados, vazamentos e outras formas de tratamento indevido (CAPANEMA, 2020).

Outro aspecto fundamental é o reconhecimento dos direitos dos titulares de dados, que incluem, entre outros, o direito de acesso, correção, anonimização, portabilidade, revogação do consentimento e eliminação dos dados. As empresas que tratam dados pessoais, por sua vez, têm o dever de informar com clareza como os dados serão utilizados, por quanto tempo serão armazenados

e com quem serão compartilhados. Esse conjunto de garantias visa fortalecer a autonomia do indivíduo sobre suas informações pessoais e promover maior equilíbrio nas relações entre consumidores e fornecedores de produtos ou serviços (BLUM, 2018).

Diante dessa nova realidade, embora tenha ocorrido grandes avanços tecnológicos, surgiu, também, grandes perigos. Esses perigos surgem quando a manipulação de dados for feita de maneira abusiva ou incorreta pelas empresas, podendo ferir os direitos garantidos na Constituição Federal, como o direito à privacidade. A ameaça aos dados ocorre pois estes têm uma natureza íntima, sendo possível, através do tratamento, identificar informações pessoais de alguém, ou, até mesmo, identificar um indivíduo (BLUM, 2018).

Assim, torna-se indispensável que o Direito evolua e se adapte para poder proteger os direitos da sociedade nessa nova realidade, criando uma relação imbricada entre o Direito e a Tecnologia. A necessidade de legislação, a fim se sanar o vácuo jurídico em relação à Internet, tornou-se evidente no mundo inteiro (CAPANEMA, 2020).

A LGPD também estabelece as figuras do controlador e do operador de dados. O controlador é a pessoa natural ou jurídica responsável pelas decisões referentes ao tratamento de dados, enquanto o operador realiza o tratamento em nome do controlador. Ambas as figuras estão sujeitas à responsabilização em caso de incidentes de segurança ou descumprimento da legislação, conforme será abordado em subtemas posteriores deste artigo (CALAZA, 2024). Por fim, é importante ressaltar que a promulgação da Emenda Constitucional nº 115/2022, que incluiu a proteção de dados pessoais no rol de direitos e garantias fundamentais, consolidou o entendimento de que esse é um direito básico do cidadão brasileiro, a ser respeitado por todos os entes da federação. Essa emenda também conferiu à União a competência privativa para legislar sobre a matéria, reforçando a necessidade de uniformização e eficácia nas políticas públicas e na regulação da proteção de dados.

Assim, os fundamentos jurídicos da proteção de dados pessoais no Brasil repousam sobre um arcabouço normativo robusto e em constante evolução, que busca equilibrar os interesses econômicos das empresas com os direitos fundamentais dos cidadãos. A responsabilidade civil das empresas em caso de falhas nesse tratamento será um dos aspectos que aprofundaremos nos próximos tópicos, destacando a importância de práticas éticas, transparentes e seguras no uso de dados pessoais (CALAZA, 2024).

Por sua vez, o Brasil, tendo como inspiração a lei europeia, passou a Lei nº 13.709 em agosto de 2018, denominada “Lei Geral de Proteção de Dados Pessoais” (LGPD). Apesar dessa lei ter sido aprovada somente em 2018, houve um processo pedagógico de oito anos sobre a discussão de proteção de dados pessoais no país.

Assim, houve seu primeiro esboço em 2010, quando o Ministério da Justiça lançou a primeira consulta pública de um Anteprojeto de Lei. A LGPD tem como foco principal proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Em relação direta com a nova realidade da pandemia, assim, ocorreram várias discussões sobre a entrada em vigor da Lei nº 13.709/2018, a qual era prevista, segundo o art. 65, inciso II, da referida lei, para ocorrer em agosto de 2020. Em verdade, a LGPD entrou em vigor, efetivamente, em setembro de 2020, colocando um fim ao tumultuado período de *vacatio legis* da referida lei, com a publicação da Lei nº 14.058/20.

Isto posto, a referida lei busca fundir os interesses das pessoas jurídicas, manipuladores de dados, e das pessoas físicas, detentores de dados. Essa combinação de interesses ocorre no artigo 2º da Lei Geral de Proteção de Dados, *in verbis*:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor;
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Verifica-se que a lei protege o respeito à privacidade e a inviolabilidade da intimidade, bem como garante o direito de livre concorrência e do desenvolvimento econômico. Assim, garantido um equilíbrio de direitos.

3 RESPONSABILIDADE CIVIL OBJETIVA NAS RELAÇÕES DE CONSUMO

A responsabilização dos fornecedores de produtos ou serviços por danos decorrentes do vazamento de dados pessoais de consumidores encontra respaldo não apenas na Lei Geral de Proteção de Dados (LGPD), mas também no Código de Defesa do Consumidor (CDC). Este último estabelece o regime de responsabilidade civil objetiva nas relações de consumo, o que significa que, para a configuração do dever de indenizar, não se exige a comprovação de culpa do fornecedor, bastando a ocorrência do dano, do defeito no serviço ou produto e o nexo de causalidade (BLUM, 2018).

O artigo 14 do CDC é claro ao dispor que o fornecedor responde, independentemente de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação de serviços. Assim, nos casos de vazamento de dados, a falha na prestação do serviço – consubstanciada na ausência de mecanismos eficazes de segurança da informação – pode ser compreendida como um defeito que gera responsabilidade indenizatória (CALAZA, 2024). A aplicação da

responsabilidade objetiva nas hipóteses de incidentes de segurança envolvendo dados pessoais encontra especial relevância em tempos de digitalização intensa, em que as empresas detêm e processam vastos volumes de informações dos consumidores. A expectativa de que tais dados sejam devidamente protegidos é legítima, e sua violação configura uma quebra da confiança que fundamenta a relação de consumo. Nesse sentido, o tratamento inadequado de dados ou a exposição indevida de informações sensíveis configura um serviço defeituoso, ensejando o dever de reparar o dano causado (DE SOUZA; ANDRÉ, 2025).

Além disso, a LGPD reforça esse entendimento ao prever, em seu artigo 42, que o controlador ou operador de dados que, em razão do exercício de atividades de tratamento de dados pessoais, causar dano patrimonial, moral, individual ou coletivo, responderá por esse dano. A responsabilidade pode ser excluída apenas se o agente demonstrar que não realizou o tratamento de dados, que não houve violação à legislação ou que o dano decorreu exclusivamente de culpa do titular ou de terceiros (SOUZA, 2025).

A junção do regime da LGPD com o CDC fortalece a posição do consumidor frente a incidentes de segurança, visto que ambos os diplomas legais buscam assegurar a dignidade da pessoa humana, a transparência nas relações contratuais e a proteção contra riscos decorrentes da atividade econômica.

Ainda, o Superior Tribunal de Justiça (STJ) já tem se posicionado de forma favorável à responsabilização das empresas em casos de vazamento de dados, reconhecendo a responsabilidade objetiva e admitindo a reparação por danos morais mesmo na ausência de prova de prejuízo material direto, dada a violação da privacidade e da confiança (DE OLIVEIRA, 2025).

É importante destacar que a responsabilidade civil nas relações de consumo também tem função pedagógica e preventiva, ao estimular que os fornecedores invistam em medidas de proteção de dados, tecnologias seguras e programas de compliance digital. Ao mesmo tempo, promove justiça ao titular de dados, que muitas vezes é colocado em situação de vulnerabilidade e exposição pública, com impactos profundos em sua vida pessoal e profissional (DE SOUZA; ANDRÉ, 2025).

Outro ponto relevante é a possibilidade de responsabilidade solidária entre diferentes agentes de tratamento, conforme estabelece a LGPD. Caso haja mais de uma empresa envolvida no ciclo de tratamento dos dados (por exemplo, uma empresa controladora que terceiriza o armazenamento para outra), ambas podem ser responsabilizadas solidariamente perante o titular pelos danos causados. Isso reforça a necessidade de contratos bem estruturados e práticas de governança entre parceiros comerciais, para mitigar riscos e garantir o cumprimento da legislação (DE OLIVEIRA, 2025).

Diante desse cenário, é evidente que a responsabilidade civil objetiva representa uma importante ferramenta de proteção do consumidor na sociedade da informação. Sua aplicação, aliada aos princípios e dispositivos da LGPD, impõe às empresas um dever redobrado de cautela e diligência

no tratamento de dados pessoais, sob pena de sanções administrativas e obrigações indenizatórias (BLUM, 2018).

A responsabilização dos fornecedores, portanto, não deve ser encarada apenas sob a ótica sancionatória, mas como um mecanismo de equilíbrio nas relações jurídicas, essencial à promoção de um ambiente digital mais ético, seguro e transparente.

Assim, ambas as partes da relação do tratamento de dados devem atentar e agir de acordo com tais princípios elencados no artigo 6º da LGPD:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa- fé e os seguintes princípios:
> VIII - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> IX - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> X - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> XI - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> XII - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> XIII - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> XIV - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> XV - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> XVI - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> XVII - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Conforme verificado no artigo acima, a lei dá uma grande distinção ao princípio da boa- fé, destacando dos outros princípios e colocando ele sozinho no *caput* do artigo. Assim, entende-se que a boa-fé é a base de todos os outros princípios.

Por sua vez, a lei em comento determina que as entidades que manipulam as informações pessoais devem assegurar a proteção dos dados de acessos não autorizados, bem como de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Ainda, garante que as empresas necessitam adotar medidas preventivas, a fim de evitar danos aos titulares dos dados (DE OLIVEIRA, 2025).

4 DEVER DE SEGURANÇA DA INFORMAÇÃO: MEDIDAS PREVENTIVAS E BOAS PRÁTICAS

Com o crescente volume de dados pessoais coletados e armazenados por empresas e instituições, o dever de garantir a segurança dessas informações tornou-se um dos aspectos mais relevantes da governança corporativa na era digital.

A Lei Geral de Proteção de Dados Pessoais (LGPD), em seu artigo 46, determina que os agentes de tratamento devem adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Esse dever configura-se como uma obrigação legal e ética que visa assegurar a integridade, a confidencialidade e a disponibilidade das informações pessoais.

O conceito de segurança da informação está diretamente relacionado à ideia de resguardar os dados de riscos internos e externos, prevenindo vazamentos e acessos indevidos. Para tanto, a LGPD exige das empresas uma postura proativa, pautada na prevenção, no monitoramento e na resposta rápida a incidentes. Isso envolve a implementação de políticas de segurança da informação, definição de papéis e responsabilidades, capacitação de colaboradores e adoção de tecnologias apropriadas para cada tipo de tratamento de dados realizado (DE OLIVEIRA, 2025).

Entre as medidas técnicas recomendadas, destacam-se a criptografia de dados, o uso de firewalls, autenticação multifator, controle de acessos, backups regulares e a constante atualização de softwares e sistemas. Já as medidas administrativas incluem a elaboração de planos de resposta a incidentes, auditorias internas, avaliação de riscos, mapeamento dos fluxos de dados e a nomeação de um encarregado de dados (Data Protection Officer – DPO), conforme previsto no artigo 41 da LGPD (DE SOUZA; ANDRÉ, 2025).

O princípio da responsabilização e prestação de contas, previsto no artigo 6º, inciso X, da LGPD, exige que as empresas não apenas implementem boas práticas de segurança, mas também sejam capazes de comprovar que adotaram essas medidas de forma eficaz. Isso implica manter registros de tratamento de dados, documentar as ações preventivas adotadas e demonstrar conformidade com os princípios da lei (DE OLIVEIRA, 2025).

Nesse contexto, ganha relevância o conceito de privacy by design (privacidade desde a concepção), segundo o qual os projetos, produtos e serviços devem ser desenvolvidos com a proteção de dados como um elemento estruturante, desde suas fases iniciais (DE SOUZA; ANDRÉ, 2025).

Da mesma forma, o princípio de privacy by default (privacidade por padrão) exige que as configurações de privacidade oferecidas ao consumidor garantam automaticamente o maior nível de proteção possível, sem necessidade de intervenção do usuário (DE OLIVEIRA, 2025). A adoção de boas práticas de segurança não apenas mitiga riscos legais e financeiros, como também fortalece a

reputação da empresa e a confiança do consumidor. Em um cenário em que a privacidade é cada vez mais valorizada, organizações que demonstram compromisso com a proteção de dados ganham vantagem competitiva e evitam danos irreparáveis à sua imagem institucional.

Além disso, a Autoridade Nacional de Proteção de Dados (ANPD), criada pela LGPD, tem papel fundamental na orientação, fiscalização e aplicação de sanções administrativas às empresas que descumprirem os requisitos legais. As sanções previstas pela LGPD incluem advertências, bloqueio e eliminação de dados pessoais, além de multas que podem alcançar até 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração (DE OLIVEIRA, 2025).

É importante destacar que, embora a LGPD não estabeleça um rol exaustivo de medidas de segurança obrigatórias, ela impõe o dever de adequação às melhores práticas de mercado, levando em consideração a natureza dos dados tratados, o porte da empresa e os riscos envolvidos. Assim, espera-se que cada organização avalie seu contexto específico e implemente um sistema de proteção proporcional, eficaz e continuamente aprimorado.

Por fim, cabe enfatizar que o dever de segurança da informação não é exclusivo de grandes corporações ou do setor de tecnologia. Toda organização que trata dados pessoais — desde um pequeno comércio até um hospital, escola ou repartição pública — está sujeita às exigências da LGPD e deve agir com diligência. A negligência, o improviso ou a ausência de políticas internas são fatores que contribuem para a ocorrência de incidentes e, consequentemente, para a responsabilização da empresa diante dos danos causados aos titulares dos dados.

Dessa forma, o dever de segurança da informação transcende a simples conformidade legal: ele representa um verdadeiro compromisso com os direitos fundamentais dos indivíduos, com a ética nas relações empresariais e com a sustentabilidade da própria atividade econômica na era digital.

5 CONSEQUÊNCIAS JURÍDICAS E REPARAÇÃO DE DANOS POR VAZAMENTO DE DADOS

A ocorrência de vazamentos de dados pessoais não representa apenas uma violação à privacidade dos indivíduos, mas também gera sérias consequências jurídicas para as empresas envolvidas. Diante da gravidade desses incidentes, o ordenamento jurídico brasileiro, por meio da Lei Geral de Proteção de Dados Pessoais (LGPD) e de outras legislações correlatas, prevê sanções administrativas, civis e, em certos casos, até penais. O objetivo é assegurar a reparação dos danos sofridos pelos titulares de dados e, ao mesmo tempo, prevenir novas violações por parte das organizações (MOURA, 2025).

No campo da responsabilidade civil, a LGPD estabelece, em seu artigo 42, que o controlador ou o operador de dados que, em razão da atividade de tratamento, causar dano patrimonial, moral, individual ou coletivo a outrem, é obrigado a repará-lo. Essa responsabilidade pode ser excluída

apenas se o agente demonstrar que não realizou o tratamento de dados, que não houve violação à legislação ou que o dano decorreu exclusivamente de culpa do titular ou de terceiros. Assim, a norma segue um modelo de responsabilidade objetiva, alinhada ao que já dispõe o Código de Defesa do Consumidor (CDC) sobre defeitos na prestação de serviços (DE OLIVEIRA, 2025).

As indenizações decorrentes do vazamento de dados podem incluir tanto danos materiais, como prejuízos financeiros resultantes de fraudes, clonagens ou uso indevido de informações pessoais, quanto danos morais, associados à violação da privacidade, da intimidade e à exposição indevida de dados sensíveis. Em diversos precedentes, o Poder Judiciário brasileiro tem reconhecido o direito à reparação por danos morais mesmo na ausência de prova de prejuízo econômico direto, com base na presunção de que o vazamento, por si só, já configura lesão a direitos da personalidade (MOURA,2025).

Ademais, a LGPD prevê sanções administrativas, aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), que vão desde advertências e bloqueio dos dados pessoais afetados até a imposição de multas que podem alcançar até 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração. As penalidades buscam não apenas punir a conduta ilícita, mas também estimular a adoção de medidas preventivas e boas práticas de governança em proteção de dados (CALAZA, 2024).

Outro aspecto importante é o impacto reputacional para a empresa envolvida em incidentes de vazamento de dados. Em um mercado cada vez mais competitivo e sensível às questões de segurança e transparência, a perda de confiança por parte dos consumidores pode significar prejuízos ainda maiores do que os decorrentes de eventuais indenizações judiciais. Em muitos casos, o abalo à imagem institucional leva à perda de contratos, redução no valor de mercado e dificuldade de atrair novos clientes (DE OLIVEIRA, 2025).

No contexto judicial, é possível também a propositura de ações civis públicas por parte do Ministério Público, da Defensoria Pública e de entidades de defesa do consumidor, visando à reparação coletiva pelos danos causados a múltiplos titulares de dados. A proteção coletiva ganha destaque nos casos em que os vazamentos afetam grandes bases de dados, como já ocorreu em episódios amplamente divulgados, envolvendo instituições bancárias, operadoras de telefonia, empresas de e-commerce e órgãos públicos (MOURA,2025).

Além disso, a depender da gravidade do caso e da natureza das informações expostas, podem surgir repercussões na esfera penal, especialmente se estiverem configurados delitos como invasão de dispositivo informático (art. 154-A do Código Penal), uso indevido de informações sigilosas, estelionato e outras fraudes digitais. Ainda que a empresa não tenha atuado com dolo, sua omissão ou negligência no dever de proteger os dados pode agravar sua situação jurídica (CALAZA, 2024).

A jurisprudência nacional tem caminhado no sentido de consolidar critérios para a reparação de danos, levando em consideração fatores como: o volume de dados vazados, a natureza sensível das informações, a conduta da empresa após o incidente (como transparência e comunicação com os titulares), e a existência ou não de medidas de segurança adequadas. Em muitos casos, a indenização é fixada levando em conta o caráter pedagógico da sanção e o porte econômico do agente infrator (DE OLIVEIRA, 2025).

Dessa forma, as consequências jurídicas do vazamento de dados não se limitam à mera compensação financeira aos titulares prejudicados. Elas refletem um processo mais amplo de amadurecimento das relações jurídicas na era digital, em que o respeito à privacidade, à informação e à segurança passa a ocupar um lugar central nas práticas empresariais (DE OLIVEIRA, 2025).

O cumprimento da LGPD e a adoção de uma cultura de proteção de dados são, portanto, exigências não apenas legais, mas estratégicas, que impactam diretamente a sustentabilidade e a legitimidade das organizações perante a sociedade.

6 CONCLUSÃO

A crescente digitalização das relações sociais e comerciais impõe às empresas um novo paradigma de responsabilidade e transparência quanto ao tratamento de dados pessoais. A entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD) representou um marco regulatório essencial na proteção da privacidade dos indivíduos, conferindo segurança jurídica tanto aos titulares de dados quanto às organizações envolvidas em sua coleta, armazenamento e tratamento.

Nesse contexto, é evidente que o tratamento inadequado de dados pessoais, especialmente quando resulta em vazamentos, impõe às empresas uma série de consequências jurídicas, administrativas e reputacionais.

O presente trabalho demonstrou que a responsabilidade civil das empresas, especialmente nas relações de consumo, é majoritariamente objetiva, conforme estabelecido pelo Código de Defesa do Consumidor e reforçado pela LGPD.

Isso significa que, diante de um incidente de vazamento de dados, não se exige a demonstração de culpa para que o consumidor lesado seja indenizado. Basta a comprovação do dano e do nexo com a falha na prestação do serviço para que surja o dever de reparação.

Ademais, o dever de segurança da informação se apresenta como uma obrigação essencial das empresas, que devem implementar medidas técnicas e administrativas capazes de mitigar riscos, prevenir acessos não autorizados e responder de forma eficiente a incidentes de segurança. O não cumprimento dessas exigências pode resultar não apenas em indenizações civis, mas também em sanções administrativas aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), conforme previsto na legislação vigente.

Portanto, conclui-se que a responsabilidade civil das empresas no tratamento de dados pessoais exige não apenas conformidade normativa, mas também um comprometimento ético com a privacidade e os direitos fundamentais dos cidadãos. A adoção de políticas de governança em privacidade, investimentos em segurança da informação e a cultura da proteção de dados não devem ser vistas como obstáculos ou encargos, mas sim como diferenciais estratégicos em um mercado cada vez mais competitivo e atento à proteção dos direitos dos consumidores. A efetivação da LGPD representa, assim, um passo importante para a construção de um ambiente digital mais seguro, transparente e confiável para todos os envolvidos.

REFERÊNCIAS

ARABI, Abhner Youssif Mota. Direito e tecnologia: relação cada vez mais necessária. **JOTA Info.** 3 jan. 2017. Acesso em: 18 abr. 2024.

BIONI, Bruno R. De 2012 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados. **JOTA Info.** 2 jul. 2018. Acesso em: 18 abr. 2024.

BLUM, Rita Peixoto Ferreira. **O direito à privacidade e a proteção dos dados do consumidor.** São Paulo: Almedina, 2018. *E-book.* Acesso em: 18 abr. 2024.

BRASIL**.** Lei nº 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 12 set. 1990. Acesso 01 mar. 2025.

BRASIL. [Constituição (1988)]. **Constituição Federal.** Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 05 jun. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Acesso em: 20 abr. 2024.

CALAZA, Tales. EVOLUÇÃO E REGULAÇÃO DA PRIVACIDADE E PROTEÇÃO DE DADOS NO CONTEXTO DA INTERNET DAS COISAS NO CENÁRIO BRASILEIRO.
Revista do CAAP. Ed.2024. PDF. Acesso 01 mar. 2025.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos, São Paulo, ano**, v. 21, p. 163-170, 2020. PDF DE OLIVEIRA, Jéssica Batista et al. A proteção de dados pessoais e a aplicação da LGPD no Brasil. **NATIVA-Revista de Ciências, Tecnologia e Inovação**, v. 7, n. 1, p. 166-178, 2025. Acesso 01 mar. 2025.

DE SOUZA, VITÓRIA LIMA; ANDRÉ, VICTOR CONTE. LEI GERAL DE PROTEÇÃO DE DADOS: COLETA DE DADOS SENSÍVEIS DO CONSUMIDOR E A RESPONSABILIDADE CIVIL. **Revista Multidisciplinar do Nordeste Mineiro**, v. 6, n. 1,
p. 1-21, 2025. Acesso 01 mar. 2025.

MOURA, Luana Clara Fernandes de. **A responsabilidade dos provedores de aplicações de internet sobre o direito à desindexação e o direito ao esquecimento: uma análise jurídica baseada no Marco Civil da Internet**. 2025. Acesso 01 mar. 2025.

SOUZA, Marcela Cristina de. **RESPONSABILIDADE CIVIL NO TRATAMENTO DE DADOS: Impactos da Inteligência Artificial na Proteção de Informações Pessoais**. 2025. Acesso 01 mar. 2025.