www.revistaft.com.br

RevistaFT | ISSN 1678-0817 | v.30, n. 159, 2026 | DOI: 10.69849/wntg8q94

Cibersegurança e responsabilidade das empresas frente a vazamento de dados

Cybersecurity and corporate responsibility in the face of data breaches

Cássio Eduardo do Couto Rodrigues[1]

Mariana Gabriela Rodrigues Silva[2]

Resumo: Com a expansão da tecnologia e a digitalização das atividades empresariais, surgiram inúmeros avanços, mas também cresceram os riscos relacionados à segurança e à privacidade dos dados pessoais. No Brasil, o megavazamento de 2021, que atingiu milhões de cidadãos, evidenciou a fragilidade das informações pessoais e a necessidade de mecanismos mais eficazes de proteção. Diante desse cenário, este trabalho analisa a responsabilidade civil das empresas em situações de falhas de segurança e vazamentos de dados, com ênfase na aplicação da Lei Geral de Proteção de Dados (LGPD). Também examina a relação entre a LGPD e o Código de Defesa do Consumidor, bem como o papel fiscalizador da Autoridade Nacional de Proteção de Dados (ANPD). A pesquisa busca compreender os desafios para a efetivação da proteção de dados e para a responsabilização das organizações.

[1] Acadêmico do curso de direito da Instituição de Ensino Superior (IES) Centro Universitário Una de Bom Despacho da rede Ânima de Educação. E-mail: cadusamonte@gmail.com. Artigo apresentado como requisito parcial para a conclusão do curso de Graduação em Direito da Instituição de Ensino Superior (IES) Centro Universitário Una de Bom Despacho da rede Ânima de Educação. 2025. Orientador: Prof. Daniel Dirino.

[2] Acadêmico do curso de direito da Instituição de Ensino Superior (IES) Centro Universitário Una de Bom Despacho da rede Ânima de Educação. E-mail: mariana.gabirodrigues@gmail.com. Artigo apresentado como requisito parcial para a conclusão do curso de Graduação em Direito da Instituição de Ensino Superior (IES) Centro Universitário Una de Bom Despacho da rede Ânima de Educação. 2025. Orientador: Prof. Daniel Dirino.

Palavras-chave: Cibersegurança; Vazamento de Dados; LGPD; Responsabilidade Civil; Proteção de Dados.

Abstract: With the expansion of technology and the digitalization of business activities, many advances have emerged, but so have the risks related to the security and privacy of personal data. In Brazil, the 2021 mega-breach, which affected millions of citizens, highlighted the fragility of personal information and the need for more effective protection mechanisms. In this context, this paper analyzes the civil liability of companies in situations involving security failures and data breaches, with emphasis on the application of the General Data Protection Law (LGPD). It also examines the relationship between the LGPD and the Consumer Defense Code, as well as the supervisory role of the National Data Protection Authority (ANPD). The study seeks to understand the challenges involved in making data protection effective and in holding organizations accountable.

Keywords: Cybersecurity; Data Breach; LGPD; Civil Liability; Data Protection.

1. INTRODUÇÃO

O avanço tecnológico e a existência dos sistemas digitais transformaram profundamente as relações sociais e econômicas, proporcionando benefícios como a otimização de processos, a agilidade na comunicação e a emergência de novos modelos de negócio. Contudo, essa evolução também intensificou os desafios relacionados à segurança e à privacidade dos dados pessoais, tornando-os ativos de valor inestimável e, simultaneamente, alvos de crescentes ameaças cibernéticas. A proteção desses dados, que outrora era tratada de forma fragmentada, ascendeu à categoria de direito fundamental, conforme o art. 5º, incisos X e XII, da Constituição Federal de 1988 (BRASIL, 1988), e ganhou contornos específicos com a promulgação de legislações dedicadas.

No cenário brasileiro, a relevância da cibersegurança e da proteção de dados foi dramaticamente evidenciada por uma série de incidentes, incluindo o notório megavazamento de dados ocorrido em 2021, que expôs informações sensíveis de milhões de cidadãos, como CPF, endereço e dados financeiros (G1,

2021). Tais episódios sublinham a fragilidade das infraestruturas de segurança e a urgência de se adotar práticas robustas de cibersegurança, bem como de se estabelecer mecanismos legais eficazes para a responsabilização de empresas que falham em proteger as informações sob sua custódia.

Nesse contexto, a Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), representou um marco regulatório fundamental. A LGPD estabelece princípios, direitos dos titulares, deveres dos agentes de tratamento e sanções administrativas, visando primordialmente garantir a privacidade e a autodeterminação informativa dos cidadãos. Dentre seus fundamentos, destacam-se os princípios da segurança, prevenção e responsabilização e prestação de contas, previstos no art. 6º (BRASIL, 2018). Adicionalmente, o art. 42 da LGPD impõe ao controlador ou operador que, em violação à legislação de proteção de dados, causar dano patrimonial, moral, individual ou coletivo, a obrigação de repará-lo.

Ainda no âmbito da proteção do indivíduo, a aplicação do Código de Defesa do Consumidor (Lei nº 8.078/1990) merece destaque, especialmente em relações de consumo que envolvem o tratamento de dados pessoais. O CDC consagra a responsabilidade objetiva do fornecedor por falhas na prestação de serviços, o que pode se estender ao ambiente digital, responsabilizando as organizações independentemente da comprovação de culpa, desde que configurado o dano ao consumidor decorrente de incidentes de segurança.

A evolução legislativa brasileira também contempla a Lei nº 15.211, de 17 de setembro de 2025, conhecida como Estatuto Digital da Criança e do Adolescente. Esta norma, embora não substitua a LGPD, complementa-a ao reforçar a necessidade de medidas mais rigorosas de segurança, transparência e cuidado por parte das empresas, especialmente quando o tratamento de dados envolve usuários em situação de maior vulnerabilidade. Assim, o Estatuto Digital da Criança e do Adolescente dialoga com a LGPD ao fortalecer o dever de prevenção e a responsabilização dos agentes que atuam no meio digital, sem afastar a aplicação dos princípios já consolidados da proteção de dados e da responsabilidade civil.

A Autoridade Nacional de Proteção de Dados (ANPD), criada pela Lei nº 13.853, de 8 de julho de 2019, desempenha papel crucial nesse ecossistema, sendo

responsável por fiscalizar, regulamentar e aplicar sanções às empresas que descumprem a legislação. A crescente atuação do órgão, aliada ao aumento da judicialização de casos envolvendo vazamentos de dados, demonstra a busca por maior efetividade na proteção das informações pessoais no Brasil.

Diante desse cenário complexo e dinâmico, o presente trabalho de pesquisa busca analisar a responsabilidade civil das empresas em casos de falhas de segurança e vazamentos de dados. A proposta é investigar como a LGPD tem sido aplicada na prática, os desafios inerentes à sua efetivação e os obstáculos que ainda precisam ser superados para assegurar uma proteção de dados realmente eficaz no ambiente corporativo brasileiro.

2. CIBERSEGURANÇA, LGPD E RESPONSABILIDADE CIVIL DAS EMPRESAS FRENTE AO VAZAMENTO DE DADOS

A proteção de dados pessoais tornou-se um dos principais desafios jurídicos da sociedade contemporânea, especialmente diante da intensificação do uso de tecnologias digitais pelas empresas e do aumento dos riscos de vazamentos e incidentes de segurança. Nesse contexto, o desenvolvimento deste trabalho analisa os fundamentos legais da responsabilidade civil das organizações, com ênfase na Lei Geral de Proteção de Dados Pessoais, no dever de segurança imposto aos agentes de tratamento e na atuação da ANPD.

2.1 O CONTEXTO DA PROTEÇÃO DE DADOS E A FUNDAMENTAÇÃO LEGAL NO BRASIL

A proteção de dados pessoais, no Brasil, transcendeu a esfera de mera preocupação setorial para se consolidar como um direito fundamental, albergado no art. 5º, incisos X e XII, da Constituição Federal de 1988 (BRASIL, 1988). A Carta Magna assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, bem como o sigilo da correspondência e das comunicações, estabelecendo as bases para a tutela da privacidade e da autodeterminação

informativa. Essa elevação do *status* da proteção de dados foi ainda mais reforçada pela Emenda Constitucional nº 115/2022, que inseriu expressamente a proteção de dados pessoais entre os direitos e garantias fundamentais, consolidando sua posição central no ordenamento jurídico brasileiro. Esse arcabouço constitucional foi progressivamente complementado por legislações infraconstitucionais que buscaram regulamentar o tratamento de dados em diferentes contextos.

Um marco importante anterior à LGPD foi a Lei nº 12.965, de 23 de abril de 2014, o Marco Civil da Internet (MCI). O MCI estabeleceu princípios, garantias, direitos e deveres para o uso da Internet no Brasil, incluindo disposições sobre a privacidade e a proteção dos dados pessoais dos usuários (BRASIL, 2014). Embora não fosse uma lei geral de proteção de dados, o MCI já sinalizava a preocupação do legislador com a segurança e a confidencialidade das informações no ambiente digital, preparando o terreno para uma regulamentação mais abrangente e sistêmica.

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, representou a consolidação de um regime jurídico específico e abrangente para a proteção de dados pessoais no país. Inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD estabelece um conjunto de princípios (art. 6º), direitos dos titulares (arts. 17 a 22), deveres dos agentes de tratamento (controlador e operador) e sanções administrativas (arts. 52 a 54 da LGPD), com o objetivo primordial de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018). Sua promulgação marcou uma mudança de paradigma, exigindo das organizações uma postura proativa e responsável na gestão das informações pessoais.

Os princípios da LGPD, em especial os da segurança, prevenção e responsabilização e prestação de contas, são pilares para a compreensão da responsabilidade das empresas frente a vazamentos de dados. O princípio da segurança impõe a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas. O princípio da prevenção exige a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Por fim, o princípio da responsabilização e prestação de contas obriga os agentes de tratamento a

demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais (BRASIL, 2018, art. 6 da LGPD). Esses princípios não são meras diretrizes, mas sim mandamentos que fundamentam o dever de cuidado e a eventual responsabilização dos agentes de tratamento.

A urgência e a relevância desse arcabouço legal foram dramaticamente sublinhadas por incidentes como o megavazamento de dados de 2021, que expôs informações sensíveis de mais de 223 milhões de brasileiros, incluindo dados como CPF, nome completo, endereço, telefone, e-mail e até mesmo informações sobre renda e score de crédito (G1, 2021). Este evento, de proporções inéditas, não apenas evidenciou a vulnerabilidade das infraestruturas de segurança de dados no país, mas também a necessidade premente de uma cultura de cibersegurança robusta e de mecanismos eficazes de responsabilização para as empresas que falham em proteger os dados sob sua custódia.

2.2 O REGIME DE RESPONSABILIDADE CIVIL NA LGPD E A NATUREZA DA RESPONSABILIDADE

A LGPD estabelece um regime de responsabilidade civil específico e rigoroso para os agentes de tratamento de dados pessoais. O art. 42 da LGPD é o dispositivo central nesse contexto, ao prever que "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo" (BRASIL, 2018). Este artigo consagra o dever de indenizar, vinculando-o à ocorrência de um dano e à violação da legislação de proteção de dados, independentemente da comprovação de culpa em muitos casos.

A doutrina majoritária e a jurisprudência incipiente têm interpretado a responsabilidade civil na LGPD com uma forte tendência à objetividade, especialmente em casos de vazamento de dados. Essa orientação decorre da própria natureza da proteção de dados, que visa tutelar um direito fundamental e equilibrar a assimetria de poder entre o titular e o agente de tratamento. Danilo

Doneda (2019, p. 234) argumenta que a LGPD, ao focar na proteção do titular e na imposição de deveres aos agentes de tratamento, desloca o ônus da prova da culpa para o agente, que deve demonstrar que adotou todas as medidas de segurança exigíveis. Assim, para a configuração do dever de indenizar, exige-se a demonstração do dano e do nexo causal entre a conduta do agente de tratamento (ou sua omissão) e o prejuízo experimentado pelo titular. A discussão se a responsabilidade é *objetiva pura* (baseada no risco da atividade) ou *objetiva com culpa presumida* (onde a culpa é presumida e o agente deve provar sua diligência) ainda persiste, mas o consenso é que o titular dos dados é desonerado da prova da culpa do agente.

A violação à legislação de proteção de dados, que é o pressuposto para a responsabilização, pode se manifestar de diversas formas. Inclui a ausência de base legal para o tratamento, o descumprimento dos princípios da LGPD (como a segurança e a prevenção), a falha na adoção de medidas de segurança adequadas, a não comunicação de incidentes de segurança às autoridades e aos titulares quando exigido, ou o tratamento de dados excessivos ou para finalidades diversas das informadas. O dever de segurança, previsto no art. 46 da LGPD, é central aqui: a falha em implementar medidas técnicas e administrativas robustas para proteger os dados é uma violação direta que pode ensejar a responsabilidade.

Os danos passíveis de reparação podem ser de natureza patrimonial (como prejuízos financeiros diretos, custos com a recuperação de identidade, fraudes bancárias) ou moral (como a angústia, o estresse, a violação da privacidade, o risco de fraude, o uso indevido da imagem ou da reputação). A quantificação do dano moral em casos de vazamento de dados é um desafio, exigindo do julgador uma análise cuidadosa das circunstâncias do caso, da natureza dos dados vazados, da extensão do vazamento e do impacto real na vida do titular.

Contudo, é importante ressaltar que a responsabilidade prevista na LGPD não possui caráter absoluto. O artigo 43 da LGPD estabelece hipóteses em que o agente de tratamento pode afastar o dever de indenizar, desde que demonstre que não realizou o tratamento de dados pessoais a ele atribuído, que, embora tenha realizado o tratamento, não houve violação à legislação de proteção de dados, ou que o dano decorreu de culpa exclusiva do titular dos dados ou de terceiros (BRASIL, 2018, art. 43 LGPD).

Assim, a análise da responsabilidade deve ser feita de forma concreta, considerando as circunstâncias específicas de cada caso, a gravidade do incidente, a natureza das informações envolvidas, as medidas de segurança adotadas e a eventual presença de fatores que rompam o nexo causal. Ainda assim, o ônus de comprovar essas excludentes recai sobre o agente de tratamento, o que reforça a necessidade de atuação preventiva, governança adequada e cuidado permanente na gestão das informações pessoais.

2.3 A INTERFACE COM O CÓDIGO DE DEFESA DO CONSUMIDOR

A proteção de dados pessoais no Brasil não se restringe à LGPD, dialogando de forma complementar com outras normas do ordenamento jurídico, notadamente o Código de Defesa do Consumidor (CDC), Lei nº 8.078, de 11 de setembro de 1990. A aplicação do CDC é crucial quando a relação jurídica entre a empresa e o titular dos dados se enquadra como uma relação de consumo (BRASIL, 1990), o que ocorre na vasta maioria dos serviços e produtos digitais oferecidos no mercado.

Nesses casos, o CDC reforça a tutela do titular dos dados, que é considerado a parte vulnerável da relação. O art. 14 do CDC estabelece a responsabilidade objetiva do fornecedor por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos (BRASIL, 1990). Laura Schertel Mendes (2014, p. 123) destaca que, em um ambiente digital, a segurança da informação e a proteção dos dados pessoais são elementos intrínsecos e indissociáveis da qualidade do serviço prestado. Assim, um vazamento de dados pode ser interpretado como um defeito na prestação do serviço, ensejando a responsabilidade objetiva do fornecedor, independentemente da comprovação de culpa. A expectativa legítima do consumidor é que seus dados sejam tratados com segurança e confidencialidade.

A interface entre LGPD e CDC é particularmente relevante em setores como instituições financeiras, plataformas digitais, empresas de comércio eletrônico, operadoras de telecomunicações e prestadores de serviços de saúde. Nesses

segmentos, o tratamento de dados pessoais é parte integrante e essencial da própria atividade empresarial, e a falha na proteção dessas informações pode configurar tanto uma violação à LGPD quanto um defeito na prestação do serviço ao consumidor. A coexistência dessas normas permite uma proteção mais robusta e cumulativa ao titular, que pode invocar os fundamentos de ambas as leis para pleitear a reparação de danos, aplicando-se o princípio do *diálogo das fontes*, onde as normas se complementam para oferecer a máxima proteção ao indivíduo.

Essa sobreposição de regimes jurídicos significa que, em muitos cenários, as empresas podem ser responsabilizadas tanto pelas sanções administrativas da ANPD e pelas ações judiciais baseadas na LGPD, quanto por ações consumeristas que buscam a reparação de danos decorrentes de falhas na segurança dos dados. A vulnerabilidade do consumidor no ambiente digital, acentuada pela complexidade das tecnologias e pela assimetria informacional, justifica plenamente essa dupla camada de proteção, garantindo que a segurança dos dados não seja apenas uma obrigação legal, mas também um componente essencial da qualidade do serviço.

2.4 O PAPEL DA ANPD E A CIBERSEGURANÇA COMO PREVENÇÃO

A efetividade da LGPD e a consequente responsabilização das empresas dependem, em grande medida, da atuação de um órgão regulador e fiscalizador com autonomia e capacidade técnica. A Autoridade Nacional de Proteção de Dados (ANPD) foi criada pela Lei nº 13.853, de 8 de julho de 2019, com a missão de zelar pela proteção dos dados pessoais, fiscalizar e aplicar sanções em caso de descumprimento da legislação, além de elaborar diretrizes e regulamentos (BRASIL, 2019). Sua existência é crucial para a concretização dos direitos previstos na LGPD e para a indução de uma cultura de conformidade no setor privado e público.

A ANPD exerce as seguintes funções:

- No âmbito regulatório, a Autoridade tem a prerrogativa de editar normas complementares e orientações sobre a aplicação da LGPD, como a Resolução CD/ANPD nº 2/2022, que estabelece o regulamento de dosimetria e aplicação de sanções administrativas, e o "Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte" (ANPD, 2024).

Essas normas são essenciais para detalhar as obrigações dos agentes de tratamento e para uniformizar a aplicação da lei.

- Na esfera fiscalizatória, a ANPD pode instaurar processos administrativos, investigar incidentes de segurança (incluindo vazamentos de dados) e aplicar as sanções previstas no art. 52 da LGPD, que incluem advertência, multa simples (até 2% do faturamento, limitada a R$ 50.000.000,00 por infração), multa diária, publicização da infração, bloqueio ou eliminação de dados, suspensão parcial ou total do funcionamento do banco de dados, entre outras (BRASIL, 2018). A atuação da ANPD, portanto, serve como um poderoso incentivo à conformidade.

- Como órgão orientador, a ANPD desempenha um papel fundamental na promoção da cultura de proteção de dados, educando tanto os titulares quanto os agentes de tratamento sobre seus direitos e deveres, por meio de guias, cartilhas e campanhas de conscientização.

Nesse cenário, a cibersegurança emerge como um pilar estratégico e indispensável na prevenção de incidentes e na mitigação da responsabilidade empresarial. O art. 46 da LGPD é explícito ao exigir que os agentes de tratamento adotem medidas de segurança, 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. Isso implica a implementação de um conjunto robusto de práticas e tecnologias, que vão muito além da mera instalação de um antivírus.

Dessa forma, a própria LGPD reforça a necessidade de uma atuação preventiva por parte dos agentes de tratamento. O artigo 46 estabelece que os dados pessoais devem ser protegidos por medidas de segurança, técnicas e administrativas aptas a resguardá-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (BRASIL, 2018, art. 46). Em conformidade com os princípios da segurança,

prevenção e responsabilização e prestação de contas, previstos no artigo 6º da LGPD (BRASIL, 2018, art. 6º).

Em termos práticos, isso significa que a empresa deve estruturar seus processos com mecanismos compatíveis com os riscos envolvidos, o que inclui controle de acesso, criptografia, monitoramento de sistemas, gestão de vulnerabilidades, treinamento de equipes, políticas internas de segurança e planos de resposta a incidentes.

A ausência ou a inadequação dessas medidas de cibersegurança pode ser interpretada como negligência organizacional, configurando uma violação ao dever legal de segurança imposto pela LGPD. Tal falha pode servir como elemento crucial para a imputação da responsabilidade civil à empresa em caso de vazamento de dados, demonstrando que a organização não agiu com a diligência esperada para proteger as informações sob sua guarda. A governança de dados e a cultura de proteção de dados tornam-se, assim, não apenas boas práticas, mas requisitos essenciais para a conformidade legal e a minimização de riscos jurídicos e reputacionais.

2.5 PROTEÇÃO DE VULNERÁVEIS E DESAFIOS PARA A EFETIVIDADE DA LGPD

A LGPD, em seu art. 14, estabelece regras específicas e mais rigorosas para o tratamento de dados pessoais de crianças e adolescentes, exigindo o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal (BRASIL, 2018). Essa proteção diferenciada reflete a maior vulnerabilidade desses grupos no ambiente digital, dada a sua menor capacidade de discernimento, a suscetibilidade a manipulações e o potencial impacto de longo prazo que a exposição indevida de seus dados pode causar em seu desenvolvimento.

A Lei nº 15.211, de 17 de setembro de 2025, o Estatuto Digital da Criança e do Adolescente, complementa a LGPD ao reforçar a necessidade de observância de padrões ainda mais rigorosos de proteção e responsabilização no ambiente digital quando se trata de menores. Essa legislação visa aprimorar a segurança, a

transparência e o cuidado por parte das empresas que interagem com esse público, sem afastar a incidência da LGPD. Ao contrário, o Estatuto Digital da Criança e do Adolescente dialoga com a LGPD ao ampliar o dever de cuidado em contextos de maior vulnerabilidade, fortalecendo a noção de prevenção e de segurança informacional, e estabelecendo diretrizes para a criação de ambientes digitais seguros e adequados à faixa etária (BRASIL, 2025).

O megavazamento de 2021, por exemplo, não apenas expôs a fragilidade técnica, mas também a complexidade de identificar a origem e os responsáveis por incidentes de tal magnitude, bem como a dificuldade em remediar os danos a milhões de indivíduos.

Apesar dos avanços legislativos e da atuação crescente da ANPD, a efetividade da proteção de dados no Brasil ainda enfrenta desafios significativos. Entre eles, destaca-se a assimetria informacional, pois a maioria dos titulares não compreende plenamente como seus dados são coletados, tratados e compartilhados, nem quais riscos decorrem desse processo, o que dificulta o exercício consciente de seus direitos. Soma-se a isso a complexidade da fiscalização, já que a ANPD precisa acompanhar um número expressivo de agentes de tratamento em um país de dimensões continentais e com uma economia digital em constante expansão.

Também merece atenção a maturidade organizacional de muitas empresas, especialmente das de pequeno e médio porte, que ainda enfrentam dificuldades para estruturar programas de governança de dados e cibersegurança compatíveis com as exigências da LGPD. Além disso, a baixa conscientização dos próprios titulares sobre seus direitos e sobre práticas mínimas de segurança no ambiente digital contribui para a permanência de vulnerabilidades e reduz a capacidade de reação diante de eventuais violações. A isso se somam os desafios ligados à interpretação e aplicação da LGPD pelo Poder Judiciário, ainda em processo de consolidação, o que pode gerar certa insegurança jurídica e decisões pouco uniformes.

Por fim, a natureza transnacional da internet e o fluxo internacional de dados tornam a fiscalização e a responsabilização ainda mais complexas, exigindo

cooperação entre autoridades e maior articulação entre os diferentes sistemas de proteção.

A superação desses obstáculos exige um esforço contínuo e multifacetado, envolvendo a educação e conscientização de todos os *stakeholders*, o fortalecimento da ANPD, o investimento em tecnologias de cibersegurança, e a promoção de uma cultura de proteção de dados que permeie todas as camadas das organizações. A prevenção deve ser a tônica, com a adoção de medidas "*privacy by design* e *security by design"*, integrando a proteção de dados desde a concepção de produtos e serviços.

Em suma, a responsabilidade civil das empresas por vazamento de dados pessoais deve ser compreendida como um instrumento multifacetado, que visa tanto à reparação dos danos sofridos pelos titulares quanto à indução da conformidade regulatória e à promoção de uma gestão de dados mais ética e segura. A LGPD, em conjunto com o CDC, o MCI e o Estatuto Digital da Criança e do Adolescente, estabelece um robusto arcabouço legal que impõe às organizações um elevado padrão de diligência, governança e transparência. A efetiva proteção de dados, portanto, depende da conjugação entre prevenção técnica, compromisso institucional, governança corporativa e atuação fiscalizadora do Estado, de modo a assegurar que a inovação tecnológica e a atividade empresarial coexistam com a preservação da dignidade da pessoa humana e dos direitos fundamentais na era digital.

2.6 IMPACTOS PSICOLÓGICOS E SOCIAIS DOS VAZAMENTOS DE DADOS

Os vazamentos de dados pessoais não produzem apenas efeitos jurídicos ou patrimoniais. Na prática, eles atingem diretamente a esfera mais sensível da vida do titular, gerando insegurança, ansiedade, sensação de exposição e perda de controle sobre informações que deveriam permanecer sob proteção. Quando dados são indevidamente acessados, compartilhados ou utilizados por terceiros, o dano ultrapassa a dimensão técnica do incidente e passa a comprometer a tranquilidade, a privacidade e até a confiança da pessoa em suas relações digitais e institucionais.

Esse impacto se torna ainda mais relevante porque o vazamento de dados costuma abrir espaço para fraudes, golpes, perfis falsos, uso indevido de identidade e outras formas de abuso que prolongam os efeitos da violação ao longo do tempo. Assim, o problema não se encerra no momento em que ocorre a falha de segurança, já que suas consequências podem se refletir na rotina da vítima, em sua imagem social e, em alguns casos, em sua vida profissional e familiar. Por isso, a discussão sobre vazamento de dados não deve ser limitada à responsabilidade civil em sentido estrito, mas também compreendida à luz da proteção da dignidade da pessoa humana, que constitui fundamento central da ordem jurídica brasileira.

Os reflexos sociais desses incidentes reforçam a gravidade da conduta ilícita. A divulgação indevida de informações pessoais pode gerar constrangimento, abalo reputacional e perda de confiança em empresas, instituições e serviços digitais. Em um cenário cada vez mais conectado, a privacidade deixou de ser apenas um aspecto formal da vida privada e passou a integrar a própria construção da autonomia do indivíduo. Quando essa proteção é violada, não se trata apenas de um erro operacional, mas de uma lesão concreta a direitos da personalidade.

Dessa forma, os impactos psicológicos e sociais dos vazamentos demonstram que a proteção de dados não se resume a uma obrigação formal de conformidade. Trata-se de um dever jurídico diretamente ligado à tutela da personalidade, da privacidade e da dignidade do titular. Quando a empresa falha nesse dever, a consequência não se limita ao incidente em si, mas alcança a própria experiência subjetiva da vítima, o que reforça a necessidade de prevenção, governança e responsabilização adequada.

3. CONSIDERAÇÕES FINAIS

A discussão apresentada ao longo deste trabalho permitiu compreender que a responsabilidade das empresas diante de vazamentos de dados pessoais é um dos desafios centrais da sociedade digital contemporânea. A consolidação da proteção de dados como direito fundamental reforça a exigência de que as organizações adotem padrões elevados de cuidado, segurança e transparência no tratamento das informações sob sua guarda. A LGPD, ao estabelecer princípios claros e um regime específico de responsabilidade civil, não só orienta a conduta

empresarial, como também fortalece os mecanismos destinados a assegurar os direitos dos titulares.

Verificou-se que a efetiva proteção de dados demanda mais do que o simples cumprimento formal das normas. Trata-se de um processo contínuo que envolve governança, prevenção e adoção de práticas estruturadas desde a concepção de produtos e serviços. A interação entre a LGPD, o Código de Defesa do Consumidor e o Marco Civil da Internet demonstra que a tutela da privacidade não é fragmentada, mas integrada a um sistema que busca equilibrar inovação tecnológica, desenvolvimento econômico e salvaguarda dos direitos da personalidade. Nesse cenário, a atuação da ANPD desempenha papel decisivo ao orientar, fiscalizar e, quando necessário, aplicar sanções capazes de induzir maior comprometimento das organizações.

Os impactos decorrentes de incidentes de segurança, no entanto, vão além da dimensão jurídica. O vazamento de dados atinge a esfera íntima do titular, produz insegurança, abalo emocional e perda de confiança em serviços essenciais da vida moderna. Essa realidade reforça que a proteção de dados não é meramente técnica, mas profundamente humana, ligada à dignidade, à autonomia e à privacidade de cada indivíduo.

Diante desse panorama, conclui-se que a responsabilização civil das empresas não têm apenas função reparatória, mas também educativa e preventiva. A consolidação de uma verdadeira cultura de proteção de dados exige compromisso institucional permanente, investimentos adequados em cibersegurança e conscientização de todos os agentes envolvidos. Somente com essa combinação de esforços será possível construir um ambiente digital mais seguro e confiável, em que o tratamento de dados pessoais ocorra em consonância com os valores fundamentais que orientam o Estado Democrático de Direito.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Site oficial da Agência Nacional de Proteção de Dados.** Brasília, DF: ANPD, 2024. Disponível em: ANPD — Agência Nacional de Proteção de Dados Acesso em: 31 mar. 2026.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 31 mar. 2026.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências**. Diário Oficial da União: seção 1, Brasília, DF, 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 31 mar. 2026.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 31 mar. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 31 mar. 2026.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. **Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados.** Diário Oficial da União: seção 1, Brasília, DF, 9 jul. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 31 mar. 2026.

BRASIL. Lei nº 15.211, de 17 de setembro de 2025. **Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente).** Diário Oficial da União: seção 1, Brasília, DF, 17 set. 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm. Acesso em: 31 mar. 2026.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados.** São Paulo: Thomson Reuters Brasil, 2019.

G1. **Megavazamento de dados atinge 223 milhões de brasileiros e inclui informações de autoridades.** G1, 28 jan. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/megavazamento-de-dados-atinge-223-milhoes-de-brasileiros-e-inclui-informacoes-de-autoridades.ghtml. Acesso em: 31 mar. 2026.

MENDES, Laura Schertel; DONEDA, Danilo. **Proteção de dados pessoais: fundamentos, conceitos e governança.** São Paulo: Thomson Reuters Brasil, 2021. Disponível em: https://books.google.com/ ou catálogo da editora. Acesso em: 8 abr. 2026.