

## RESPONSABILIDADE CIVIL NO VAZAMENTO DE DADOS

Anna Luiza Cardoso Silva<sup>1</sup>  
Bruna Barbosa Silva<sup>2</sup>  
Luiza Cardozo Leocadio<sup>3</sup>

**RESUMO:** O artigo analisa a responsabilidade civil por vazamento de dados pessoais à luz da Lei Geral de Proteção de Dados (LGPD) e da jurisprudência brasileira recente. O objetivo é compreender os fundamentos legais e doutrinários que orientam a responsabilização de agentes de tratamento — públicos e privados — diante de incidentes que comprometam a segurança e a privacidade dos titulares. A pesquisa adota metodologia bibliográfica, com abordagem dedutiva, e inclui análise de precedentes do Superior Tribunal de Justiça. Os principais achados indicam a prevalência da responsabilidade objetiva, com base nas teorias do risco da atividade e do risco administrativo, e a crescente consolidação do dano moral presumido em casos de vazamento de dados sensíveis. Conclui-se que a responsabilização civil é essencial para assegurar a efetividade da proteção de dados pessoais e promover a confiança nas relações digitais contemporâneas.

**Palavras-chaves:** Responsabilidade civil. Vazamento de dados. LGPD. Dano moral. Proteção de dados pessoais. Jurisprudência. Direito à privacidade.

1765

**ABSTRACT:** This article examines civil liability for personal data breaches under the Brazilian General Data Protection Law (LGPD) and recent national case law. The study aims to analyze the legal and doctrinal foundations that guide the liability of data controllers and processors — both public and private — in the event of security incidents that compromise data subjects' privacy. The research adopts a bibliographic methodology with a deductive approach and includes analysis of decisions from the Superior Court of Justice (STJ). The main findings point to the predominance of strict liability, grounded in the theories of enterprise risk and administrative risk, and the increasing recognition of presumed moral damages in cases involving sensitive data. The study concludes that civil liability plays a key role in ensuring the effectiveness of data protection and strengthening digital trust in contemporary legal and social relations.

**Keywords:** Civil liability. Data breach. LGPD. Moral damages. Personal data protection. Case law. Right to privacy.

<sup>1</sup> Graduando em Direito, Universidade Presbiteriana Mackenzie, São Paulo, São Paulo, Brasil,

<sup>2</sup> Graduando em Direito, Universidade Presbiteriana Mackenzie, São Paulo, São Paulo, Brasil,

<sup>3</sup> Graduando em Direito, Universidade Presbiteriana Mackenzie, São Paulo, São Paulo, Brasil,

## INTRODUÇÃO

O desenvolvimento tecnológico e a crescente digitalização das relações sociais, econômicas e administrativas trouxeram benefícios inegáveis à sociedade contemporânea. Contudo, esse avanço também revelou vulnerabilidades, em especial no que se refere à proteção de dados pessoais. A circulação massiva de informações sensíveis em ambientes digitais tem potencializado riscos de vazamentos, acessos indevidos, usos abusivos e violações à privacidade dos indivíduos.

No Brasil, a responsabilidade civil por vazamento de dados ganhou contornos mais definidos com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), que instituiu um microssistema de regulação da matéria. Essa legislação, inspirada em modelos internacionais como o GDPR europeu, busca garantir aos titulares de dados maior controle sobre suas informações, ao mesmo tempo em que impõe obrigações rigorosas a entes públicos e privados quanto à segurança e à transparência no tratamento dos dados.

Este trabalho tem por objetivo analisar a responsabilidade civil decorrente de vazamentos de dados pessoais à luz da legislação brasileira, com especial enfoque na LGPD e em sua articulação com o Código Civil e o Código de Defesa do Consumidor. Para tanto, serão examinados os pressupostos legais, as modalidades de responsabilidade (objetiva ou subjetiva),<sup>1766</sup> as excludentes previstas em lei, bem como a atuação do Poder Judiciário na consolidação da jurisprudência sobre o tema. Também serão abordadas as distinções entre os regimes de responsabilidade aplicáveis a entes públicos e privados, além das contribuições doutrinárias contemporâneas que moldam o entendimento jurídico da matéria.

Ao final, busca-se oferecer uma visão crítica e atualizada sobre os mecanismos de responsabilização existentes, destacando seus desafios práticos e a importância da responsabilidade civil como instrumento de efetivação do direito fundamental à proteção de dados pessoais no Brasil.

### I. CONCEITO DE RESPONSABILIDADE CIVIL EM VAZAMENTOS DE DADOS

A responsabilidade civil, em termos gerais, é o dever jurídico de reparação imposto àquele que causa dano a outrem, seja por ação ou omissão ilícita. No contexto do direito brasileiro, tradicionalmente exige-se a presença de três pressupostos: a conduta (dolosa ou culposa) do agente, o dano experimentado pela vítima e o nexo de causalidade entre ambos. A regra geral prevista no art. 186 do Código Civil baseia-se na culpa: aquele que, por negligência

ou imprudência, viola direito e causa dano a outrem comete ato ilícito e deve indenizar<sup>4</sup>. Todavia, o próprio ordenamento prevê situações de responsabilidade objetiva, independentemente de culpa, quando a atividade desempenhada pelo agente desempenhar riscos para os direitos de outrem (art. 927, parágrafo único, do Código Civil).

Quando se trata de vazamento de dados pessoais, ou seja, a divulgação, acesso ou extração não autorizada de informações privadas, discute-se em que medida aplica-se a responsabilidade subjetiva ou objetiva. Antes da vigência da legislação específica de proteção de dados, a tutela desses casos estava dispersa em diversas normas, como a Constituição Federal, Código Civil e na Lei do Marco Civil da Internet (Lei nº 12.925/14). Essa dispersão normativa levava a soluções casuísticas e muitas vezes contraditórias na jurisprudência, pois faltava um regramento específico<sup>5</sup>.

Com o advento da Lei Geral de Proteção de Dados Pessoais (LGPD, Lei 13.709/2018), inaugurou-se um microssistema jurídico específico para o tratamento de dados pessoais, incluindo disposições explícitas acerca da responsabilidade civil em casos de incidentes de segurança (vazamentos). A LGPD incorporou conceitos modernos de proteção de dados alinhados a legislações internacionais (a exemplo do GDPR europeu), mas adaptados à realidade brasileira. Uma das inovações centrais foi estabelecer, no art. 42, a responsabilidade objetiva do controlador pelos danos decorrentes de tratamento de dados em violação à legislação de proteção de dados.

1767

Importante destacar que a responsabilidade civil por vazamento de dados não tem apenas função reparatória, mas também preventiva e sancionatória. Ao impor obrigações de segurança da informação e penalizar sua inobservância com indenizações vultosas, o direito busca incentivar empresas e órgãos a adotarem medidas eficazes de proteção de dados, mitigando riscos de incidentes. Nesse sentido, a responsabilidade civil cumpre papel complementar a outras esferas de responsabilização: a administrativa e até mesmo a penal, em hipóteses de crimes informáticos. Entretanto, este artigo concentra-se no âmbito civil, ou seja, na obrigação de reparar danos causados aos titulares dos dados, tema este que ganha contornos próprios com a legislação brasileira recente e a construção jurisprudencial em curso.

<sup>4</sup> RIZZARDO, Arnaldo. **Responsabilidade Civil - 8ª Edição 2019**. Rio de Janeiro: Forense, 2019, p.4.

<sup>5</sup> ENCARNACÃO, Paulo Vitor Faria da. **A responsabilidade civil pelo vazamento de dados pessoais**. Migalhas, 2025. Disponível em: <https://www.migalhas.com.br/depeso/436476/a-responsabilidade-civil-pelo-vazamento-de-dados-pessoais>.

## 2. LEGISLAÇÃO BRASILEIRA APLICÁVEL

A legislação brasileira evoluiu significativamente nos últimos anos para abarcar a proteção de dados e responsabilizar os agentes pelos vazamentos. O marco central é a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, que entrou em vigor em setembro de 2020. A LGPD estabelece princípios, direitos e deveres relativos ao tratamento de dados pessoais, aplicáveis tanto a entidades privadas quanto ao Poder Público. A LGPD dedica seção específica à responsabilidade civil, adotando o regime objetivo: o controlador ou operador que, no exercício da atividade de tratamento, causar dano em violação à lei, deve repará-lo, bastando a comprovação do nexo causal.

O art. 42 da LGPD é interpretado como consagrador da responsabilidade civil objetiva no âmbito da proteção de dados, dispensando a prova de culpa do agente e exigindo apenas a demonstração do nexo causal entre o vazamento e o dano sofrido pelo titular dos dados. Em outras palavras, se o incidente de segurança ocorreu em descumprimento da LGPD e causou prejuízo, presume-se a responsabilidade do agente, cabendo a este indenizar.

Há casos previstos em lei que adotam a lógica do direito consumidor, é o caso do art. 45, que dispõe que em casos de violação de direitos do titular em relações de consumo estão sujeitas as regras de responsabilidade do CDC. Com isso, aplica-se o art. 14 do CDC, que estabelece a responsabilidade objetiva do fornecedor de serviços pelos danos causados ao consumidor por defeitos na prestação dos serviços<sup>6</sup>.

1768

Contudo, a objetividade da responsabilidade na LGPD não é absoluta, pois a própria lei prevê excludentes de responsabilização. O art. 43 da LGPD elenca as hipóteses em que os agentes de tratamento não serão responsabilizados, desde que provem: I) que não realizaram o tratamento de dados pessoais que lhes é atribuído; II) que, embora tenham realizado o tratamento, não houve violação à legislação de proteção de dados; ou III) que o dano decorreu de culpa exclusiva do titular dos dados ou de terceiro. Esses incisos funcionam como defesas do controlador/operador, semelhantes às excludentes do CDC (por exemplo, no caso de produto, provar que o defeito inexiste ou foi culpa exclusiva do consumidor/terceiro). Portanto, se a empresa provar que adotou todas as medidas de segurança adequadas e, ainda assim, o vazamento ocorreu sem qualquer contribuição de sua parte, poderia invocar a exclusão de responsabilidade por força maior ou culpa exclusiva de terceiro.

---

<sup>6</sup> GUILHERME, Luiz Fernando Do Vale De A. **Manual de proteção de dados**. São Paulo: Almedina, 2021, p. 48.

A LGPD ainda traz definições importantes para avaliar a conduta do agente. O art. 44 considera irregular o tratamento de dados que deixar de observar a legislação ou não fornecer a segurança que o titular pode esperar, tendo em vista as circunstâncias, incluindo o modo do tratamento, os riscos e as técnicas disponíveis. Ou seja, se a empresa não atualiza seus protocolos de segurança conforme o estado da técnica, ou subestima riscos conhecidos, seu tratamento será considerado “irregular”.

Outro elemento normativo relevante é a obrigação legal de comunicar incidentes de segurança. O art. 48 da LGPD impõe ao controlador o dever de comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante. Embora o descumprimento dessa comunicação gere principalmente sanções administrativas, ele também pode influenciar a análise da responsabilidade civil. Uma resposta tardia ou omissão na comunicação pode agravar os danos (por exemplo, impedindo que os titulares tomem medidas para se proteger), caracterizando negligência que pesa contra o agente na aferição de sua diligência.

Além da LGPD, o Brasil conta com outras normas correlatas. O Marco Civil da Internet (Lei 12.965/2014) estabeleceu princípios para o uso da internet no país, incluindo a proteção da privacidade e de dados pessoais nos registros das conexões e aplicações (arts. 7º e 10). No entanto, com o advento da LGPD, a disciplina específica de tratamento de dados pessoais passou a ser regida principalmente por esta última, que substituiu e aperfeiçoou as regras antes dispersas<sup>7</sup>. O Código Civil também permanece aplicável, no que tange às regras gerais de responsabilidade civil (arts. 186 e 927) e à tutela dos direitos da personalidade (art. 21 do CC).

Por fim, cabe lembrar a inserção definitiva do tema no texto constitucional. Como mencionado, a Emenda Constitucional 115/2022 elevou a proteção de dados pessoais a direito fundamental expresso (CF, art. 5º, LXXIX)<sup>8</sup>. Essa mudança não só reforça a importância do tema, como fixou a competência privativa da União para legislar sobre proteção de dados e atribuiu-lhe a função de organizar e fiscalizar o tratamento de dados pessoais no Brasil. Em nível infraconstitucional, a autoridade central encarregada disso é a ANPD, criada

<sup>7</sup> TIBÚRCIO, Ana Luiza. **Emenda Constitucional 115/2022: Direito à Proteção de Dados Pessoais**. Estratégia Concursos, 2022. <https://www.estategiaconcursos.com.br/blog/emenda-constitucional-115-2022/#:~:text=Ademais%20a%20mat%C3%A9ria%20j%C3%A1%20possui,pessoais%20principalmente%20em%20meios%20digitais>.

<sup>8</sup> TIBÚRCIO, Ana Luiza. **Emenda Constitucional 115/2022: Direito à Proteção de Dados Pessoais**. Estratégia Concursos, 2022. <https://www.estategiaconcursos.com.br/blog/emenda-constitucional-115-2022/#:~:text=Ademais%20a%20mat%C3%A9ria%20j%C3%A1%20possui,pessoais%20principalmente%20em%20meios%20digitais>.

originalmente via Medida Provisória convertida na Lei 13.853/2019 e posteriormente confirmada pela EC 115/2022.

A ANPD pode aplicar sanções administrativas, mas também tem editado regulamentações e recomendações que, de forma indireta, influenciam a aferição de responsabilidade civil (por exemplo, orientando sobre padrões de segurança esperados, planos de resposta a incidentes, etc.). Entretanto, é no Poder Judiciário que a responsabilização civil ganha concretude, como exploraremos ao examinar a jurisprudência.

### 3. JURISPRUDÊNCIA E DOUTRINA

A interpretação dos tribunais brasileiros acerca da responsabilidade civil em casos de vazamento de dados tem evoluído rapidamente desde a vigência da LGPD. Em especial, o Superior Tribunal de Justiça (STJ), já enfrentou diversos processos envolvendo vazamentos e tem delineado parâmetros importantes. Nesta seção, analisaremos alguns precedentes relevantes e a contribuição da doutrina jurídica para o tema.

#### 3.1 Jurisprudência Recente do STJ

Um dos primeiros pontos de debate na jurisprudência foi se o mero vazamento de dados pessoais, por si só, já configuraria dano moral indenizável (*dano in re ipsa*), dispensando prova de prejuízo, ou se seria necessária a comprovação de danos concretos. Inicialmente, a orientação parecia cautelosa quanto a presumir dano moral. Em 2023, em um caso apreciado pelo STJ (AgRg no AREsp 2.130.619/SP), entendeu-se que o vazamento de dados pessoais, ainda que sensíveis, não gera por si só dano moral indenizável, sendo necessária a demonstração de algum prejuízo concreto no caso<sup>9</sup>.

Esse julgado, de relatoria do Ministro Francisco Falcão, causou discussão justamente por impor ao titular dos dados o ônus de provar um prejuízo que muitas vezes é de natureza intangível, como o risco futuro de fraudes ou a mera violação da confiança e privacidade. A doutrina especializada criticou essa postura restritiva, argumentando que a violação da segurança de dados frequentemente acarreta abalos psicológicos e sentimento de insegurança que nem sempre se traduzem em evidências materiais.

<sup>9</sup> LEMOS, Vinicius S.; ROCHA, Madson. **Responsabilidade civil por dados vazados: o que nos ensina o REsp 2.147.374/SP.** Migalhas, São Paulo, 29 maio 2025. Disponível em: <https://www.migalhas.com.br/depeso/431249/responsabilidade-civil-por-dados-vazados-resp-2-147-374-sp>. Acesso em: 16 out. 2025.

Pouco tempo depois, o STJ avançou para um entendimento mais protetivo. Em dezembro de 2024, a 3<sup>a</sup> Turma do STJ julgou o REsp 2.147.374/SP, de Relatório do Min. Ricardo Villas Bôas Cueva) envolvendo o vazamento de dados pessoais não sensíveis em razão de um ataque hacker. A empresa ré alegava que o incidente ocorreu por culpa de terceiro (o hacker), o que afastaria sua responsabilidade com base no art. 43, III, da LGPD<sup>io</sup>.

Nesse julgamento, o STJ consolidou a visão de que o regime de responsabilidade na LGPD se orienta pela lógica do risco e da confiança: cabe ao controlador garantir a expectativa legítima de proteção dos dados por parte dos titulares, respondendo sempre que não conseguir comprovar que atuou com diligência adequada.

O acórdão destacou que a existência de vazamento, mesmo de dados não sensíveis, não afasta automaticamente a responsabilidade da empresa controladora, a tese do “fortuito externo” (ataque de hacker inevitável) só se sustenta se ficar evidenciado que o evento estava fora de sua esfera de prevenção e sem nexo com eventual deficiência de segurança.

Esse entendimento dialoga com outro precedente importante da 3<sup>a</sup> Turma, julgado pouco antes. No REsp 2.121.904/SP, relatado pela Ministra Nancy Andrighi (julgado em 2023), o STJ examinou o caso de uma seguradora que deixou vazar dados pessoais sensíveis de um cliente (informações médicas fornecidas para contratação de seguro de vida). A Turma concluiu que, tratando-se de dados sensíveis, o vazamento por si só expõe o consumidor a riscos graves à sua intimidade, imagem, segurança e até patrimônio, configurando dano moral presumido (*in re ipsa*)<sup>ii</sup>.

1771

A jurisprudência do STJ, portanto, vem diferenciando o tratamento conforme a natureza dos dados vazados. Para dados comuns (não sensíveis), tende-se a exigir alguma demonstração de consequência lesiva concreta, evitando-se condenações automáticas por meros incidentes sem impacto percebido. Já para dados sensíveis, a violação acarreta presunção de dano moral, dada a potencialidade de causar discriminação, constrangimentos ou riscos graves ao titular.

Outro caso paradigmático envolveu o chamado “score de crédito”. No REsp 2.201.694/SP (2021), também relatado pela Min. Nancy Andrighi, discutiu-se a responsabilidade de um

<sup>io</sup> LEMOS, Vinícius S.; ROCHA, Madson. **Responsabilidade civil por dados vazados: o que nos ensina o REsp 2.147.374/SP.** Migalhas, São Paulo, 29 maio 2025. Disponível em: <https://www.migalhas.com.br/depeso/431249/responsabilidade-civil-por-dados-vazados-resp-2-147-374-sp>. Acesso em: 16 out. 2025.

<sup>ii</sup> DUQUE, Felipe. **Vazamento de dados pessoais e danos morais: jurisprudência recente sobre responsabilidade civil digital.** Portal Carreiras Jurídicas – Estratégia Concursos, 16 set. 2025. Disponível em: <https://cj.estrategia.com/portal/vazamento-dados-pessoais-danos-morais-xp/>. Acesso em: 16 out. 2025.

bureau de crédito que teria compartilhado dados cadastrais e de adimplemento de consumidores além do permitido, para fins de cálculo de pontuação de crédito.

O STJ entendeu que o gestor de banco de dados que disponibiliza informações pessoais a terceiros fora dos limites legais deve responder objetivamente pelos danos morais causados aos titulares, sendo esses danos presumidos diante da forte sensação de insegurança experimentada pela vítima.

Nesse precedente<sup>12</sup>, ficou claro que a quebra indevida do sigilo de dados financeiros (mesmo não sendo dados “sensíveis” no rol da LGPD) gera ofensa à privacidade e justifica indenização.

Esse raciocínio fortalece a ideia de que certos dados pessoais, embora não formalmente classificados como sensíveis pela LGPD, situam-se numa “zona cinzenta” em que a divulgação indevida é altamente lesiva (no caso, dados de patrimônio, contas bancárias, limite de crédito etc.), merecendo o mesmo tratamento rigoroso dispensado a dados sensíveis.

Em síntese, o STJ vem construindo um arcabouço no qual: (a) a responsabilidade do agente de tratamento é objetiva, alinhada ao previsto na LGPD, com inversão do ônus da prova favorecendo o titular dos dados em caso de dúvida<sup>13</sup>; (b) a alegação de ataque hacker ou ação de terceiro só ilide a responsabilidade se comprovar a ausência de falha do agente e a exclusividade da atuação externa<sup>14</sup>; (c) a reparabilidade do dano moral decorrente de vazamento depende da natureza e consequência do dado vazado – sendo presumida (*in re ipsa*) nos casos de dados altamente pessoais ou situações de ofensa grave, e exigindo demonstração de impacto nos casos de menor potencial ofensivo. Essa orientação tem repercutido nas instâncias ordinárias, servindo de norte para julgamentos em tribunais estaduais e federais.

1772

### 3.2 Decisões Envolvendo Entes Públicos e Casos Práticos

Não apenas no STJ, mas também nos demais tribunais, observa-se a vasta casuística sobre vazamentos de dados. Por exemplo, o Tribunal de Justiça do Distrito Federal e Territórios (TJDFT), em um julgado de 2024, reconheceu-se a responsabilidade civil objetiva do Estado em

<sup>12</sup> DUQUE, Felipe. **Vazamento de dados pessoais e danos morais: jurisprudência recente sobre responsabilidade civil digital.** Portal Carreiras Jurídicas – Estratégia Concursos, 16 set. 2025. Disponível em: <https://cj.estategia.com/portal/vazamento-dados-pessoais-danos-morais-xp/>. Acesso em: 16 out. 2025.

<sup>14</sup> LEMOS, Vinicius S.; ROCHA, Madson. **Responsabilidade civil por dados vazados: o que nos ensina o REsp 2.147.374/SP.** Migalhas, São Paulo, 29 maio 2025. Disponível em: <https://www.migalhas.com.br/depeso/431249/responsabilidade-civil-por-dados-vazados-resp-2-147-374-sp>. Acesso em: 16 out. 2025.

um caso de vazamento de dados por agente público. No caso, uma servidora do DETRAN/DF acessou e repassou ilegalmente dados pessoais de uma usuária a terceiro, o qual utilizou as informações para ameaçar a vítima. A Turma Recursal do TJDFT confirmou que a Administração Pública responde objetivamente pelos danos causados, seja pela regra constitucional do art. 37, §6º da CF, seja pelas disposições da LGPD (arts. 42 e 43), as quais são aplicáveis às pessoas jurídicas de direito público<sup>15</sup>.

O acórdão enfatizou que o vazamento de dados em sistemas públicos impõe ao Estado o dever de reparar os danos resultantes, diante da violação do dever de segurança. No caso concreto, reputou-se demonstrado o nexo entre a conduta da agente (quebrou o sigilo dos dados) e o dano sofrido (ameaças e transtornos à autora), razão pela qual foi mantida a condenação do Distrito Federal em danos morais (fixados em R\$ 5.000,00).

Por outro lado, há decisões em que os tribunais negaram indenização por entenderem não configurado um dano juridicamente indenizável. Em certas situações de divulgação acidental de dados pouco sensíveis – por exemplo, a divulgação de um número de telefone funcional de servidor público sem consentimento – julgados consideraram que não houve abalo moral suficientemente grave, indeferindo o pedido de dano moral por falta de prova de prejuízo concreto.

1773

Esses casos demonstram que, embora a LGPD imponha obrigações de segurança e possa ter sido violada, nem todo vazamento resultará necessariamente em indenização, sobretudo se o conteúdo vazado for trivial ou já acessível publicamente e se a parte lesada não comprovar nenhum impacto negativo.

### 3.3 Perspectivas da Doutrina

A doutrina brasileira tem se debruçado sobre a responsabilidade civil decorrente do vazamento de dados pessoais, enfatizando a posição dos controladores e operadores à luz da LGPD e do Código Civil. Autores como Bruno Miragem, Danilo Doneda, Ingo Sarlet e Laura Schertel Mendes convergem, em linhas gerais, no sentido de afirmar um regime de responsabilização robusto desses agentes, com base em fundamentos como a natureza da responsabilidade, os pressupostos do dever de indenizar e a função preventiva da reparação civil. Um dos pontos centrais de debate reside na natureza objetiva ou subjetiva da responsabilidade

<sup>15</sup> TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS (TJDFT). Ementário 09/2025 – Lei Geral de Proteção de Dados Pessoais. TJDFT, 2025. Disponível em: <https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/ementario-eletronico-tematico/ementario-09-2025-lei-geral-de-protecao-de-dados-pessoais>. Acesso em: 16 out. 2025.

civil nesses casos. Para Bruno Miragem, "a LGPD consagra um modelo de responsabilidade objetiva, fundado na teoria do risco da atividade"<sup>16</sup>.

Tal compreensão decorre da constatação de que o tratamento de dados pessoais é uma atividade de risco e, por isso, quem dela se beneficia deve responder pelos danos que eventualmente cause, mesmo que sem culpa.

Danilo Doneda e Laura Schertel Mendes destacam que "a legislação brasileira adotou um modelo híbrido, em que a responsabilidade objetiva é a regra nos casos de dano decorrente da violação à LGPD"<sup>17</sup>.

Para os autores, a função preventiva é reforçada quando os controladores se veem obrigados a adotar medidas efetivas de proteção de dados, sob pena de arcarem com os prejuízos de sua omissão. O ilícito, nesse sentido, está diretamente relacionado à inobservância dos deveres de segurança e conformidade, previstos nos artigos 6º, 44 e 46 da LGPD. Ingo Sarlet, por sua vez, sustenta que a proteção de dados deve ser compreendida como "dimensão autônoma dos direitos da personalidade", cuja violação enseja reparação integral, inclusive por danos morais<sup>18</sup>. Dessa forma, o dano imaterial não depende de comprovação econômica, bastando a demonstração de que houve lesão à esfera privada do titular.

A reparação, conforme apontam os autores, também cumpre papel preventivo. Nesse sentido, Miragem salienta que a responsabilidade civil no contexto da LGPD "deve ser compreendida não apenas como mecanismo de reparação, mas como forma de imposição de condutas proativas, em atenção ao dever geral de segurança"<sup>19</sup>. Essa perspectiva se alinha à noção de que o direito à proteção de dados impõe não só obrigações negativas (de não violar), mas também positivas (de proteger). A responsabilização, portanto, opera como instrumento de accountability, em conformidade com os princípios da prevenção, da segurança e da responsabilização previstos no art. 6º da LGPD.

1774

#### 4. ENTES PÚBLICOS E PRIVADOS: DIFERENÇAS DE REGIME DE RESPONSABILIDADE

O aumento exponencial dos incidentes de vazamento de dados pessoais, tanto em instituições públicas quanto privadas, revela um dos maiores desafios do direito

<sup>16</sup> MIRAGEM, Bruno. *Curso de direito do consumidor*. 7. ed. São Paulo: Atlas, 2022. p. 498.

<sup>17</sup> DONEDA, Danilo; MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: elementos para uma convergência normativa*. Revista de Direito do Consumidor, v. 121, p. 139-159, jan./fev. 2020.

<sup>18</sup> SARLET, Ingo Wolfgang. *A efetividade dos direitos fundamentais*. 10. ed. Porto Alegre: Livraria do Advogado, 2021. p. 298.

<sup>19</sup> MIRAGEM, Bruno. *Curso de direito do consumidor*. 7. ed. São Paulo: Atlas, 2022. p. 500.

contemporâneo: determinar como e em que medida cada agente que trata dados deve responder pelos danos causados aos titulares. A responsabilidade civil, nesse contexto, assume uma função que ultrapassa a mera compensação de prejuízos, convertendo-se em instrumento de garantia da confiança e da segurança jurídica nas relações informacionais. Por essa razão, compreender as diferenças entre o regime de responsabilização dos entes públicos e o das entidades privadas é fundamental para a efetividade da tutela de dados pessoais no Brasil.

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) inovou ao instituir um sistema único de proteção, aplicável tanto a pessoas naturais quanto jurídicas, de direito público ou privado, estabelecendo um conjunto de deveres mínimos de transparência, segurança e prestação de contas. Todavia, a aplicação desses deveres não ocorre de maneira uniforme, pois a natureza do agente de tratamento e a finalidade do uso dos dados influenciam diretamente o regime jurídico de responsabilidade. Assim, ainda que o ponto de partida seja o mesmo, o dever de proteger o dado pessoal, as consequências jurídicas da violação variam conforme se trate de ente público ou de entidade privada.

O art. 5º da LGPD define os agentes de tratamento, distinguindo o controlador, responsável pelas decisões sobre o tratamento, e o operador, que o realiza em nome do controlador. Ambos podem responder civilmente pelos danos causados, de forma solidária, quando o tratamento irregular ou a falha na segurança resultar em prejuízo ao titular, conforme art. 42, §1º do mesmo dispositivo. Essa solidariedade não é acidental, mas expressa a função protetiva da lei: garantir que o titular de dados não fique desamparado diante de estruturas empresariais complexas ou da burocracia administrativa.

A doutrina tem destacado que o dado pessoal é um bem jurídico dotado de valor existencial, expressão da personalidade e da dignidade humana. Ingo Wolfgang Sarlet observa que “a proteção de dados pessoais representa uma dimensão essencial da dignidade da pessoa humana e da liberdade individual, traduzindo o direito à autodeterminação informativa” (SARLET, 2022, p. 41)<sup>20</sup>. Sob essa ótica, tanto o Estado quanto as empresas assumem um dever jurídico positivo de tutela, não podendo se eximir de adotar medidas concretas de prevenção.

A responsabilidade civil, nesse cenário, não se limita à compensação. Ela também tem função de controle social e de indução de boas práticas, como observa Guilherme A. Silva ao afirmar que “a responsabilidade civil pelo vazamento de dados deve ser compreendida não apenas como instrumento de compensação do dano individual, mas como técnica de controle

<sup>20</sup> SARLET, Ingo Wolfgang. **A Constituição Digital e a Proteção de Dados Pessoais**. Porto Alegre: Livraria do Advogado, 2022, p. 41.

social e de indução de comportamentos éticos no uso das tecnologias de informação e comunicação” (SILVA, 2020, p. 9)<sup>21</sup>.

A lição de Silva evidencia a dimensão preventiva e pedagógica da responsabilidade civil no ambiente digital. Ao impor a reparação, o direito busca não apenas recompor o dano, mas induzir mudanças estruturais de conduta, reforçando padrões de diligência e ética informacional. Essa natureza normativa explica por que, em muitos casos, o dano moral é presumido: a simples exposição indevida de informações pessoais já configura violação da esfera íntima e quebra da confiança legítima do titular.

Para Ana Frazão, a confiança é o elemento estruturante das relações digitais: “sua quebra implica ofensa à boa-fé objetiva e à segurança jurídica, justificando a responsabilização mesmo na ausência de prejuízo econômico direto” (FRAZÃO, 2021, p. 88)<sup>22</sup>. Essa perspectiva aproxima o regime de responsabilidade civil informacional da teoria da confiança, tradicionalmente aplicada às relações contratuais, agora transposta para o domínio da proteção de dados.

Os danos materiais e morais decorrentes do vazamento de dados assumem contornos específicos. Os primeiros dizem respeito a prejuízos patrimoniais mensuráveis – como fraudes bancárias, clonagem de cartões e perdas financeiras diretas. Já os segundos se ligam à violação da intimidade e da privacidade, podendo ser presumidos quando há exposição indevida de dados sensíveis. Como reforça o artigo “A Responsabilidade Civil pelo Vazamento Digital de Dados sob a Ótica do Direito Brasileiro”, “não se exige, em casos de vazamento de dados pessoais, a demonstração de prejuízo econômico concreto. A violação da privacidade e o sentimento de vulnerabilidade bastam para caracterizar o dano moral” (SILVA, 2020, p. 9-12)<sup>23</sup>.

1776

Além disso, nas hipóteses de vazamento em larga escala, pode-se reconhecer o dano moral coletivo, sobretudo quando há exposição de dados de consumidores, pacientes ou cidadãos. Nesses casos, o prejuízo ultrapassa a esfera individual e atinge a própria confiança da coletividade nas instituições. Bruno Miragem pontua que “a lesão massiva a dados pessoais compromete o equilíbrio das relações de consumo e o tecido de confiança que sustenta o mercado informacional” (MIRAGEM, 2022, p. 498)<sup>24</sup>.

A partir dessa compreensão, torna-se evidente que a responsabilidade civil por vazamento de dados deve ser interpretada conforme o papel e a finalidade de cada agente. As

<sup>21</sup> SILVA, Guilherme A. *A Responsabilidade Civil pelo Vazamento Digital de Dados sob a Ótica do Direito Brasileiro*. Revista de Direito e Tecnologia, 2020, p. 9.

<sup>22</sup> FRAZÃO, Ana. *Direito Civil e Proteção de Dados Pessoais*. São Paulo: Revista dos Tribunais, 2021, p. 88.

<sup>23</sup> SILVA, Guilherme A. *A Responsabilidade Civil pelo Vazamento Digital de Dados sob a Ótica do Direito Brasileiro*. Revista de Direito e Tecnologia, v. 5, n. 2, 2020. p. 9-12.

<sup>24</sup> MIRAGEM, Bruno. *Curso de Direito do Consumidor*. 7. ed. São Paulo: RT, 2022, p. 498.

entidades privadas respondem pela teoria do risco da atividade, porque exploram economicamente a coleta e o uso das informações, assumindo os riscos inerentes à sua atuação. Já os entes públicos se submetem à teoria do risco administrativo, consagrada no art. 37, §6º, da Constituição Federal, segundo a qual o Estado responde objetivamente pelos danos causados a terceiros por seus agentes.

De acordo com Maria Sylvia Zanella Di Pietro, “o Estado deve responder objetivamente pelos danos que seus agentes causem a terceiros, porque exerce atividades que podem gerar prejuízos, e tais ônus não podem ser suportados individualmente pelos administrados” (DI PIETRO, 2023, p. 104)<sup>25</sup>. Assim, no setor público, o fundamento da responsabilidade não é o proveito econômico, mas a necessidade de redistribuir os riscos inerentes à atuação estatal.

Essa diferenciação é fundamental para evitar interpretações uniformes que desconsiderem as particularidades de cada regime. No setor privado, a responsabilidade está ligada à eficiência e à confiança nas relações comerciais; no setor público, ela se conecta à legalidade, à probidade e à eficiência administrativa. Em ambos, contudo, o ponto de convergência é o mesmo: proteger o titular de dados como expressão concreta da dignidade humana.

Dessa forma, o exame que se segue volta-se a detalhar os fundamentos específicos da responsabilidade civil no setor privado e na Administração Pública, evidenciando como cada um desses regimes expressa, a seu modo, o compromisso do ordenamento jurídico brasileiro com a tutela efetiva da privacidade e da segurança informacional.

1777

#### 4.1 Setor Privado

O tratamento de dados pessoais por entidades privadas é, em regra, movido por finalidades econômicas, razão pela qual o legislador optou por um regime de responsabilidade objetiva, nos termos do art. 42 da LGPD<sup>26</sup>. Assim, o dever de indenizar surge da simples ocorrência do dano e do nexo causal, independentemente da prova de culpa.

A opção pela objetividade decorre da aplicação da teoria do risco da atividade, segundo a qual quem auferir proveito econômico deve suportar os riscos inerentes à sua atuação. Conforme explica Bruno Bioni, “a LGPD incorpora o paradigma do risco informacional, em que o agente assume deveres reforçados de prevenção e segurança diante da natureza sensível

<sup>25</sup> DI PIETRO, Maria Sylvia Zanella. *Direito Administrativo*. 36. ed. São Paulo: Atlas, 2023, p. 104.

<sup>26</sup> Art. 42 da Lei Geral de Proteção de Dados: “O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar dano patrimonial, moral, individual ou coletivo a outrem, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.”

dos dados tratados” (BONI, 2020, p. 89)<sup>27</sup>. Essa responsabilidade está atrelada ao dever de diligência empresarial e à obrigação de adotar medidas técnicas e administrativas eficazes para evitar incidentes.

A LGPD, em seu artigo 42, §1º, também prevê a responsabilidade solidária entre controlador e operador, o que reforça a proteção do titular e evita a fragmentação da reparação. Walter Capanema observa que “a solidariedade entre controlador e operador garante a efetividade do sistema e evita que a complexidade tecnológica das cadeias digitais inviabilize o acesso à reparação” (CAPANEMA, 2021, p. 95)<sup>28</sup>. Essa concepção expressa a vocação protetiva da LGPD, que privilegia o princípio da confiança e a tutela do consumidor digital.

Nesse contexto, a boa-fé objetiva assume papel estruturante. Para Ana Frazão, “a confiança legítima do titular de que seus dados serão tratados com lealdade e segurança integra o conteúdo do dever de proteção e sua violação configura inadimplemento contratual e ilícito civil” (FRAZÃO, 2021, p. 91)<sup>29</sup>. A quebra dessa confiança gera não apenas danos materiais, mas também danos morais presumidos, na medida em que a exposição indevida de informações atinge a dignidade e a privacidade do titular.

De fato, como reforça o artigo A Responsabilidade Civil pelo Vazamento Digital de Dados sob a Ótica do Direito Brasileiro, “não se exige, em casos de vazamento de dados pessoais, a demonstração de prejuízo econômico concreto. A violação da privacidade e o sentimento de vulnerabilidade bastam para caracterizar o dano moral” (SILVA, 2020, p. 12)<sup>30</sup>. Nessa linha, a responsabilidade civil atua como mecanismo não apenas reparatório, mas também preventivo e pedagógico, incentivando as empresas a adotarem padrões de governança e compliance informacional.

Por fim, observa-se que a função da responsabilidade civil no setor privado ultrapassa a reparação individual, constituindo instrumento de autorregulação do mercado e de fortalecimento da confiança digital. Como ensina Rogério Montai de Lima, “a governança de dados se tornou elemento central da função social da empresa, e a negligência nesse aspecto compromete sua legitimidade institucional” (LIMA, 2021, p. 77)<sup>31</sup>. Assim, o sistema jurídico impõe às entidades privadas não apenas a obrigação de indenizar, mas o dever permanente de

<sup>27</sup> BONI, Bruno Ricardo. *Proteção de Dados Pessoais: A Função e os Limites do Consentimento*. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 89.

<sup>28</sup> CAPANEMA, Walter. *Responsabilidade Civil na LGPD*. São Paulo: Thomson Reuters Brasil, 2021, p. 95.

<sup>29</sup> FRAZÃO, Ana. *Direito Civil e Proteção de Dados Pessoais*. São Paulo: Revista dos Tribunais, 2021, p. 91.

<sup>30</sup> SILVA, Guilherme A. *A Responsabilidade Civil pelo Vazamento Digital de Dados sob a Ótica do Direito Brasileiro. Revista de Direito e Tecnologia*, v. 5, n. 2, 2020, p. 12.

<sup>31</sup> LIMA, Rogério Montai de. *Direito Digital e Sociedade da Informação*. São Paulo: Atlas, 2021, p. 77.

prevenir riscos e zelar pela integridade informacional como expressão da boa-fé e da dignidade da pessoa humana.

#### 4.2 Administração Pública

A responsabilidade civil da Administração Pública em casos de vazamento de dados pessoais deve ser compreendida à luz da teoria do risco administrativo, consagrada no art. 37, §6º, da Constituição Federal. Essa teoria impõe ao Estado o dever de indenizar o dano causado a terceiros, independentemente de culpa, bastando a comprovação do dano e do nexo causal. O fundamento é de natureza solidária e distributiva: os ônus decorrentes da atuação estatal não podem recair exclusivamente sobre o cidadão que deles sofre os efeitos.

A atuação administrativa, por sua própria natureza, cria situações de risco que não se confundem com as atividades econômicas do setor privado. Enquanto as empresas assumem o risco de sua atividade visando lucro, o Estado o faz em nome do interesse público, devendo responder pelos danos que sua atuação ou omissão cause aos particulares. Conforme explica Maria Sylvia Zanella Di Pietro, “o Estado deve responder objetivamente pelos danos que seus agentes causem a terceiros, porque exerce atividades que podem gerar prejuízos, e tais ônus não podem ser suportados individualmente pelos administrados” (DI PIETRO, 2023, p. 104)<sup>32</sup>.

1779

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) é expressamente aplicável à Administração Pública. O art. 23 determina que o tratamento de dados pessoais pelo poder público deve ser realizado para o atendimento de sua finalidade pública, na persecução do interesse coletivo e na execução de suas competências legais. Essa norma impõe ao Estado um dever reforçado de proteção, em razão da natureza sensível das informações sob sua guarda e do vínculo de confiança existente entre governo e cidadão.

Como observa Danilo Doneda, “a responsabilidade do Estado no tratamento de dados é ampliada pela natureza fiduciária da relação entre governo e cidadão, pois o titular não escolhe fornecer suas informações: ele o faz por imposição legal ou institucional” (DONEDA, 2020, p. 132)<sup>33</sup>. O cidadão não consente voluntariamente com a coleta de seus dados quando se trata de informações exigidas por lei, como registros fiscais, previdenciários ou de saúde, o que aumenta o dever estatal de diligência e cuidado.

Dessa forma, a Administração Pública deve garantir não apenas a licitude do tratamento, mas também a segurança, integridade e confidencialidade das informações, adotando medidas

<sup>32</sup> DI PIETRO, Maria Sylvia Zanella. *Direito Administrativo*. 36. ed. São Paulo: Atlas, 2023, p. 104.

<sup>33</sup> DONEDA, Danilo. *Proteção de Dados Pessoais e Democracia Digital*. Rio de Janeiro: Forense, 2020, p. 132.

técnicas e administrativas eficazes. A violação dessas medidas caracteriza falha no dever de proteção e gera o dever de indenizar, independentemente de comprovação de culpa. A omissão em adotar padrões mínimos de segurança é, portanto, causa autônoma de responsabilidade civil estatal.

A Emenda Constitucional nº 115/2022 elevou a proteção de dados pessoais à categoria de direito fundamental, reforçando o dever estatal de tutela. Para Ingo Wolfgang Sarlet, “a omissão estatal na proteção dos dados pessoais viola diretamente o núcleo da dignidade humana, caracterizando descumprimento de dever fundamental de proteção” (SARLET, 2022, p. 63)<sup>34</sup>. Essa constitucionalização da proteção de dados transforma o dever de indenizar em dever constitucional, conectando-o aos princípios da legalidade, moralidade e eficiência.

A responsabilidade civil do Estado também possui dimensão política e institucional. Quando há um vazamento de dados públicos, como registros de cidadãos, cadastros eleitorais ou informações de saúde, a lesão ultrapassa o plano individual e afeta a confiança da coletividade nas instituições públicas. Trata-se do chamado dano moral coletivo, que, segundo Bruno Miragem, “decorre da violação de um bem jurídico transindividual, afetando a confiança e a estabilidade das relações públicas” (MIRAGEM, 2022, p. 501)<sup>35</sup>. O dano, nesse caso, não é apenas patrimonial ou subjetivo, mas institucional.

1780

Além da reparação civil, o Estado deve adotar medidas preventivas e corretivas, em consonância com o princípio da transparência previsto no art. 6º, VI, da LGPD. A sociedade tem o direito de ser informada sobre incidentes de segurança que possam comprometer dados pessoais sob guarda estatal. A omissão em comunicar o vazamento à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares constitui violação autônoma, com potencial de agravar a responsabilidade do ente público.

Cabe ressaltar que, embora os órgãos públicos não estejam sujeitos às sanções pecuniárias da ANPD, conforme art. 52, §3º, LGPD, essa limitação não afasta sua responsabilidade civil perante o cidadão. O Estado pode ser compelido a reparar danos individuais e coletivos e a adotar medidas de reestruturação de seus sistemas de informação. Em outras palavras, a ausência de multa administrativa não representa imunidade, mas apenas uma adequação à natureza pública da atividade estatal.

<sup>34</sup> SARLET, Ingo Wolfgang. **A Constituição Digital e a Proteção de Dados Pessoais**. Porto Alegre: Livraria do Advogado, 2022, p. 63.

<sup>35</sup> MIRAGEM, Bruno. **Curso de Direito do Consumidor**. 7. ed. São Paulo: Revista dos Tribunais, 2022, p. 501.

A responsabilidade civil da Administração Pública, todavia, não é ilimitada. O próprio art. 37, §6º, assegura ao Estado o direito de regresso contra o agente público causador do dano, quando comprovado dolo ou culpa grave. Essa previsão reforça o equilíbrio entre a proteção do administrado e a responsabilização pessoal do servidor. Assim, preserva-se o interesse coletivo sem gerar impunidade individual.

O controle judicial da responsabilidade estatal em matéria de proteção de dados tem ganhado relevância nos últimos anos. Tribunais vêm reconhecendo que a falha na guarda de informações sigilosas, especialmente aquelas de natureza sensível, como registros médicos e dados fiscais, configura ilícito civil e atinge direitos da personalidade. Esse entendimento reforça o papel do Judiciário na concretização do direito fundamental à privacidade informacional.

Por fim, a responsabilidade do Estado por vazamentos de dados deve ser compreendida como uma manifestação da função protetiva do poder público, inerente ao Estado Democrático de Direito. O dever de indenizar, aqui, não é apenas uma reação ao dano, mas um meio de reafirmar a confiança entre o cidadão e as instituições. Quando o Estado falha em proteger os dados sob sua guarda, compromete não apenas o direito individual, mas o próprio pacto de legitimidade que sustenta a autoridade pública.

1781

## 5. CONCLUSÃO

A análise da responsabilidade civil em casos de vazamento de dados pessoais revela a consolidação de um novo paradigma jurídico, no qual a informação deixa de ser mero bem patrimonial e passa a ser reconhecida como projeção da própria personalidade humana. O tratamento indevido de dados representa, portanto, uma violação à dignidade, à privacidade e à liberdade informacional do indivíduo, valores que hoje possuem assento constitucional expresso. Essa transformação foi impulsionada pela entrada em vigor da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e pela posterior Emenda Constitucional 115/2022, que conferiu à proteção de dados a natureza de direito fundamental, vinculando tanto entes públicos quanto privados a um dever positivo de tutela.

O estudo demonstrou que a responsabilidade civil no contexto da proteção de dados tem natureza objetiva para os agentes de tratamento, baseando-se na teoria do risco da atividade e no dever de segurança. Essa objetividade decorre da constatação de que quem se beneficia economicamente ou institucionalmente do tratamento de dados deve responder pelos riscos que a atividade cria. A LGPD, ao exigir a adoção de medidas técnicas e administrativas adequadas,

impõe aos controladores e operadores um padrão elevado de diligência, cuja violação, ainda que sem culpa, enseja o dever de indenizar. Assim, a reparação civil assume dupla função: recompor o dano sofrido e prevenir novas falhas, funcionando como instrumento pedagógico e de indução de comportamentos responsáveis.

Ainda, verificou-se que os danos indenizáveis decorrentes de vazamentos podem ser de natureza material, moral ou coletiva. O dano material se manifesta em perdas econômicas concretas, como fraudes e desvios; o dano moral decorre da ofensa à esfera íntima e ao sentimento de segurança; e o dano coletivo surge quando o incidente atinge grande número de titulares, comprometendo a confiança social nas instituições. A jurisprudência recente, especialmente do Superior Tribunal de Justiça, tem diferenciado o tratamento conforme a gravidade e a sensibilidade dos dados violados, reconhecendo o dano moral *in re ipsa* nos casos mais graves, como a divulgação de informações de saúde ou financeiras.

No âmbito privado, o regime de responsabilidade se ancora na teoria do risco da atividade e na boa-fé objetiva. O controlador e o operador assumem o dever de assegurar padrões técnicos de segurança compatíveis com o risco de suas operações, respondendo solidariamente por falhas que resultem em vazamento. A negligência em implantar mecanismos de compliance, criptografia ou controle de acesso caracteriza ilícito civil e quebra da confiança legítima do consumidor. A responsabilização, nesses casos, serve também como instrumento de autorregulação e de fortalecimento da função social da empresa na sociedade digital.

1782

Quanto aos entes públicos, o estudo confirmou a aplicação da teoria do risco administrativo, segundo a qual o Estado responde objetivamente pelos danos causados a terceiros, assegurado o direito de regresso contra o agente culpado. A LGPD estende suas regras à Administração, impondo-lhe deveres de segurança e transparência reforçados, dada a natureza fiduciária da relação entre Estado e cidadão. O poder público atua como guardião de informações que o titular é obrigado a fornecer, o que agrava seu dever de proteção. Quando ocorre vazamento, o dano ultrapassa a esfera individual e adquire dimensão institucional, pois corrói a confiança pública e fragiliza o pacto de legitimidade democrática.

Constatou-se ainda que a jurisprudência administrativa e judicial tem papel decisivo na concretização desses princípios. Decisões recentes do STJ e de tribunais locais consolidam o entendimento de que a invocação genérica de ataque cibernético ou culpa de terceiro não basta para afastar a responsabilidade do controlador, que deve provar a adoção de medidas preventivas eficazes. A tendência é de fortalecimento da proteção do titular de dados, invertendo-se o ônus da prova e reafirmando a importância da diligência preventiva.

A conjugação entre lei, doutrina e jurisprudência indica que a responsabilidade civil por vazamento de dados no Brasil avança para um modelo sistêmico, que alia função reparatória, preventiva e sancionatória. O direito civil passa a atuar como instrumento de regulação tecnológica e ética, impondo padrões de conduta que transcendem o mero cumprimento formal da lei. A indenização deixa de ser apenas consequência do dano para tornar-se mecanismo de indução de políticas de segurança e de governança informacional.

Em síntese, a consolidação desse regime jurídico demonstra que a proteção de dados pessoais é condição indispensável à efetivação da dignidade humana na era digital. Tanto o Estado quanto as empresas devem compreender que o dever de proteger informações é também o dever de proteger pessoas. Somente com a aplicação coerente dos princípios analisados, risco, boa-fé, confiança e função social, será possível equilibrar inovação tecnológica e segurança jurídica, garantindo que o progresso informacional ocorra sem sacrificar os direitos fundamentais do indivíduo.

## REFERÊNCIAS

BONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

1783

BRASIL. *Constituição da República Federativa do Brasil de 1988*. (dispositivos: art. 5º, X e LXXIX; art. 37, §6º). Emenda Constitucional nº 115/2022. Disponível em: <https://www.estrategiaconcursos.com.br/blog/emenda-constitucional-115-2022/>. Acesso em: 16 out. 2025.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <https://lgpd-brasil.info/>. Acesso em: 16 out. 2025.

CAPANEMA, Walter. *Responsabilidade civil na LGPD*. São Paulo: Thomson Reuters Brasil, 2021.

CISO ADVISOR. Brasil responde por 43% dos dados vazados no mundo. 16 mar. 2023. Disponível em: <https://www.cisoadvisor.com.br/>. Acesso em: 16 out. 2025.

DI PIETRO, Maria Sylvia Zanella. *Direito administrativo*. 36. ed. São Paulo: Atlas, 2023.

DONEDA, Danilo. *Proteção de dados pessoais e democracia digital*. Rio de Janeiro: Forense, 2020.

DONEDA, Danilo; MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: elementos para uma convergência normativa. *Revista de Direito do Consumidor*, v. 121, p. 139-159, jan./fev. 2020.

DUQUE, Felipe. Vazamento de dados pessoais e danos morais: jurisprudência recente sobre responsabilidade civil digital. *Portal Carreiras Jurídicas – Estratégia Concursos*, 16 set. 2025.

Disponível em: <https://cj.estrategia.com/portal/vazamento-dados-pessoais-danos-morais-xp/>. Acesso em: 16 out. 2025.

ENCARNAÇÃO, Paulo Vitor Faria da. A responsabilidade civil pelo vazamento de dados pessoais. *Migalhas*, 2025. Disponível em: <https://www.migalhas.com.br/depeso/436476/a-responsabilidade-civil-pelo-vazamento-de-dados-pessoais>. Acesso em: 16 out. 2025.

FERREIRA, Lucia M. T.; GARCIA, Matheus. Responsabilidade civil por vazamento de dados pessoais: análise da decisão AREsp 2.130.619/SP. *Revista de Direito Civil Contemporâneo*, v. 13, n. 2, 2024. Disponível em: <https://civilistica.emnuvens.com.br/.../1038>. Acesso em: 16 out. 2025.  
FRAZÃO, Ana. *Direito civil e proteção de dados pessoais*. São Paulo: Revista dos Tribunais, 2021.

GUILHERME, Luiz Fernando do Vale de A. *Manual de proteção de dados*. São Paulo: Almedina, 2021.

LEMOS, Vinicius Silva; ROCHA, Madson. Responsabilidade civil por vazamento de dados: o que nos ensina o REsp 2.147.374-SP? *Migalhas*, 2025. Disponível em: <https://www.migalhas.com.br/depeso/431249/responsabilidade-civil-por-dados-vazados-resp-2-147-374-sp>. Acesso em: 16 out. 2025.

LIMA, Rogério Montai de. *Direito digital e sociedade da informação*. São Paulo: Atlas, 2021.

MIRAGEM, Bruno. *Curso de direito do consumidor*. 7. ed. São Paulo: Revista dos Tribunais, 2022.

RIZZARDO, Arnaldo. *Responsabilidade civil*. 8. ed. Rio de Janeiro: Forense, 2019.

1784

SARLET, Ingo Wolfgang. *A constituição digital e a proteção de dados pessoais*. Porto Alegre: Livraria do Advogado, 2022.

SARLET, Ingo Wolfgang. *A efetividade dos direitos fundamentais*. 10. ed. Porto Alegre: Livraria do Advogado, 2021.

SILVA, Guilherme A. A responsabilidade civil pelo vazamento digital de dados sob a ótica do direito brasileiro. *Revista de Direito e Tecnologia*, v. 5, n. 2, 2020.

TIBÚRCIO, Ana Luiza. Emenda Constitucional 115/2022: direito à proteção de dados pessoais. *Estratégia Concursos*, 2022. Disponível em: <https://www.estrategiaconcursos.com.br/blog/emenda-constitucional-115-2022/#:~:text=Ademais%2C%20a%20mat%C3%A9ria%20j%C3%A1%20possui,pessoais%2C%20principalmente%20em%20meios%20digitais>. Acesso em: 16 out. 2025.

TJDFT – TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. Acórdão 1885894 – Caso DETRAN/DF (Processo 0760950-11.2023.8.07.0016). Julgado em 28 jun. 2024. Disponível em: <https://www.tjdft.jus.br/.../ementario-09-2025-lei-geral-de-protecao-de-dados-pessoais>. Acesso em: 16 out. 2025.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS (TJDFT). *Ementário 09/2025 – Lei Geral de Proteção de Dados Pessoais*. Brasília, 2025. Disponível em: <https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/ementario-09-2025-lei-geral-de-protecao-de-dados-pessoais>.



[eletronico-tematico/ementario-09-2025-lei-geral-de-protectao-de-dados-pessoais. Acesso em: 16 out. 2025.](#)