Revista Brasileira de Direito e Gestão Pública
www.gvaa.com.br/revista/index.php/RDGP/
ISSN: 2358-2405

A efetividade da função punitivo-pedagógica nas indenizações por danos morais nos vazamentos de dados à luz da LGPD: uma análise normativo-jurisprudencial

The effectiveness of the punitive-pedagogical function in moral damage indemnifications in data breaches under the LGPD: a normative-jurisprudential analysis

Marina Duarte Tinoco[1] e João Paulo dos Santos Melo[2]

v. 14/ n. 2 (2026)
Abril/Junho

Aceito para publicação em 16/05/2026.

[1]Graduanda em Direito pela Universidade Federal do Rio Grande do Norte, Natal, Rio Grande do Norte. ORCID: 0009-0005-7887-1230. E-mail: marinadtinoco1@gmail.com;
[2]Doutor em Direito pela Universidade Federal do Paraná, Advogado e Professor da Universidade Federal do Rio Grande do Norte, Natal, Rio Grande do Norte. ORCID: 0009-0006-7891-6360. E-mail: joaopaulo@meloadvogadosassociados.com.

https://www.gvaa.com.br/revista/index.php/RDG

RESUMO: A efetividade da responsabilidade civil como instrumento de proteção dos titulares de dados pessoais constitui um dos debates centrais do direito privado contemporâneo no Brasil. Apesar da entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD) em 2020, os vazamentos de dados continuam crescendo em número e escala, enquanto as condenações judiciais permanecem em patamares reduzidos e a atuação sancionatória da Autoridade Nacional de Proteção de Dados (ANPD) ainda se mostra incipiente. O presente artigo tem como objetivo analisar a efetividade da responsabilidade civil como instrumento de proteção dos direitos dos titulares de dados pessoais no Brasil, com especial enfoque na função punitivo-pedagógica das indenizações por danos morais decorrentes de vazamentos de dados. Para tanto, adota-se o método hipotético-dedutivo, com pesquisa bibliográfica, documental e análise empírica de acórdãos do Superior Tribunal de Justiça e de Tribunais de Justiça estaduais. Os resultados demonstram que o modelo atual de responsabilização civil possui baixa capacidade dissuasória, em razão da oscilação jurisprudencial quanto à configuração do dano moral, dos valores reduzidos das indenizações fixadas e da alta taxa de improcedência das demandas. Conclui-se que a LGPD não é uma lei meramente simbólica, mas sua efetividade depende de aprimoramentos consistentes: ampliação do reconhecimento do dano moral presumido, revisão dos critérios de fixação do quantum indenizatório com incorporação da função punitivo-pedagógica, e fortalecimento da atuação administrativa da ANPD.

Palavras-chave: proteção de dados pessoais; responsabilidade civil; LGPD; dano moral; função punitivo-pedagógica

ABSTRACT: The effectiveness of civil liability as an instrument for protecting personal data subjects is one of the central debates in contemporary private law in Brazil. Despite the entry into force of the General Personal Data Protection Law (LGPD) in 2020, data breaches continue to grow in number and scale, while judicial convictions remain at low levels and the sanctioning activity of the National Data Protection Authority (ANPD) is still incipient. This article aims to analyze the effectiveness of civil liability as an instrument for protecting the rights of personal data subjects in Brazil, with special focus on the punitive-pedagogical function of moral damage indemnifications arising from data breaches. To this end, the hypothetical-deductive method is adopted, with bibliographic, documentary and empirical analysis of decisions from the Superior Court of Justice and state courts. The results show that the current civil liability model has low deterrent capacity, due to jurisprudential oscillation regarding the characterization of moral damage, the low values of indemnifications set and the high rate of dismissed claims. It is concluded that the LGPD is not a merely symbolic law, but its effectiveness depends on consistent improvements: expanding the recognition of presumed moral damage, revising the criteria for setting the quantum of indemnification with incorporation of the punitive-pedagogical function, and strengthening the administrative action of the ANPD.

Keywords: personal data protection; civil liability; LGPD; moral damage; punitive-pedagogical function

1. CONSIDERAÇÕES INICIAIS

A revolução digital e o avanço das tecnologias da informação e comunicação transformaram drasticamente a sociedade contemporânea, alterando as formas de organização social, a economia e a política. Para descrever essa nova realidade, Manuel Castells (2010) criou a expressão "sociedade em rede", na qual a geração, o processamento e a transmissão da informação se tornam as fontes principais de produtividade e poder.

Nesse contexto, os dados passaram a ocupar papel central, sendo coletados em grandes volumes, processados por algoritmos complexos e usados para finalidades que muitas vezes extrapolam aquelas para as quais foram originalmente fornecidos. É nesse cenário que a proteção de dados pessoais passa a figurar como uma das principais questões enfrentadas pelo Judiciário no século XXI.

O direito à privacidade já havia sido positivado na Declaração Universal dos Direitos Humanos de 1948 e na Constituição da República Federativa do Brasil de 1988, no entanto, com os avanços tecnológicos, esse direito adquiriu novos contornos. Atualmente, o conceito de privacidade deixou de ser apenas o direito de não ser incomodado e se tornou o direito de gerir suas próprias informações e moldar a sua própria identidade (RODOTÀ, 2008).

A dimensão dos riscos envolvidos no tratamento massivo de dados ganhou visibilidade mundial com o escândalo envolvendo a empresa Cambridge Analytica, abordado no documentário "Privacidade Hackeada" (*The Great Hack*, 2019), disponibilizado pela Netflix. A obra revela como dados pessoais de milhões de usuários do Facebook foram coletados sem consentimento e utilizados pela Cambridge Analytica para a criação de perfis psicológicos detalhados, os quais serviram de base para a segmentação e o direcionamento de propaganda política durante as eleições presidenciais dos Estados Unidos em 2016 e o referendo do Brexit, no Reino Unido.

O escândalo da Cambridge Analytica acendeu o debate sobre a necessidade de regulamentação específica e robusta do tratamento de dados pessoais. Na Europa, o General Data Protection Regulation (GDPR), Regulamento (UE) nº 2016/679, já havia sido aprovado em 2016, entrando em vigor em maio de 2018, e passou a ser reconhecido como o marco regulatório mais avançado do mundo em matéria de proteção de dados. O GDPR estabeleceu princípios fundamentais, consagrou direitos dos titulares e impôs obrigações concretas aos controladores e operadores de dados, com a previsão de sanções pecuniárias significativas pelo seu descumprimento.

No contexto brasileiro, o aumento exponencial dos incidentes de segurança da informação e dos vazamentos de dados exigiu a criação de um arcabouço normativo específico. Foi nesse cenário que se sancionou, em 14 de agosto de 2018, a Lei n.º 13.709, a Lei Geral de Proteção de Dados Pessoais (LGPD), com entrada em vigor a partir de setembro de 2020. Amplamente inspirada na

legislação europeia, a LGPD estabeleceu um conjunto de princípios, direitos dos titulares e deveres aos agentes de tratamento, além de criar a Autoridade Nacional de Proteção de Dados (ANPD) como órgão regulador e fiscalizador.

Entretanto, a existência de uma legislação específica não é, por si só, suficiente para garantir a efetiva proteção dos titulares de dados. Apesar de todas as exigências legais da LGPD, os vazamentos de dados continuam ocorrendo em larga escala, gerando prejuízos de natureza patrimonial e extrapatrimonial que, muitas vezes, sequer são reconhecidos pelo próprio sistema jurídico.

Diante disso, a responsabilidade civil se apresenta como o mecanismo essencial para proteger os direitos dos titulares de dados, na medida em que permite responsabilizar os agentes de tratamento pelos danos decorrentes do tratamento inadequado ou ilícito das informações pessoais, impondo o dever de reparação.

A responsabilidade civil dos agentes de tratamento de dados encontra fundamento no artigo 42 da LGPD, que impõe ao controlador ou ao operador que causar dano em razão do exercício de atividade de tratamento de dados pessoais a obrigação de repará-lo.

Contudo, a análise da jurisprudência brasileira revela um cenário de significativa instabilidade: de um lado, há julgados que reconhecem o dano moral como presumido *(in re ipsa*) em determinadas hipóteses, especialmente quando envolvem dados sensíveis; de outro, prevalece o entendimento de que o mero vazamento de dados comuns não gera, por si só, a obrigação de indenizar, sendo necessária a prova de dano concreto pelo titular.

A falta de uma posição firme na jurisprudência, aliada aos baixos valores das indenizações estabelecidas, levanta questões relevantes sobre a eficácia da responsabilidade civil em cumprir com suas funções compensatória, preventiva e punitivo-pedagógica em casos de vazamento de dados pessoais.

É nessa perspectiva que se originam as questões centrais que norteiam o presente artigo: até que ponto a responsabilidade civil, como é aplicada atualmente pelo Poder Judiciário brasileiro, consegue exercer sua função punitivo-pedagógica em casos de vazamento de dados pessoais, de forma a desestimular condutas negligentes por parte dos agentes de tratamento e assegurar a proteção real dos titulares?

Ademais, diante crescimento expressivo dos incidentes de segurança no país, aliado à ainda reduzida quantidade de condenações judiciais e à atuação incipiente da ANPD, estaria a LGPD se tornando, na prática, uma legislação meramente simbólica, a chamada "lei para inglês ver"?

Diante dessa problemática, este artigo tem como objetivo geral analisar a efetividade da responsabilidade civil como instrumento de proteção dos direitos dos titulares de dados pessoais no

Brasil, com especial enfoque na função punitivo-pedagógica das indenizações por danos morais decorrentes de vazamentos de dados.

No que diz respeito à metodologia, a presente pesquisa adota o método hipotético-dedutivo, tendo como premissa inicial a ser investigada a possibilidade de que o modelo atual de responsabilização civil por vazamento de dados pessoais possa ser insuficiente para cumprir sua função punitivo-pedagógica, considerando que os patamares indenizatórios fixados pelos tribunais brasileiros podem não alcançar a capacidade dissuasória necessária para induzir mudanças efetivas de comportamento nos agentes de tratamento.

2. A PROTEÇÃO DE DADOS PESSOAIS E A RESPONSABILIDADE CIVIL NA LGPD

2.1. O DEVER DE SEGURANÇA NO TRATAMENTO DE DADOS

Ao definir as regras para o tratamento de dados no Brasil, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD) consagrou como um de seus princípios basilares o da segurança. Nesse sentido, a proteção de dados pessoais pressupõe a adoção de diversas medidas para garantir que os agentes de tratamento dos dados preservem a integridade, confidencialidade e a disponibilidade das informações coletadas. Essas medidas não se limitam a soluções técnicas voltadas a evitar ataques cibernéticos, por exemplo, mas englobam uma verdadeira gestão organizacional e uma cultura de boas práticas de governança.

Ademais, esse dever de segurança não é uma inovação da LGPD, uma vez que o Marco Civil da Internet (Lei nº 12.965/2014) já disciplinava a proteção de dados e segurança na utilização da internet no Brasil. Na mesma perspectiva, o Código de Defesa do Consumidor, (Lei nº 8.078/1990), promulgado em 1990, ao impor ao fornecedor de serviços o dever de adequação e segurança, protege, ainda que indiretamente, os dados pessoais dos consumidores. Isso porque eventual vazamento de dados infringe o dever de segurança esperado pelo consumidor ao fornecer suas informações, caracterizando um defeito do serviço.

A partir dessa construção normativa, evidencia-se que o tratamento de dados no Brasil deve assumir natureza essencialmente preventiva, de modo a evitar a ocorrência de incidentes de vazamento. Sendo assim, a LGPD, ao positivar o dever de segurança, impõe a adoção de medidas técnicas e administrativas capazes de evitar acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Embora a LGPD exija a adoção de medidas técnicas e administrativas voltadas à segurança da informação, a legislação não explicita, de forma detalhada, quais seriam essas medidas e de que forma devem ser implementadas.

Tendo em vista essa lacuna, para auxiliar os agentes de tratamento de dados, a Autoridade Nacional de Proteção de Dados (ANPD), em parceria com o Governo Federal, produziu o "Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte" (ANPD, 2021), o qual oferece, de forma simples, acessível e objetiva, diretrizes para a implementação de mecanismos que buscam efetivar a segurança dos dados, tais como: a elaboração de uma Política de Segurança da Informação - PSI, conscientização e treinamento interno, gerenciamento de contratos, controle de acesso a dados, manutenção de programas de gerenciamento de vulnerabilidades, entre outros.

Todavia, apesar de todas as exigências legais e orientações administrativas voltadas à estruturação de práticas adequadas de segurança da informação, observa-se um aumento desenfreado de vazamentos de dados.

Conforme dados do Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR Gov), 2025 foi o ano com o maior número de incidentes de segurança e vulnerabilidades já registradas pelo órgão, tendo sido contabilizadas 18.092 notificações, o que representa um aumento de 21% em relação ao ano de 2024. Entre os incidentes reportados, o vazamento de dados foi o mais recorrente, o que evidencia a dificuldade de efetivação das medidas previstas no ordenamento jurídico.

2.2. O REGIME DE RESPONSABILIDADE DOS AGENTES DE TRATAMENTO

Diante do aumento do vazamento de dados no Brasil e do descumprimento dos deveres legais, torna-se necessário analisar o regime de responsabilização aplicável aos agentes de tratamento de dados, de modo a entender quem deve ser responsabilizado, quando tais violações ensejam o dever de reparar os danos causados aos titulares de dados e de que forma isso é feito.

Sob essa perspectiva, é importante pontuar que a LGPD subdivide os agentes de tratamento em dois tipos: o controlador e o operador. O controlador é o agente que efetivamente detém o poder sobre os dados, decidindo sobre a forma como o tratamento será realizado. Já o operador é aquele que realiza o tratamento dos dados em nome do controlador, devendo se submeter às instruções adotadas por ele. Essa diferenciação entre os agentes é essencial para compreender as hipóteses de responsabilização.

Ao disciplinar o regime de responsabilização, a Lei Geral de Proteção de Dados dispôs que:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Analisando esse dispositivo, observa-se que a responsabilização recai, em regra, sobre o agente que causou o dano.

Todavia, como bem ressaltou Walter Aranha Capanema em seu artigo "A responsabilidade civil na Lei Geral de Proteção de Dados" (2020), se a relação jurídica entre o controlador/operador e o titular dos dados for consumerista, deve ser utilizado o Código de Defesa do Consumidor, aplicando-se as normas de responsabilização solidária constantes nos artigos 12 e 18 do CDC.

Porém, ainda que a relação entre o agente de tratamento e o titular dos dados não seja consumerista, a LGPD dispõe situações específicas em que a responsabilidade do controlador e do operador será solidária. Uma dessas hipóteses ocorre quando o operador descumprir as obrigações impostas pela legislação de dados ou desobedecer às instruções do controlador. Nesse caso, a atuação do operador ultrapassa sua condição de mero executor do tratamento, aproximando-se da posição do controlador, o que justifica a ampliação de sua responsabilidade.

Além disso, a legislação também prevê a responsabilidade solidária em casos em que há uma cadeia de controladores envolvidos diretamente no tratamento do qual decorrer o dano ao titular. Nesse caso, reconhece-se que a atuação conjunta de todos os controladores contribuiu para o dano.

Dessa forma, a solidariedade entre agentes, seja em relações consumeristas ou em hipóteses específicas elencadas pela LGPD, busca conceder maior efetividade à reparação de danos, permitindo que o titular dos dados possa acionar qualquer dos responsáveis, sem prejuízo do posterior direito de regresso entre os agentes, ressalvadas as hipóteses de exclusão de responsabilidade previstas na própria legislação.

Outro ponto relevante a ser analisado é de que forma será a responsabilização dos agentes de tratamento, se se objetiva, independente de culpa, ou subjetiva, com necessidade de sua comprovação. Essa é uma das principais discussões acerca da responsabilização dos agentes de tratamento, tendo em vista que a LGPD não estabelece, expressamente, a natureza de responsabilização aplicável, o que dá margem para interpretações divergentes na doutrina e jurisprudência.

O entendimento doutrinário majoritário, adotado por grandes doutrinadores como Flávio Tartuce (2023), é de que a responsabilidade dos agentes de tratamento é objetiva. Para eles, o modelo de responsabilização adotado pela LGPD, ao não exigir comprovação de culpa ou dolo e adotar a teoria do risco da atividade em seu artigo 44, se assemelha ao disposto no artigo 927, parágrafo único, do

CC. Ademais, segundo Tartuce (2023, p. 72), "o fato de a lei apontar quais são as excludentes de responsabilização civil é próprio do modelo de responsabilidade objetiva, como se dá com o CDC, o que pode ser defendido a respeito do uso dos dados pessoais".

Em relação ao entendimento jurisprudencial, este também não é pacífico, tendo ocorrido diversas mudanças no regime adotado pela jurisprudência ao longo dos anos. No entanto, atualmente, os Tribunais têm adotado o regime de responsabilização objetiva nos casos de vazamentos de dados em relações de direito do consumidor e quando o vazamento é de dados sensíveis, ao passo que, em casos envolvendo dados comuns, frequentemente se exige a demonstração de culpa ou de dano concreto (FEDERIGHI; CATTA PRETA, 2025).

Além disso, como já exposto, a LGPD elenca, no seu artigo 43, hipóteses em que é excluída a responsabilidade dos agentes de tratamento. Para que isso ocorra, faz-se necessário que o agente de tratamento prove que não realizou o tratamento do dado, que, embora tenha realizado o tratamento, não houve violação à legislação de proteção de dados pessoais, ou ainda que o dano decorreu de culpa exclusiva do titular dos dados ou de terceiros.

Nos casos de vazamento de dados, especialmente em casos de relações de consumo, tem-se aplicado a inversão do ônus da prova, já que a produção de provas acerca de falhas no tratamento de dados é bem mais difícil para o titular, passando a ser dever do agente comprovar fato modificativo, extintivo ou impeditivo do direito do titular dos dados.

Porém, embora a lei tenha estabelecido um sistema de responsabilização bastante abrangente, a eficácia dessa proteção depende de como os prejuízos causados pelos vazamentos são reconhecidos e compensados pelo Judiciário, especialmente no que diz respeito à configuração e quantificação dos danos morais, assunto que será discutido no próximo tópico.

3. O DANO MORAL NO VAZAMENTO DE DADOS PESSOAIS

3.1. O DANO MORAL NO DIREITO BRASILEIRO: CONCEITOS E FUNÇÕES

Até a Constituição de 1988, a responsabilização civil no Brasil possuía caráter essencialmente patrimonialista, estando voltada à reparação de prejuízos de natureza econômica. Nesse contexto, a tutela dos interesses extrapatrimoniais ainda era muito incipiente, havendo significativa resistência doutrinária e jurisprudencial quanto ao reconhecimento autônomo do dano moral e à possibilidade de sua reparação pecuniária. Embora já existissem decisões judiciais admitindo a indenização por lesões a direitos da personalidade, a ausência de previsão expressa gerava insegurança quanto à sua plena aceitação no sistema jurídico brasileiro (TARTUCE, 2021).

É somente com a Constituição de 1988 que o dano moral foi efetivamente positivado no ordenamento jurídico brasileiro. Nesse sentido, a CRFB/88 reconheceu a reparabilidade do dano moral ao assegurar, em seu artigo 5º, incisos V e X, o direito à indenização por danos decorrentes da violação à honra, à imagem, à intimidade e à vida privada.

A partir da constitucionalização do dano moral, este passou a ocupar posição central na responsabilização civil brasileira, sendo um dos pilares do direito civil contemporâneo. Nessa toada, o dano moral tem como finalidade compensar a vítima pelo dano causado aos seus direitos da personalidade em decorrência de ato ilícito. Para Wilson Melo da Silva (1999), o dano moral pode ser definido como: "lesões sofridas pelo sujeito físico ou pessoal natural de direito em seu patrimônio ideal, entendendo-se por patrimônio ideal, em contraposição ao patrimônio material, o conjunto de tudo aquilo que não seja suscetível de valor econômico".

Em relação à sua finalidade, a indenização por danos morais surge essencialmente com a função compensatória, buscando reparar economicamente a vítima pelo prejuízo imaterial sofrido. Trata-se de uma reparação de natureza compensatória, que não restitui integralmente o *status quo ante* à lesão, mas apenas tentar amenizar seus efeitos com uma indenização pecuniária.

Entretanto, ao longo do tempo, viu-se que a tutela do dano moral não deveria restringir sua função a uma mera compensação, mas, na verdade, deveria servir como um verdadeiro desestimulador à prática do ilícito. É nessa perspectiva que a reparação moral passou a assumir função preventiva e punitivo-pedagógica, voltadas a mitigar a repetição de condutas lesivas e promover a proteção aos direitos da personalidade.

Nessa lógica, as funções atribuídas à indenização por dano moral desempenham papel importante na doutrina e jurisprudência brasileira, influenciando diretamente na compreensão da responsabilidade civil e na forma de fixação da indenização pelos tribunais. Tal debate é ainda mais relevante em situações nas quais a violação a direitos da personalidade decorre de atividades que possuem potencial de afetar simultaneamente muitos indivíduos, como ocorre nos casos de vazamento de dados pessoais. Nessas situações, a indenização por dano moral passa a desempenhar papel relevante não apenas na compensação dos titulares afetados, mas também na prevenção de novas falhas no tratamento de dados pessoais.

3.2. A FIXAÇÃO DOS DANOS MORAIS NO BRASIL E SEUS CRITÉRIOS GERAIS

Em relação à fixação do valor da indenização, o Código Civil dispõe, no seu art. 944, que esta é medida de acordo com a extensão do dano. No caso da reparação por danos morais, em que não há

um prejuízo econômico concreto, a aplicação desse dispositivo legal enfrenta dificuldades práticas evidentes, tendo em vista que não é possível quantificar lesões aos direitos da personalidade. Desse modo, a subjetividade para a quantificação do dano moral faz com que a fixação da indenização seja, em grande parte, uma discricionariedade do magistrado.

Diante da inexistência de critérios objetivos, a doutrina e a jurisprudência brasileira passaram a adotar parâmetros que buscam conferir maior racionalidade na quantificação da indenização. Dentre eles, destacam-se: a gravidade da lesão, a extensão do dano causado, a intensidade do sofrimento suportado pela vítima, o grau de culpa ou reprovabilidade da conduta do agente, bem como a capacidade econômica das partes envolvidas. A adoção desses critérios busca garantir uma indenização proporcional e razoável ao ilícito praticado, evitando indenizações irrisórias ou que possam gerar enriquecimento sem causa.

O Superior Tribunal de Justiça comumente adota o método bifásico para a fixação das indenizações por danos morais, o qual, nas palavras do Ministro Paulo de Tarso Sanseverino, funciona da seguinte forma: "Na primeira etapa, deve-se estabelecer um valor básico para a indenização, considerando o interesse jurídico lesado, com base em grupo de precedentes jurisprudenciais que apreciaram casos semelhantes. Na segunda etapa, devem ser consideradas as circunstâncias do caso, para fixação definitiva do valor da indenização, atendendo à determinação legal de arbitramento equitativo pelo juiz" (STJ, REsp 1.152.541/RS, 2011).

Ademais, como exposto no tópico anterior, o arbitramento deve atender as funções compensatória, preventiva e punitivo pedagógica das indenizações por danos morais, buscando não apenas compensar a vítima pela lesão sofrida, mas constranger o autor de forma a desestimular a prática do ilícito.

Entretanto, apesar das tentativas de trazer mais objetividade e racionalidade na quantificação do dano moral, os valores arbitrados, em muitos casos são extremamente reduzidos, que acabam por não compensar a vítima pelo ilícito e não possuem o condão de impedir a repetição da conduta ilegal. Essa realidade esvazia as funções da responsabilização civil, tornando o cometimento do dano vantajoso para aqueles que o praticam.

À vista do exposto, percebe-se a forma como o dano moral é quantificado possui impacto direto na efetividade da responsabilidade civil. A ausência de critérios objetivos e a discricionariedade judicial tornam o arbitramento das indenizações um ponto de intenso debate na doutrina e jurisprudência brasileira, sobretudo quando se busca garantir que a reparação cumpra adequadamente suas funções compensatória, preventiva e punitivo-pedagógica. Essa discussão ganha contornos ainda mais relevantes quando aplicada a novas formas de violação aos direitos da personalidade, como no

caso de tratamento inadequado de dados pessoais. Assim, antes de analisar o papel das indenizações como instrumento de desestímulo a essas práticas, torna-se necessário examinar de que maneira o dano moral tem sido configurado nos casos de vazamento de dados pessoais.

3.3. A CONFIGURAÇÃO DO DANO MORAL NOS CASOS DE VAZAMENTO DE DADOS PESSOAIS

Com o avanço da sociedade da informação e o aumento do tratamento de dados pessoais por empresas e organizações, o surgimento de disputas judiciais relacionadas ao vazamento ou compartilhamento inadequado dessas informações tornou-se cada vez mais frequente. Diante desse cenário, um dos principais dilemas relacionados a essa temática consiste em definir quando é configurado o dano moral no vazamento de dados, se a mera exposição ou divulgação de dados pessoais é suficiente para caracterizar dano moral indenizável ou se seria necessária a comprovação de prejuízo concreto por parte do titular.

Como já evidenciado em tópico anterior, a LGPD estabelece que quando ocorrem vazamentos de dados por falhas na segurança da informação ou descumprimento de normas legais, como a não implementação de medidas técnicas e administrativas de proteção dos dados, o agente de tratamento pode ser responsabilizado pelos danos causados ao titular dos dados. Todavia, nem sempre o vazamento dos dados, por si só, gera o dever de indenizar o titular por danos morais.

Para analisarmos quando o vazamento de dados enseja dano moral indenizável, fazer-se primeiro, uma distinção entre os dois tipos de dados: os dados pessoais comuns e os dados sensíveis. Devido ao potencial discriminatório e grau de exposição da intimidade do indivíduo, a Lei Geral de Proteção de Dados estabeleceu que dados relacionados à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, bem como dados referentes à saúde, à vida sexual, dados genéticos ou biométricos quando vinculados a uma pessoa natural, são considerados sensíveis, sendo necessária uma proteção maior contra essas informações pessoais (BRASIL, 2018, art. 5º, II).

Portanto, como o vazamento desse tipo de dados possui o condão de gerar maior violação aos direitos da personalidade do titular, o prejuízo do titular pela ocorrência do ilícito é, em regra, *in re ipsa*, ou seja, presumido, não sendo necessário que o titular dos dados comprove que o vazamento das informações gerou dano concreto aos seus direitos da personalidade. Desse modo, a jurisprudência tem fixado o entendimento que, nesses casos, o simples vazamento desses dados configura dano moral indenizável (STJ, REsp 2.121.904/SP, 2025).

No entanto, quando o dano decorre de vazamento de dados comuns, a jurisprudência nacional entendeu, em diversos precedentes, que é preciso que seja comprovado o efetivo prejuízo causado à vítima do ilícito. Nessa análise, o simples vazamento de dados comuns não ensejaria a indenização por danos morais ao titular dos dados.

Foi o que Superior Tribunal de Justiça entendeu em recente julgamento do REsp 2221650/SP. No caso analisado, o consumidor alegava que informações como endereço, telefone e título de eleitor teriam sido disponibilizadas sem autorização por empresas gestoras de banco de dados. Contudo, a Quarta Turma do STJ, por unanimidade, decidiu que a indenização somente seria cabível caso fosse demonstrado que houve efetiva divulgação indevida das informações e que tal conduta ocasionou abalo relevante aos direitos da personalidade do titular. Dessa forma, concluiu-se que a mera presença de dados pessoais comuns em bancos de dados utilizados para proteção do crédito não configura automaticamente dano moral indenizável.

Por outro lado, a Terceira Turma do STJ adotou entendimento distinto ao analisar hipótese de disponibilização indevida de informações pessoais em banco de dados. Em apertada votação de três a dois, prevaleceu o entendimento de que o compartilhamento de dados cadastrais do consumidor a terceiros, sem autorização ou comunicação prévia, configura violação aos direitos da personalidade e gera dano moral presumido. Segundo o voto vencedor da Ministra Nancy Andrighi, a divulgação indevida de informações pessoais em bancos de dados acessíveis a terceiros provoca forte sensação de insegurança no titular dos dados, razão pela qual o dano moral pode ser reconhecido independentemente da demonstração de prejuízo concreto (STJ, REsp 2.132.043/SP, 2024).

Outro caso de importante destaque é o julgamento do REsp nº 2.147.374/SP, que abordava a responsabilidade civil de uma empresa controladora de dados em caso de vazamento por ataque de hacker. Após análise, o STJ entendeu que a atuação de terceiro não afasta automaticamente a responsabilidade do agente de tratamento, devendo haver a efetiva demonstração de que foram adotadas medidas de segurança da informação adequadas para que seja possível aplicar a excludente de responsabilização.

Feita essa exposição, é possível constatar que a jurisprudência brasileira ainda não firmou entendimento consolidado no que se refere à configuração do dano moral em casos de vazamento de dados pessoais. O que se percebe é uma análise caso a caso, sendo os tribunais mais rigorosos quando os dados são sensíveis ou há condutas ilícitas.

Nos casos em que é exigida a prova do dano, a produção dessa prova pelo titular é muitas vezes complexa, pois os incidentes de segurança da informação frequentemente atingem simultaneamente diversos titulares, o que dificulta a individualização do dano causado à cada indivíduo. A

exigência dessa prova cria obstáculo significativo à tutela dos direitos dos titulares e a efetivação do dever constitucional de proteção de dados, devendo ser aplicada à inversão do ônus da prova nesses casos.

3.4. O DANO MORAL COLETIVO NOS VAZAMENTOS DE DADOS

Em casos como de publicidade enganosa, infrações ao meio ambiente e danos ao patrimônio histórico, o dano causado pelo ilícito atinge toda a coletividade, sem que seja possível mensurar especificamente o impacto a cada indivíduo. No âmbito do vazamento de dados, é comum que o incidente não se restrinja apenas ao compartilhamento indevido da informação de um titular, mas decorrem de falhas sistêmicas no tratamento de informações, expondo simultaneamente um conjunto de titulares.

É na busca de tutelar os interesses difusos e coletivos que surge a ideia de dano moral coletivo, instrumento utilizado quando há lesão a direitos fundamentais compartilhados por uma coletividade. Para a caracterização do dano moral coletivo, não é preciso a demonstração específica do abalo psíquico decorrente do ilícito, bastando a existência de uma conduta antijurídica, a ofensa a direitos fundamentais, de natureza extrapatrimonial, de determinada coletividade, a intolerabilidade da ilicitude e o nexo causal entre a conduta e o dano (MEDEIROS NETO, 2012).

O dano extrapatrimonial coletivo encontra embasamento jurídico no sistema de proteção dos direitos difusos e coletivos, especialmente nas disposições da Lei da Ação Civil Pública e do Código de Defesa do Consumidor. Esses diplomas reconhecem a possibilidade de responsabilização civil por danos causados a interesses transindividuais, permitindo a propositura de ações coletivas voltadas à reparação de lesões que afetam a coletividade. Nesse contexto, são legitimados para a defesa desses interesses, entre outros, o Ministério Público, a Defensoria Pública e associações civis que tenham por finalidade a proteção dos direitos envolvidos.

No âmbito do vazamento de dados pessoais, o dano moral coletivo tem sido usado como um instrumento jurídico para responsabilizar os agentes de tratamento quando há falhas estruturais na segurança da informação, principalmente quando a conduta deixa de cumprir padrões mínimos exigidos pela legislação. Nesses cenários, a análise tem como objetivo constatar a ofensa a valores essenciais ligados à proteção de dados, como privacidade, segurança e confiança nas relações digitais.

Dessa forma, a responsabilização coletiva ajuda a enfrentar situações em que o ilícito é causado por deficiência sistêmica no tratamento dos dados, destacando a importância da tutela transindividual nesse tipo de violação.

Nesse aspecto, vale destacar que a LGPD, em seu artigo 47, reconhece os direitos coletivos dos titulares, ao prever que agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se ao respeito à legislação de proteção de dados pessoais e aos direitos do titular em toda sua extensão.

Além disso, a Autoridade Nacional de Proteção de Dados (ANPD) possui legitimidade para atuar em casos de repercussão coletiva, podendo instaurar processo administrativo sancionador e adotar medidas preventivas e corretivas, o que reforça a dimensão coletiva da tutela da proteção de dados e amplia os meios de responsabilização para além da esfera judicial individual.

4. A FUNÇÃO PUNITIVO-PEDAGÓGICA DAS INDENIZAÇÕES E SUA EFETIVIDADE NOS VAZAMENTOS DE DADOS À LUZ DA JURISPRUDÊNCIA BRASILEIRA

4.1. A FIXAÇÃO DO QUANTUM INDENIZATÓRIO E A (IN)CAPACIDADE DISSUASÓRIA DAS CONDENAÇÕES

Nos casos em que é reconhecida a responsabilização civil pelos vazamentos de dados, há outro ponto que exige atenção e debate: o *quantum* indenizatório das condenações. A efetividade da tutela jurídica depende, em larga medida, do valor atribuído à condenação, sobretudo quando se pretende aferir sua aptidão para cumprir não apenas a função compensatória, mas sua função punitivo-pedagógica.

Como já exposto, o ordenamento jurídico brasileiro não adota critérios objetivos para a quantificação do dano moral, havendo ampla margem de discricionariedade do magistrado no arbitramento das condenações. Embora a jurisprudência busque meios para uniformizar critérios a serem utilizados para a fixação do quantum, há significativa variação nos valores fixados, inclusive em casos de características assemelhadas e a condenação em valores baixos, que não possuem o condão de constranger o causador do ilícito à uma mudança no comportamento.

Para embasar essa constatação, foi feita uma pequena análise jurimétrica de acórdãos do STJ e diversos Tribunais do Brasil envolvendo danos morais nos casos de vazamento de dados, com o objetivo de identificar padrões na fixação das indenizações. Vejamos:

Tabela 1 – Indenizações por dano moral em casos de vazamento de dados

Tribunal	Processo	Valor (R$)	Natureza do Caso	Observações

STJ	REsp 2.121.904/SP	15.000,00	Vazamento de dados sensíveis	Dados fiscais, bancários e de saúde; dano presumido
TJ-SP	1011977-87.2022.8.26.0361	15.000,00	Fraude em financiamento	Valor majorado em grau recursal
TJ-SP	1025549-54.2021.8.26.0100	15.000,00	Vazamento de dados sensíveis	Dados de saúde, bens e beneficiários
TJ-SP	1001438-40.2025.8.26.0011	10.000,00	Compartilhamento indevido de dados	Violação à LGPD e ao CDC; dano presumido
STJ	REsp 2.187.854/SP	8.000,00	Golpe do boleto	Vazamento de dados bancários sigilosos
TJ-SP	1001283-62.2022.8.26.0457	8.000,00	Fraude em consignado	Descontos indevidos em benefício previdenciário
TJ-PR	0054597-84.2022.8.16.0014	8.000,00	Falsa portabilidade	Uso de dados pessoais e contratuais
STJ	REsp 2.117.561/SP	5.000,00	Compartilhamento de dados cadastrais	Dano moral in re ipsa
TJ-PE	0013999-64.2024.8.17.2480	5.000,00	Fraude bancária	Vítima aposentada por incapacidade
TJ-SP	1008008-78.2023.8.26.0248	5.000,00	Golpe do boleto	Uso de dados contratuais precisos
TJ-PR	0026395-97.2022.8.16.0014	5.000,00	Fraude via PIX	Uso de dados bancários vazados
TJ-RJ	0804433-67.2023.8.19.0207	5.000,00	Golpe da falsa central	Vítima idosa
STJ	REsp 2.222.983/SP	3.000,00	Divulgação de dados cadastrais	Dano presumido
TJ-DF	0715047-16.2024.8.07.0016	3.000,00	Spoofing bancário	Vítima idosa
TJ-AL	0701717-79.2024.8.02.0051	2.500,00	Fraude com empréstimos	Consumidora idosa e vulnerável
TJ-SP	1008787-17.2023.8.26.0609	1.000,00	Tentativa de fraude	Indício de vazamento de dados

Fonte: Elaboração própria a partir de decisões do STJ e Tribunais de Justiça (2021–2026).

Conforme se observa na tabela acima, os valores das condenações concentram-se em uma faixa intermediária, predominantemente entre R$ 3.000,00 e R$ 8.000,00, sendo raras as hipóteses em que a condenação ultrapassa o patamar de R$ 10.000,00. Os valores mais elevados, na ordem de R$ 15.000,00, aparecem de forma excepcional e estão, em geral, associados a casos que envolvem o vazamento de dados pessoais sensíveis ou fraudes com repercussões concretas na esfera patrimonial do titular. Por outro lado, situações envolvendo dados cadastrais, tentativas de fraude ou ausência de

prejuízo material direto tendem a resultar em indenizações significativamente inferiores, chegando a patamares mínimos, como R$ 1.000,00.

Desse modo, é possível inferir que os montantes fixados permanecem relativamente irrisórios quando comparados ao potencial econômico dos agentes, o que reforça a percepção de uma resposta judicial ainda limitada diante da gravidade potencial dos vazamentos de dados no contexto da sociedade digital.

Ademais, ao construir a análise dos acórdãos, priorizou-se aqueles em que o julgamento foi procedente para a indenização por danos morais. Todavia, o que se vê na prática é que a maioria das decisões é, na verdade, de improcedência. Em grande parte dos casos, especialmente aqueles que envolvem dados pessoais não sensíveis, os tribunais exigem a comprovação de prejuízo concreto, afastando a indenização sob o argumento de ausência de lesão efetiva à esfera extrapatrimonial do titular (FEDERIGHI; CATTA PRETA, 2025).

Diante disso, tem-se um cenário em que a responsabilização não apenas é limitada em termos de valor, mas também em sua própria aplicação, reduzindo significativamente o risco jurídico associado à atividade de tratamento de dados.

Nesse contexto, a responsabilidade civil corre o risco de assumir um caráter meramente residual, incidindo apenas em hipóteses mais graves ou em que há prova evidente de prejuízo, o que compromete sua função preventiva. A alta taxa de improcedência e a fixação de indenizações baixas contribuem significativamente para o esvaziamento do potencial punitivo-pedagógico do instituto, tornando-o insuficiente para desestimular práticas negligentes e garantir a efetiva proteção dos direitos dos titulares de dados.

Essa realidade revela não apenas uma limitação pontual da atuação jurisdicional, mas um problema mais amplo de efetividade da própria Lei Geral de Proteção de Dados no cenário brasileiro. Embora a LGPD represente um avanço normativo significativo na proteção dos direitos da personalidade, sua aplicação ainda se mostra insuficiente para conter a recorrência de vazamentos e o uso indevido de dados pessoais.

Isso contribui para a formação de uma percepção social de ineficácia da lei, passando a LGPD a ser vista como uma legislação que “não pegou” ou “para inglês ver”. Ainda que tais afirmações devam ser vistas com cautela, é inegável que a ausência de respostas jurídicas contundentes compromete a confiança dos titulares de dados na capacidade do ordenamento jurídico de proteger efetivamente sua privacidade. Assim, a inefetividade não decorre da ausência de norma, mas da fragilidade de sua concretização.

4.2. A INSUFICIÊNCIA DA RESPOSTA INDENIZATÓRIA TRADICIONAL DIANTE DA FUNÇÃO PUNITIVO-PEDAGÓGICA

A constatação de que a responsabilização civil por vazamento de dados pessoais tem se mostrado limitada, tanto em sua incidência quanto na intensidade das condenações, nos leva à uma análise mais aprofundada acerca do modelo tradicional adotado e da efetividade da lei. É certo que a LGPD estabeleceu um arcabouço normativo robusto, com deveres claros de segurança, prevenção e responsabilização. No entanto, a prática revela que tais comandos não têm sido capazes de produzir alterações significativas no comportamento dos agentes de tratamento.

Essa percepção de inefetividade é reforçada pelos dados de incidentes de segurança da informação no Brasil. Segundo dados do IBM (2025), o custo médio de uma violação de dados no país atingiu R$ 7,19 milhões em 2025, com crescimento anual de 6,5%. Em setores mais sensíveis, como o da saúde, os prejuízos são ainda mais expressivos, alcançando médias superiores a R$ 11 milhões por incidente. Além disso, o tempo médio para detecção e contenção de vazamentos permanece elevado, girando em torno de 276 dias, o que demonstra falhas estruturais na gestão de riscos e na adoção de medidas preventivas.

O cenário agrava-se diante da crescente complexidade tecnológica do tratamento de dados, especialmente com o avanço da inteligência artificial. Estima-se que o uso indevido de sistemas de IA já esteja relacionado a parcela relevante dos incidentes de segurança, ao passo que grande parte das empresas brasileiras ainda não possui políticas estruturadas de governança nessa área.

Nessa toada, é perceptível a discrepância entre o custo real das violações e a resposta jurídica atualmente conferida pelo sistema de responsabilidade civil. Enquanto os danos decorrentes dos vazamentos atingem cifras milionárias e afetam um número expressivo de titulares, as consequências impostas aos agentes de tratamento mostram-se reduzidas e, muitas vezes, incapazes de produzir qualquer efeito dissuasório relevante.

Devido a isso, pode ser mais vantajoso para certas organizações assumir o risco de eventuais condenações judiciais do que investir de forma consistente em segurança da informação e governança de dados. A baixa probabilidade de responsabilização, aliada aos baixos valores fixados, contribui para transformar o ilícito em um custo operacional previsível, esvaziando a função preventiva da responsabilidade civil.

Para inverter essa lógica, é preciso que o ordenamento jurídico brasileiro incorpore mecanismos de natureza punitivo-pedagógica mais incisivos, inspirados, ainda que com as devidas adaptações, no modelo dos *punitive damages* do direito norte-americano. Diferentemente da lógica tradicional brasileira, centrada na recomposição do dano, tais mecanismos têm como finalidade principal

punir condutas especialmente reprováveis e desestimular sua repetição, por meio da imposição de condenações economicamente significativas.

É importante situar que os *punitive damages* operam fundamentalmente no sistema da *common law*, em especial no ordenamento norte-americano, onde a indenização pode superar em muito o valor do dano efetivamente sofrido, com o objetivo expresso de punir o ofensor e dissuadir condutas semelhantes.

A principal crítica à transposição direta dessa figura para o direito brasileiro reside na vedação ao enriquecimento sem causa, consagrada no artigo 944 do Código Civil, segundo o qual a indenização mede-se pela extensão do dano.

A doutrina nacional já debate amplamente essa tensão: autores como Flávio Tartuce (2023) e Cláudia Lima Marques (2019) reconhecem a necessidade de incorporar, com cautela, elementos punitivos à responsabilidade civil brasileira, sobretudo em contextos de danos massificados e condutas reiteradamente negligentes, como os verificados no tratamento inadequado de dados pessoais. Tartuce, em particular, enxerga a utilização do chamado *caráter pedagógico-punitivo* da indenização como forma de compatibilizar a função preventiva da responsabilidade civil com os limites impostos pelo ordenamento pátrio, sem que isso implique transposição mecânica do modelo norte-americano.

A adoção de uma lógica sancionatória mais robusta no âmbito da proteção de dados pessoais poderia contribuir para a efetivação da LGPD, ao tornar o descumprimento de suas normas economicamente desvantajoso.

Contudo, a incorporação de mecanismos dessa natureza deve ser acompanhada de parâmetros claros quanto aos requisitos e limites de sua aplicação ao ordenamento jurídico brasileiro, não sendo possível apenas incorporar o modelo americano. A aplicação deve, ao passo que constrange o agente de tratamento a adotar medidas para mitigar o ilícito, não importar em enriquecimento sem causa ao titular, devendo haver um equilíbrio na fixação das indenizações.

Não obstante tais desafios, a análise desenvolvida ao longo deste trabalho evidencia que o modelo atual de responsabilização civil se mostra insuficiente para assegurar a efetiva proteção dos direitos dos titulares de dados. A recorrência de vazamentos, a baixa incidência de condenações e os valores reduzidos das indenizações indicam a necessidade de repensar os instrumentos disponíveis, de modo a fortalecer a função preventiva e dissuasória da responsabilidade civil.

Por fim, cumpre destacar que fortalecimento da função punitivo-pedagógica na proteção de dados pessoais não deve se limitar à atuação do Poder Judiciário. A efetividade da LGPD depende, igualmente, da atuação firme e estruturada da Autoridade Nacional de Proteção de Dados (ANPD), a quem compete exercer funções fiscalizatórias e sancionatórias no âmbito administrativo.

Nesse viés, é fundamental que a ANPD otimize seus métodos de fiscalização e passe a aplicar, de forma mais consistente e rigorosa, as sanções previstas na legislação, especialmente em casos de falhas reiteradas de segurança e vazamentos de grande impacto. A atuação administrativa é essencial para a efetivação da LGPD, sendo capaz de produzir efeitos mais amplos e rápidos do que a responsabilização individual em demandas judiciais. Sem a efetiva aplicação dessas sanções, o sistema de proteção de dados tende a permanecer desequilibrado, concentrando excessivamente no Judiciário a tarefa de repressão das condutas ilícitas, o que contribui para a manutenção do atual cenário de baixa dissuasão e reduzida efetividade da LGPD.

4.3. O DANO MORAL COLETIVO NA JURISPRUDÊNCIA COMO MECANISMO DE REFORÇO DA EFETIVIDADE DA PROTEÇÃO DE DADOS PESSOAIS

O dano moral coletivo, conceituado anteriormente, também é um instrumento que pode ser aplicado como reforço para efetividade da proteção de dados pessoais no Brasil. A tutela coletiva tem se mostrado especialmente relevante diante da natureza massificada dos vazamentos de dados, os quais, em regra, decorrem de falhas estruturais e atingem simultaneamente diversos titulares.

A jurisprudência brasileira já admite, de forma consolidada, a utilização do dano moral coletivo como resposta a violações que transcendem a esfera individual. O Superior Tribunal de Justiça reconhece que o dano moral coletivo é autônomo e prescinde da comprovação de abalo individual, sendo aferido *in re ipsa* quando há violação relevante a valores fundamentais da coletividade. Esse entendimento é fundamental para o contexto da proteção de dados, em que a exigência de prova individual do dano inviabilizaria a responsabilização em casos de vazamentos massivos.

Nesse sentido, o dano moral coletivo já vem sendo utilizado no ordenamento jurídico brasileiro para casos de vazamentos de dados. Um exemplo disso é a ação civil pública nº 0418456-71.2013.8.19.0001, proposta pelo Ministério Público do Rio de Janeiro, envolvendo o vazamento de dados de clientes de instituições financeiras mantidos por empresas terceirizadas. No caso, os dados permaneceram expostos na internet por período prolongado, evidenciando falha sistêmica de segurança. Como resposta, o Judiciário reconheceu o dano moral coletivo e condenou as empresas envolvidas ao pagamento de R$ 500 mil, além de indenizações individuais aos consumidores. Trata-se de precedente relevante, pois demonstra a responsabilização conjunta de controlador e operador, inclusive com fundamento em falhas de fiscalização e gestão do tratamento de dados.

Além disso, observa-se a crescente utilização de ações civis públicas em casos envolvendo grandes plataformas digitais. A ação proposta pelo Instituto Defesa Coletiva em face da Meta

Platforms, por exemplo, evidencia a tentativa de responsabilização por violações em larga escala relacionadas ao tratamento de dados pessoais de usuários (INSTITUTO DATA PRIVACY BRASIL, 2025)

A utilização do dano moral coletivo, nesse contexto, apresenta uma vantagem significativa em relação à tutela individual, pois possui capacidade de produzir efeitos dissuasórios mais relevantes. Enquanto as indenizações individuais, como demonstrado anteriormente, tendem a ser reduzidas e muitas vezes insuficientes para alterar o comportamento dos agentes econômicos, as condenações coletivas permitem a fixação de valores mais expressivos, compatíveis com a gravidade da conduta e com sua repercussão social.

Todavia, a ausência de consolidação jurisprudencial específica em matéria de LGPD, aliada à dependência da atuação de legitimados coletivos e à morosidade das ações civis públicas, limita a expansão desse instrumento. Ademais, há o risco de utilização restrita apenas a casos de grande repercussão, o que pode comprometer seu potencial preventivo.

Ainda assim, diante do cenário de baixa efetividade da responsabilização individual, o dano moral coletivo se apresenta como um dos mecanismos mais promissores para fortalecer a proteção de dados pessoais no Brasil. Ao permitir uma resposta jurídica mais adequada à dimensão dos danos e à natureza estrutural das falhas de segurança, esse instrumento contribui para a concretização das funções preventiva e punitivo-pedagógica da responsabilidade civil, aproximando a aplicação da LGPD de seus objetivos normativos.

5. CONSIDERAÇÕES FINAIS

Feita essa exposição, é possível inferir que, apesar de existir no ordenamento jurídico brasileiro uma legislação sofisticada e robusta como a Lei Geral de Proteção de Dados Pessoais (LGPD), os vazamentos de dados continuam a crescer, as condenações judiciais permanecem em patamares baixos, incapazes de assumir posição dissuasória e os agentes de tratamento, em grande medida, não adotam de forma consistente as medidas de segurança exigidas pela própria lei.

A análise desenvolvida demonstra que o dever de segurança previsto na LGPD, embora inserido em um sistema normativo mais amplo que inclui o Marco Civil da Internet e o Código de Defesa do Consumidor, tem sido frequentemente descumprido, como indicam os dados recentes sobre o aumento de incidentes de segurança no país.

Nesse contexto, a responsabilidade civil dos agentes de tratamento, prevista no artigo 42 da LGPD, foi examinada como principal instrumento de tutela dos direitos dos titulares, destacando-se

a tendência doutrinária e jurisprudencial de adoção da responsabilidade objetiva, especialmente em casos envolvendo dados sensíveis ou relações de consumo, com base na teoria do risco da atividade.

Quanto ao dano moral, verificou-se uma oscilação jurisprudencial relevante, ora exigindo prova concreta do prejuízo, ora admitindo sua presunção, especialmente em casos de dados sensíveis. Na prática, essa exigência de prova pode dificultar a proteção dos titulares, diante da desigualdade de informações que caracteriza as relações de tratamento de dados. A análise empírica realizada confirma que o modelo atual de responsabilização possui baixa capacidade dissuasória, uma vez que os valores das indenizações são, em geral, reduzidos e desproporcionais em relação aos prejuízos causados pelos vazamentos, o que pode levar à internalização do ilícito como custo operacional pelas organizações.

Assim, o problema da efetividade da LGPD não decorre da ausência de normas, mas da insuficiência das respostas judiciais e administrativas, que ainda não são capazes de alterar de forma significativa o comportamento dos agentes de tratamento.

A responsabilidade civil, nesse cenário, deve ser compreendida não apenas como mecanismo de reparação, mas também como instrumento de prevenção, capaz de induzir a adoção de medidas adequadas de governança e segurança da informação.

Para que essa função seja efetivamente desempenhada, é necessário um aprimoramento consistente do modelo de responsabilização. A ampliação do reconhecimento do dano moral presumido em hipóteses de vazamento decorrente de falha de segurança mostra-se medida compatível com a lógica protetiva da LGPD, uma vez que reduz os obstáculos probatórios enfrentados pelo titular e reconhece que a própria violação do dever de segurança já configura lesão.

Paralelamente, é preciso que seja feita uma revisão dos critérios de fixação do quantum indenizatório, de modo a incorporar de forma mais clara a função punitivo-pedagógica da responsabilidade civil, considerando a gravidade da conduta, a extensão do dano, o número de titulares afetados e, sobretudo, a capacidade econômica do agente de tratamento, evitando que a condenação seja absorvida como custo ordinário da atividade.

Além disso, revela-se indispensável o fortalecimento da atuação sancionatória da Autoridade Nacional de Proteção de Dados, com a aplicação mais frequente, transparente e proporcional das sanções administrativas previstas na LGPD, especialmente em casos de falhas estruturais ou vazamentos de grande escala.

A articulação entre a responsabilização judicial e a atuação administrativa deve ser compreendida como complementar, de modo a produzir efeitos não apenas reparatórios, mas também preventivos. Nesse mesmo sentido, o reconhecimento e a utilização do dano moral coletivo contribuem

para enfrentar a dimensão massificada dos vazamentos de dados, permitindo respostas mais adequadas à gravidade social das violações e potencializando o efeito dissuasório das decisões.

Conclui-se, portanto, que a LGPD não é uma lei meramente simbólica, contudo, sua efetividade depende da aplicação mais rigorosa e consistente de seus mecanismos de responsabilização, sendo a responsabilidade civil um elemento central para tornar o descumprimento das normas de proteção de dados juridicamente e economicamente desvantajoso.

REFERÊNCIAS

ALAGOAS. Tribunal de Justiça do Estado de Alagoas. **Apelação Cível nº 0701717-79.2024.8.02.0051**. Relator: Des. Márcio Roberto Tenório de Albuquerque. Data de Julgamento: 28/08/2025. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-al/4608654404. Acesso em: 01 maio 2026.

AMER, Karim; NOUJAIM, Jehane (dir.). **Privacidade Hackeada** [The Great Hack]. Produção: Netflix. EUA, 2019. 1h 54min.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte.** Versão 1.0. Brasília: ANPD, out. 2021. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-vf.pdf. Acesso em: 28 abr. 2026.

BRASIL. Gabinete de Segurança Institucional. Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov). **CTIR Gov em Números**. Brasília: GSI/PR, 2026. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros. Acesso em: 21 maio 2026.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 abr. 2026.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o **Código Civil**. Diário Oficial da União, Brasília, DF, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 28 abr. 2026.

BRASIL. Lei nº 7.347, de 24 de julho de 1985. Disciplina a ação civil pública de responsabilidade por danos causados ao meio-ambiente... [ementa]. Brasília, DF, 24 jul. 1985. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm. Acesso em: 10 abr. 2026.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 10 abr 2026.

BRASIL. Superior Tribunal de Justiça (3. Turma). **Recurso Especial nº 2.132.043/SP**. Relatora: Ministra Nancy Andrighi, 3 de setembro de 2024. Disponível em: stj.jus.br. Acesso em: 20 abril 2026.

BRASIL. Superior Tribunal de Justiça (3. Turma). **Recurso Especial nº 2.132.043/SP**. Relatora: Ministra Nancy Andrighi, 3 de setembro de 2024. Disponível em: stj.jus.br. Acesso em: 20 maio 2026.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.152.541/RS**. Relator: Min. Paulo de Tarso San Severino, julgado em 13/09/2011.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2.117.561/SP**. Relator: Ministro Humberto Martins. Data de Julgamento: 10/11/2025. DJEN, 13/11/2025. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/94caa4d6-f510-4fcc-b499-a4bdedd72bcc. Acesso em: 01 maio 2026.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2.121.904/SP**. Relatora: Ministra Nancy Andrighi. Data de Julgamento: 11/02/2025. DJEN, 17/02/2025. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/3306714629. Acesso em: 01 maio 2026.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2.147.374/SP**. Relator: Ministro Ricardo Villas Bôas Cueva. Data de Julgamento: 03/12/2024. DJEN, 06/12/2024.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2.187.854/SP**. Relatora: Ministra Nancy Andrighi. Data de Julgamento: 06/05/2025. DJEN, 13/05/2025. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/3737380215. Acesso em: 01 maio 2026.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2.221.650/SP**. Relatora: Ministra Maria Isabel Gallotti. Data de Julgamento: 04/11/2025. DJEN, 14/11/2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2.222.983/SP.** Relator: Ministro Humberto Martins. Data de Julgamento: 02/03/2026. DJEN, 05/03/2026. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/e11b5b6b-c9dc-4637-a5ea-83d86ff0d6b6. Acesso em: 01 maio 2026.

BRASIL. [Código de Processo Civil (2015)]. Lei nº 13.105, de 16 de março de 2015. **Código de Processo Civil.** Brasília, DF: Senado Federal, 2015. Disponível em: planalto.gov.br. Acesso em: 3 maio 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.** Brasília, DF: Presidência da República, [abril 2014]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 mar 2026.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [1988]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 28 abr. 2026.

CAPANEMA, Walter Aranha. **A responsabilidade civil na Lei Geral de Proteção de Dados.** São Paulo: Cadernos Jurídicos, ano 21, nº 53, p. 163-170, 2020.

CASTELLS, Manuel. **The Rise of the Network Society**. 2. ed. Oxford/West Sussex: Wiley-Blackwell, 2010. (The information age: economy, society, and culture, v. 1).

CONSULTOR JURÍDICO. **Decisão do STJ sobre dano moral em proteção de dados afeta crédito.** ConJur, 16 set. 2025. Disponível em: https://www.conjur.com.br/2025-set-16/decisao-do-stj-sobre-dano-moral-em-protecao-de-dados-afeta-credito/. Acesso em: 28 abr. 2026.

DINIZ, Nathalie Pagni. **Dano moral coletivo – uma análise sob o enfoque da LGPD**. Migalhas, 7 maio 2024. Disponível em: https://www.migalhas.com.br/depeso/406713/dano-moral-coletivo--uma-analise-sob-o-enfoque-da-lgpd. Acesso em: 28 abr. 2026.

DISTRITO FEDERAL. Tribunal de Justiça do Distrito Federal e dos Territórios. **Recurso Inominado nº 0715047-16.2024.8.07.0016.** Relatora: Marilia de Avila e Silva Sampaio. Data de Julgamento: 07/10/2024. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-df/2795810482. Acesso em: 01 maio 2026.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

FEDERIGHI, André Catta Preta; CATTA PRETA, Suzana. **Virada na jurisprudência de responsabilidade em proteção de dados?** JOTA, 24 set. 2025. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/virada-na-jurisprudencia-de-responsabilidade-em-protecao-de-dados. Acesso em: 20 abril 2026.

IBM SECURITY. **Cost of a Data Breach Report 2025**. Disponível em: https://brasil.newsroom.ibm.com/2025-07-30-Relatorio-da-IBM-Custo-medio-de-uma-violacao-de-dados-no-Brasil-atinge-R-7,19-milhoes. Acesso em: 28 abr. 2026.

INSTITUTO DATA PRIVACY BRASIL. **A ação civil pública do Instituto Defesa Coletiva contra a Meta: entrevista com Lilian Salgado**. Data Privacy Brasil, 2025. Disponível em: https://www.dataprivacybr.org/a-acao-civil-publica-do-instituto-defesa-coletiva-contra-a-meta-entrevista-com-lilian-salgado/. Acesso em: 28 abr. 2026.

MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais**. 9. ed. São Paulo: Revista dos Tribunais, 2019.

MEDEIROS NETO, Xisto Tiago de. **Dano moral coletivo**. 3. ed. São Paulo: LTr, 2012.

MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (coord.); BIONI, Bruno Ricardo (org.). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021.

MINAS GERAIS. Tribunal de Justiça do Estado de Minas Gerais. **Apelação Cível nº 1.0000.24.174731-0/001**. Relator para o acórdão: Des. Newton Teixeira Carvalho. Data de Julgamento: 05/06/2025. 13ª Câmara Cível.

ONU – ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Paris, 1948. Disponível em: http://www.un.org/en/universaldeclaration-human-rights/. Acesso em: 10 fev. 2026.

PARANÁ. Tribunal de Justiça do Estado do Paraná. **Apelação Cível nº 0026395-97.2022.8.16.0014**. Relator: Iraja Pigatto Ribeiro. Data de Julgamento: 12/08/2024. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-pr/2895649411. Acesso em: 01 maio 2026.

PARANÁ. Tribunal de Justiça do Estado do Paraná. **Apelação Cível nº 0054597-84.2022.8.16.0014**. Relator: Fabio Andre Santos Muniz. Data de Julgamento: 14/08/2024. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-pr/2895623139. Acesso em: 01 maio 2026.

PERNAMBUCO. Tribunal de Justiça do Estado de Pernambuco. **Apelação Cível nº 0013999-64.2024.8.17.2480**. Relator: Luciano de Castro Campos. Data de Julgamento: 16/04/2025. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-pe/3481554687. Acesso em: 01 maio 2026.

REDAÇÃO. **Disponibilização não autorizada de dados pessoais não gera dano moral presumido, decide STJ.** JuriNews, 14 fev. 2026. Disponível em: https://jurinews.com.br/destaque-nacional/disponibilizacao-nao-autorizada-de-dados-pessoais-nao-gera-dano-moral-presumido-decide-stj. Acesso em: 28 abr. 2026.

RIO DE JANEIRO. Tribunal de Justiça do Estado do Rio de Janeiro. **Apelação Cível nº 0418456-71.2013.8.19.0001**. Relator: Des. Fabio Dutra. Data de Julgamento: 23/02/2021. Décima Câmara de Direito Privado. Data de Publicação: 10/03/2021.

RIO DE JANEIRO. Tribunal de Justiça do Estado do Rio de Janeiro. **Apelação Cível nº 0804433-67.2023.8.19.0207**. Relator: Des. José Carlos Paes. Data de Julgamento: 23/07/2025. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-rj/4294808494. Acesso em: 01 maio 2026.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Organização e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RUIZ, Matheus Cordeiro. **O direito fundamental à proteção de dados pessoais no Brasil: desafios e perspectivas para a efetivação da LGPD.** Revista FT, v. 29, ed. 146, maio 2025. Disponível em: https://revistaft.com.br/o-direito-fundamental-a-protecao-de-dados-pessoais-no-brasil-desafios-e-perspectivas-para-a-efetivacao-da-lgpd/. Acesso em: 28 abr. 2026.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Apelação Cível nº 1001283-62.2022.8.26.0457**. Relator: Alexandre Coelho. Data de Julgamento: 30/08/2024. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2699612149. Acesso em: 01 maio 2026.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Apelação Cível nº 1001438-40.2025.8.26.0011**. Relator: Olavo Paula Leite Rocha. Data de Julgamento: 29/09/2025. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/5011302961. Acesso em: 01 maio 2026.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Apelação Cível nº 1008008-78.2023.8.26.0248**. Relator: Domingos de Siqueira Frascino. Data de Julgamento: 10/10/2024. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2783493373. Acesso em: 01 maio 2026.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Apelação Cível nº 1011977-87.2022.8.26.0361**. Relator: Mendes Pereira. Data de Julgamento: 16/09/2024. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2739845175. Acesso em: 01 maio 2026.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Apelação Cível nº 1025549-54.2021.8.26.0100.** Relatora: Maria Lúcia Pizzotti. Data de Julgamento: 08/03/2023. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2490795503. Acesso em: 01 maio 2026.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Recurso Inominado Cível nº 1008787-17.2023.8.26.0609**. Relatora: Tonia Yuka Koroku. Data de Julgamento: 24/10/2024. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2809687975. Acesso em: 01 maio 2026.

SARLET, Ingo Wolfgang. **Fundamentos constitucionais: o direito fundamental à proteção de dados.** In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (coord.); BIONI, Bruno Ricardo (org.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021, p. 21-59.

SILVA, Wilson Melo da. **O dano moral e sua reparação.** 3. ed. rev. e atual. Rio de Janeiro: Forense, 1999.

TARTUCE, Flávio. **Manual de direito civil: volume único.** 13. ed. Rio de Janeiro: Forense, 2023.

TARTUCE, Flavio. NEVES, Daniel Amorim Assumpção. **Manual de Direito do Consumidor: direito material e processual.** 12. ed. Rio de Janeiro: Método, 2023.

TARTUCE, Flavio. **Direito Civil: direito das obrigações e responsabilidade civil.** 16. ed. Rio de Janeiro: Forense, 2021.

LEMOS, Vinicius Silva; ROCHA, Madson. **Responsabilidade civil por vazamento de dados: o que nos ensina o REsp 2.147.374-SP?** Migalhas, 29 maio 2025. Disponível em: https://www.migalhas.com.br/depeso/431249/responsabilidade-civil-por-dados-vazados-resp-2-147-374-sp. Acesso em: 28 abr. 2026.

TEMER, Thaís; ASPERTI, Maria Cecília de Araújo. **Dano moral coletivo no Brasil: parâmetros para adequada quantificação e destinação dos valores.** Civilistica.com, Rio de Janeiro, a. 13, n. 2, 2024. Disponível em: https://civilistica.emnuvens.com.br/redc. Acesso em: 28 abr. 2026.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (General Data Protection Regulation – GDPR).** Jornal Oficial da União Europeia, L 119, 4 maio 2016. Disponível em: https://gdpr-info.eu. Acesso em: 27 abr. 2026.

VILELA, Maria Eduarda Marçal; GIOLO JÚNIOR, Cildo. **Lei geral de proteção de dados (LGPD) e general data protection regulation (GDPR): uma análise entre os principais elementos das legislações e suas sanções aos casos de vazamento de dados.** Revista de Iniciação Científica e Extensão da Faculdade de Direito de Franca, Franca, v. 8, n. 1, p. 637–661, dez. 2023. Disponível em: https://www.revista.direitofranca.br/index.php/icfdf/article/view/1516. Acesso em: 03 maio 2026.