REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

# VAZAMENTO DE DADOS PESSOAIS E DANO MORAL: A DIVERGÊNCIA NO STJ E CRITÉRIOS PARA A AFERIÇÃO DO DANO

****PERSONAL DATA BREACHES AND MORAL DAMAGES: JURISPRUDENTIAL DIVERGENCE WITHIN THE BRAZILIAN SUPERIOR COURT OF JUSTICE (STJ) AND CRITERIA FOR ASSESSING DAMAGES****

Ciências Humanas, Ciências Sociais Aplicadas • 10/11/2026

REGISTRO DOI: 10.70773/revistatopicos/794198669

Ketelyn Lorrainy Bastos Rodrigues[1]

Gabriela Calixto Peres[2]

**RESUMO**

Objetiva-se analisar a natureza do dano indenizável em situações de vazamento de dados pessoais e de compartilhamento de informações sem base legal, distinguindo-se essas hipóteses quanto à origem da conduta e aos efeitos produzidos. A pesquisa adota abordagem qualitativa, com raciocínio dedutivo na análise normativa e indutivo no exame jurisprudencial, mediante revisão bibliográfica, documental e jurisprudencial. O corpus é composto por seis julgados do Superior Tribunal de Justiça, proferidos entre 2023 e 2026, selecionados a partir de pesquisa na base jurisprudencial do Tribunal com os termos “vazamento de dados” e “dano moral”, bem como “LGPD” e “dano presumido”. Verificou-se que a Segunda Turma afasta o dano moral presumido em vazamentos de dados comuns, enquanto a Terceira Turma reconhece a presunção em hipóteses envolvendo dados sensíveis e disponibilização indevida de dados cadastrais. A divergência quanto à disponibilização de dados por gestores de bancos de dados de proteção ao crédito foi afetada ao Tema 1.404 do STJ, ainda pendente de julgamento. Conclui-se que a natureza e o volume dos dados expostos, o contexto da relação jurídica, a origem do incidente, o uso efetivo ou o risco concreto de utilização das informações e a conduta posterior do agente de tratamento devem ser analisados conjuntamente.

**Palavras-chave:** Proteção de dados pessoais; Vazamento de dados; Dano moral; Dano in re ipsa; Superior Tribunal de Justiça.

**ABSTRACT**

This article aims to analyze the nature of compensable damage in cases involving personal data breaches and the unlawful sharing of personal information, distinguishing these situations according to the origin of the conduct and the effects produced. The research

adopts a qualitative approach, combining deductive reasoning in the normative analysis with inductive reasoning in the examination of case law, based on bibliographical, documentary and jurisprudential research. The corpus consists of six decisions issued by the Brazilian Superior Court of Justice between 2023 and 2026, selected through searches in the Court's jurisprudence database using the terms "data breach" and "moral damage", as well as "LGPD" and "presumed damage". The analysis shows that the Second Panel rejects presumed non-pecuniary damage in cases involving ordinary personal data breaches, whereas the Third Panel has recognized such presumption in cases involving sensitive data and unlawful disclosure of personal information. The divergence concerning the disclosure of data by credit bureau database managers has been submitted to Theme 1,404 of the Superior Court of Justice, which remains pending judgment. It is concluded that the nature and volume of the exposed data, the context of the legal relationship, the origin of the incident, the actual misuse or concrete risk of misuse of the information, and the controller's subsequent conduct must be assessed jointly.
**Keywords:** Personal data protection; Data breach; Non-pecuniary damage; In re ipsa damage; Superior Court of Justice.

## 1. INTRODUÇÃO

A divulgação de notícias sobre invasões de sistemas e exposição de informações pessoais tornou-se frequente na vida cotidiana. Nome, CPF, endereço, telefone, dados de consumo e, em determinadas situações, informações de saúde ou financeiras podem deixar o ambiente em que foram fornecidos e passar a circular sem o controle do titular. O problema jurídico não se limita, portanto, à

ocorrência do incidente, mas alcança as consequências que dele podem decorrer para a pessoa afetada.

A resposta do ordenamento jurídico brasileiro foi construída de forma progressiva. A Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), disciplinou o tratamento de dados e estabeleceu, nos arts. 42 a 45, regras próprias de responsabilidade civil dos agentes de tratamento. Em maio de 2020, ao referendar a medida cautelar na ADI 6.387, o Supremo Tribunal Federal reconheceu a proteção de dados pessoais como direito fundamental autônomo. Em 2022, a Emenda Constitucional nº 115 incorporou expressamente esse direito ao art. 5º, inciso LXXIX, da Constituição Federal (BRASIL, 1988; BRASIL, 2022).

Apesar desse avanço normativo, permanece uma questão relevante para as demandas decorrentes da exposição indevida de dados: qual dano deve ser reparado? O art. 42 da LGPD prevê a responsabilidade por dano patrimonial ou moral causado em violação à legislação, mas não estabelece, de forma expressa, se a exposição indevida dos dados basta para caracterizar a lesão ou se o titular deve demonstrar alguma consequência concreta, como fraude, golpe ou repercussão comprovada em sua esfera pessoal.

A jurisprudência do Superior Tribunal de Justiça ainda não apresenta orientação uniforme. Em 2023, a Segunda Turma, no AREsp 2.130.619/SP, entendeu que o vazamento de dados pessoais comuns não gera, por si só, dano moral presumido. Entre 2024 e 2025, a Terceira Turma admitiu o dano presumido em situações envolvendo dados sensíveis (REsp 2.121.904/SP) e disponibilização de informações cadastrais a terceiros sem base legal (REsp 2.133.261/SP e REsp 2.201.694/SP). Em novembro de 2025, a Quarta Turma, no

REsp 2.221.650/SP, afastou a presunção em hipótese semelhante à julgada pela Terceira Turma. Diante da divergência, a Segunda Seção afetou ao rito dos recursos repetitivos a controvérsia relativa à disponibilização de dados por gestores de bancos de dados de proteção ao crédito (Tema 1.404), ainda pendente de julgamento.

Convém delimitar o objeto. O estudo abrange duas hipóteses de exposição indevida de dados pessoais: o vazamento decorrente de incidente de segurança, em que terceiros acessam as informações sem autorização, e a disponibilização ou o compartilhamento de dados sem base legal, praticados voluntariamente pelo próprio agente de tratamento. As situações não são idênticas, e a diferença entre elas é incorporada à proposta da seção 6 como critério autônomo. São, porém, comparáveis para os fins desta pesquisa por três razões. Ambas configuram tratamento irregular à luz da LGPD, que inclui a comunicação, a difusão e a transferência no conceito de tratamento (art. 5º, X) e exige proteção contra situações acidentais ou ilícitas de comunicação ou difusão (art. 46). Em ambas, a consequência para o titular é a mesma: a perda do controle sobre informações que lhe dizem respeito. E o próprio STJ as trata como parte de uma mesma linha de precedentes: a Quarta Turma, ao julgar caso de disponibilização de dados por gestor de banco de dados, invocou como fundamento o AREsp 2.130.619/SP, que versava sobre vazamento (BRASIL, 2025c), e a Terceira Turma, ao examinar o vazamento de dados de segurado, apoiou-se em precedente sobre disponibilização indevida por banco de dados (BRASIL, 2025a).

A discussão possui relevância prática e jurídica. Os incidentes de segurança podem atingir grande número de titulares e, em determinadas circunstâncias, facilitar fraudes e outras formas de uso indevido das informações. Ao mesmo tempo, a falta de

uniformidade entre os julgados pode produzir decisões diferentes em situações semelhantes. O desafio consiste em evitar, de um lado, a transformação automática de qualquer exposição de dados em dano moral e, de outro, a desconsideração dos riscos efetivamente impostos ao titular.

Diante desse cenário, o problema de pesquisa pode ser formulado nos seguintes termos: a exposição indevida de dados pessoais, por si só, configura dano moral indenizável ou a reparação depende da demonstração de prejuízo concreto pelo titular? A distinção entre dados comuns e sensíveis, utilizada em parte da jurisprudência, é suficiente para solucionar essa questão?

A hipótese adotada é a de que a violação da proteção de dados pode, em determinadas circunstâncias, justificar a presunção do dano extrapatrimonial, mas que essa conclusão não deve decorrer exclusivamente da classificação legal do dado. A aferição deve considerar cinco critérios combinados: a natureza e volume dos dados expostos; o contexto e finalidade da relação jurídica; a origem do incidente; o uso efetivo ou risco concreto de uso dos dados; e a conduta do agente de tratamento após o incidente.

O objetivo geral é analisar a natureza do dano indenizável decorrente da exposição indevida de dados pessoais à luz da LGPD, da Constituição Federal e da jurisprudência do Superior Tribunal de Justiça. Especificamente, busca-se situar a proteção de dados pessoais como direito fundamental autônomo (seção 2); examinar o regime de responsabilidade civil dos arts. 42 a 45 da LGPD e seu diálogo com o Código de Defesa do Consumidor (seção 3); distinguir o dano moral presumido do dano que exige prova de prejuízo (seção 4); comparar os fundamentos dos precedentes da Segunda, da

Terceira e da Quarta Turma do STJ (seção 5); e propor critérios para a aferição do dano indenizável (seção 6).

A pesquisa é qualitativa e combina procedimentos bibliográfico, documental e jurisprudencial. Na parte teórica, adota-se raciocínio dedutivo, partindo das normas constitucionais e legais e da doutrina sobre proteção de dados e responsabilidade civil. Na análise das decisões, o raciocínio é indutivo: os critérios propostos na seção 6 foram extraídos da comparação entre os casos, e não deduzidos de uma premissa prévia. A pesquisa documental abrangeu a Constituição Federal, a LGPD, o Código de Defesa do Consumidor, a Lei nº 12.414/2011 (Lei do Cadastro Positivo) e a Resolução CD/ANPD nº 15/2024.

O exame jurisprudencial foi realizado com base nas decisões do Superior Tribunal de Justiça, utilizando-se os termos “vazamento de dados” e “dano moral”, bem como “LGPD” e “dano presumido”. Foram considerados julgados publicados entre 2023 e 2026, incluídos aqueles que examinassem: a natureza dos dados tratados; a origem do incidente; a existência ou não de fundamento legal para o tratamento; a responsabilidade do agente; e a exigência ou dispensa de comprovação do dano. Foram excluídas decisões sem exame efetivo da responsabilidade civil, julgados que tratassem exclusivamente de matéria processual e decisões sem relação direta com vazamento, compartilhamento indevido ou disponibilização de dados pessoais. Ao final, foram selecionados seis julgados principais, complementados por precedente anterior da Terceira Turma (REsp 1.758.799/MG), que antecede a orientação examinada, e pela afetação do Tema 1.404 do STJ.

O artigo está organizado em cinco seções de desenvolvimento, além desta introdução e das considerações finais. A seção 2 situa a proteção de dados pessoais como direito fundamental autônomo; a seção 3 examina o regime de responsabilidade civil da LGPD e seu diálogo com o Código de Defesa do Consumidor; a seção 4 discute as concepções de dano moral e a experiência do Tribunal de Justiça da União Europeia; a seção 5 analisa os precedentes do Superior Tribunal de Justiça e a afetação do Tema 1.404; e a seção 6 propõe critérios para a aferição do dano indenizável.

## 2. A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL AUTÔNOMO

### 2.1. Da Privacidade à Autodeterminação Informativa

Compreender o dano que decorre da exposição indevida de dados exige, antes, identificar o bem jurídico atingido. Se os dados pessoais forem tratados apenas como extensão da intimidade, o vazamento de informações banais, como nome e telefone, dificilmente seria lesivo. Se, ao contrário, se reconhecer um direito autônomo ao controle sobre as próprias informações, a análise muda de figura.

A tutela tradicional da privacidade foi construída em torno da ideia de segredo: protegia-se aquilo que a pessoa desejava manter longe do olhar alheio. Esse modelo mostrou-se insuficiente diante do tratamento automatizado de grandes volumes de informação. Doneda (2006) demonstra que a informatização deslocou o eixo da tutela do resguardo da vida íntima para o controle sobre a circulação das informações pessoais, e Rodotà (2008) descreve a privacidade contemporânea como o direito de manter o controle sobre as próprias informações. A expressão autodeterminação informativa

tem origem no julgamento da lei do recenseamento pelo Tribunal Constitucional Federal alemão, em 1983, que afirmou não existirem, nas condições do processamento automatizado, dados insignificantes (ALEMANHA, 1983). No Brasil, Mendes (2014) sustentou, antes da LGPD, a existência de um novo direito fundamental à proteção de dados, articulado à defesa do consumidor.

A LGPD incorporou essa mudança de perspectiva. Entre os fundamentos da disciplina, o art. 2º arrola, ao lado do respeito à privacidade, a autodeterminação informativa, a inviolabilidade da intimidade, da honra e da imagem, e o livre desenvolvimento da personalidade (BRASIL, 2018). O art. 17, por sua vez, assegura a toda pessoa natural a titularidade de seus dados pessoais. A lei protege, portanto, não só o conteúdo da informação, mas o poder do titular de decidir quem a trata, para quê e por quanto tempo.

Dessa premissa decorre uma consequência importante para o tema deste estudo: a proteção alcança também os chamados dados comuns. O art. 5º, inciso I, da LGPD define dado pessoal como qualquer informação relacionada a pessoa natural identificada ou identificável, sem exigir que ela seja íntima ou sigilosa. A categoria dos dados sensíveis (art. 5º, II) recebe proteção reforçada, mas não esgota o campo de tutela.

Parte da doutrina critica, inclusive, a rigidez da divisão entre dados comuns e sensíveis. Para Rodotà (2008, p. 56), dados aparentemente não sensíveis podem tornar-se sensíveis quando contribuem para a elaboração de um perfil. Bioni (2019) observa que um dado trivial pode converter-se em sensível quando correlacionado a outros por tecnologias de análise em larga escala, e Mulholland (2020) propõe

que o conceito de dado sensível seja funcionalizado de acordo com o uso que dele se faz e com seu potencial discriminatório. Na mesma linha, Konder (2019) sustenta que a qualificação de um dado como sensível não pode ser feita em abstrato, devendo-se verificar em concreto seu potencial de estigmatização ou discriminação, crítica que Couto (2023, p. 176) aplica ao AREsp 2.130.619/SP. A mesma obra de Konder, contudo, foi invocada pela Quarta Turma do STJ para justificar o tratamento diferenciado entre dados sensíveis e comuns (BRASIL, 2025c), o que mostra que a categoria legal admite leituras opostas. Essa observação será retomada na análise da jurisprudência.

### 2.2. A ADI 6.387 e a Emenda Constitucional N° 115/2022

O reconhecimento constitucional da proteção de dados veio primeiro pela via jurisprudencial. Em abril de 2020, a Medida Provisória nº 954 determinou que as empresas de telefonia compartilhassem com o Instituto Brasileiro de Geografia e Estatística (IBGE) os nomes, números de telefone e endereços de seus consumidores. A Ordem dos Advogados do Brasil e diversos partidos políticos ajuizaram ações diretas de inconstitucionalidade, e a relatora, Ministra Rosa Weber, suspendeu liminarmente a eficácia da medida.

Nos dias 6 e 7 de maio de 2020, o Plenário referendou a cautelar na ADI 6.387, julgada em conjunto com as ADIs 6.388, 6.389, 6.390 e 6.393 (BRASIL, 2020). A Corte reconheceu, naquela oportunidade, um direito fundamental autônomo e implicitamente positivado à proteção de dados pessoais, reconduzindo-o à dignidade da pessoa humana, ao livre desenvolvimento da personalidade e à autodeterminação informativa (Sarlet, 2021). Chama atenção, para os

fins deste estudo, que os dados em discussão eram justamente dados cadastrais comuns. O Supremo não exigiu que fossem íntimos para que sua circulação indevida fosse considerada lesiva a direitos fundamentais.

A Emenda Constitucional nº 115, de 10 de fevereiro de 2022, consolidou esse entendimento ao acrescentar ao art. 5º o inciso LXXIX, segundo o qual "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (BRASIL, 2022). Com a positivação, esse direito passou a gozar do regime reforçado dos direitos fundamentais, incluídas a aplicabilidade imediata e a condição de cláusula pétrea (Sarlet, 2021).

O reconhecimento de um direito fundamental autônomo não resolve, por si, a questão do dano indenizável, mas desloca o ponto de partida. Se a exposição indevida atinge um direito fundamental, a afirmação de que se trata de mero aborrecimento precisa ser justificada, e não apenas presumida.

## 3. A RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO NA LGPD

### 3.1. O Regime de Responsabilidade Civil dos Arts. 42 a 45 da LGPD

A LGPD dedicou uma seção específica à responsabilidade e ao ressarcimento de danos. A redação escolhida pelo legislador, porém, gerou um dos debates mais intensos da doutrina nacional sobre a lei: saber se o regime adotado é subjetivo, objetivo ou algo distinto de ambos. O dispositivo central é o art. 42, cuja redação convém transcrever:

> *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. (BRASIL, 2018).*

O artigo exige, portanto, três elementos: o exercício de atividade de tratamento, a violação à legislação de proteção de dados e o dano. O § 2º autoriza o juiz a inverter o ônus da prova em favor do titular quando a alegação for verossímil, houver hipossuficiência ou a produção da prova lhe for excessivamente onerosa. O art. 43 enumera as hipóteses em que os agentes de tratamento não serão responsabilizados: quando provarem que não realizaram o tratamento, que não houve violação à legislação ou que o dano decorreu de culpa exclusiva do titular ou de terceiro.

O art. 44, por sua vez, define o tratamento irregular como aquele que deixa de observar a legislação ou "não fornecer a segurança que o titular dele pode esperar", consideradas circunstâncias como o modo de realização, os riscos razoavelmente esperados e as técnicas disponíveis à época (BRASIL, 2018). Seu parágrafo único atribui responsabilidade pelos danos decorrentes da violação da segurança ao agente que deixar de adotar as medidas previstas no art. 46. Finalmente, o art. 45 dispõe que as violações ocorridas no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade da legislação pertinente.

A ausência de expressões como "independentemente de culpa" levou parte da doutrina a sustentar que a LGPD adotou a responsabilidade subjetiva. Guedes e Meireles (2019) defendem essa

leitura com base na exigência de violação à lei, na excludente do art. 43, II, que permite ao agente provar que observou o padrão de conduta exigido, e no conjunto de deveres de segurança e boas práticas dos arts. 46 a 54, que funcionariam como parâmetros de culpa normativa. Em sentido oposto, Mendes e Doneda (2018) partem do risco intrínseco à atividade de tratamento de dados, e Mulholland (2020) conclui que o art. 42 impõe a obrigação de indenizar independentemente da análise da culpa, situando os incidentes de segurança como fortuito interno. Moraes e Queiroz (2019) propõem uma terceira leitura, de responsabilização proativa, centrada no dever de prevenção e de prestação de contas.

O histórico legislativo reforça a primeira leitura. Bioni e Dias (2020) demonstram que tanto a primeira versão do anteprojeto quanto a proposta do Senado previam expressamente a responsabilidade objetiva, qualificando o tratamento de dados como atividade de risco ou impondo o dever de reparar independentemente de culpa. Essas expressões foram suprimidas no curso da tramitação, o que indica uma opção deliberada do legislador.

Os mesmos autores, contudo, advertem que a discussão binária perde de vista o essencial. A combinação entre a presunção de violação que decorre do art. 43, a possibilidade de inversão do ônus da prova e o padrão de segurança esperada do art. 44 torna extremamente difícil ao agente afastar sua responsabilidade. O resultado, para Bioni e Dias (2020), seria um regime de responsabilidade civil subjetiva dotado de alto grau de objetividade. Moraes (2019, p. 6) identifica na lei um sistema de responsabilização proativa, fundado no princípio da prestação de contas (art. 6º, X), que não seria “nem subjetivo nem objetivo” e que privilegia a prevenção do dano.

Para o tema deste trabalho, o ponto relevante é que nenhuma das correntes dispensa o dano. Seja subjetiva, objetiva ou proativa, a responsabilidade civil prevista no art. 42 pressupõe a existência de um prejuízo patrimonial ou moral. O debate sobre a culpa, portanto, não resolve a pergunta sobre o que conta como dano quando os dados são indevidamente expostos.

### 3.2. O Diálogo com o Código de Defesa do Consumidor

Grande parte dos incidentes ocorre em relações de consumo: bancos, operadoras de telefonia, lojas virtuais, concessionárias de serviço público, seguradoras e bancos de dados de proteção ao crédito. Nesses casos, o art. 45 da LGPD remete expressamente às regras de responsabilidade da legislação pertinente, o que atrai a incidência do art. 14 do Código de Defesa do Consumidor. Segundo esse dispositivo, o fornecedor de serviços responde, independentemente de culpa, pelos danos causados por defeitos na prestação, considerando-se defeituoso o serviço que não fornece a segurança que o consumidor dele pode esperar (BRASIL, 1990).

Bioni e Dias (2020) chamam atenção para a semelhança textual entre o art. 44 da LGPD e o art. 14, § 1º, do CDC: os três incisos que orientam a aferição da segurança esperada foram praticamente transpostos de um diploma para o outro. Essa proximidade facilita o diálogo entre as fontes e explica por que a jurisprudência, nas relações de consumo, tem aplicado a responsabilidade objetiva aos vazamentos.

Foi o que fez a Terceira Turma do STJ no REsp 2.121.904/SP, ao reconhecer, em contrato de seguro de vida, a responsabilidade objetiva da seguradora pelo vazamento de dados do segurado

(BRASIL, 2025a). No mesmo sentido, no REsp 2.147.374/SP, a Turma rejeitou a alegação de culpa exclusiva de terceiro em caso de ataque hacker, por não ter sido comprovada a excludente do art. 43, III, e invocou a expectativa legítima de proteção do titular (BRASIL, 2024b).

Nas relações de consumo, portanto, a discussão sobre a culpa tende a perder importância prática. O ponto de atrito se desloca para o dano: provada a exposição e afastada a excludente, resta saber se o consumidor precisa demonstrar algum prejuízo além da própria exposição de seus dados.

## 4. O DANO MORAL NO VAZAMENTO DE DADOS: PRESUNÇÃO OU PROVA

### 4.1. Dano Moral *In Re Ipsa* ou Dano-Prejuízo

A controvérsia sobre a exposição indevida de dados é, no fundo, uma controvérsia sobre o conceito de dano moral. A resposta à pergunta sobre se o vazamento gera dano presumido depende de como se compreende aquilo que o dano moral protege.

Duas concepções disputam o espaço na doutrina brasileira. A primeira, mais antiga, identifica o dano moral com a dor, o sofrimento, a angústia ou a humilhação experimentados pela vítima. Nessa perspectiva, o que se indeniza é um estado anímico negativo, e a reparação pressupõe, em regra, que esse estado seja demonstrado ou ao menos razoavelmente inferido das circunstâncias. A segunda concepção, ligada à constitucionalização do direito civil, entende o dano moral como lesão à dignidade da pessoa humana, isto é, a um interesse existencial merecedor de

tutela, independentemente da reação emocional que provoque (Moraes, 2003).

Farias, Rosenvald e Braga Netto (2022) ilustram a fragilidade da primeira concepção com o exemplo da pessoa em estado vegetativo: se o dano moral fosse a dor sentida, quem não pode senti-la jamais teria direito à reparação por ofensa à honra ou à imagem, conclusão evidentemente inaceitável. A dor, o desgosto e a aflição seriam, assim, consequências eventuais da lesão, e não a própria lesão.

A escolha entre as duas concepções tem efeito direto sobre o ônus da prova. Adotada a ideia de dano como lesão a interesse existencial, a exposição indevida de dados, por atingir o direito fundamental à proteção de dados e à autodeterminação informativa, já configuraria o dano, cabendo ao juiz apenas dimensioná-lo. Adotada a concepção de dano como sofrimento, o titular teria de demonstrar que a exposição lhe causou abalo psicológico relevante ou consequências concretas (Couto, 2023, p. 178).

É nesse ponto que entra a figura do dano moral *in re ipsa*, ou presumido. Trata-se do dano que decorre do próprio fato ofensivo, dispensando a prova do prejuízo. A jurisprudência do STJ consolidou essa técnica em diversas situações. A Súmula 403 dispensa a prova do prejuízo na publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais (BRASIL, 2009b), e a Súmula 385, ao afastar a indenização apenas quando preexistente legítima inscrição, pressupõe que a anotação irregular em cadastro de proteção ao crédito gera, em regra, dano indenizável (BRASIL, 2009a). A presunção, contudo, é técnica probatória, e não regra geral: apoia-se nas regras de experiência comum, que o juiz aplica a

partir da observação do que ordinariamente acontece (BRASIL, 2015, art. 375), e se justifica quando essa experiência indica que determinado fato, em regra, lesa a personalidade de quem o sofre. Para os dados sensíveis, Mulholland (2020) sustenta que o tratamento irregular gera dano *in re ipsa*, por violar diretamente direitos de privacidade, liberdade e igualdade.

Aplicada aos vazamentos, essa lógica revela uma dificuldade real. Muitos titulares sequer sabem que seus dados foram expostos, e o prejuízo, quando ocorre, pode se manifestar meses depois, na forma de um golpe, de uma fraude ou de uma enxurrada de contatos indesejados. Exigir do titular a prova de um dano que ainda não se materializou, ou cuja ligação com o incidente é difícil de demonstrar, pode tornar a tutela inócua. Por outro lado, presumir o dano em todo e qualquer incidente, inclusive naqueles em que os dados expostos já eram de amplo conhecimento público, pode converter a responsabilidade civil em fonte de indenizações automáticas. Schreiber (2015) adverte justamente para a erosão dos filtros tradicionais da responsabilidade civil e para o risco de expansão descontrolada das demandas indenizatórias, preocupação que reaparece no debate sobre dados pessoais.

### 4.2. A Experiência do Tribunal de Justiça da União Europeia

O direito europeu oferece um contraponto útil. Ao interpretar o art. 82 do RGPD, o Tribunal de Justiça da União Europeia fixou, no caso Österreichische Post, que a mera violação do regulamento não basta para gerar o direito à indenização, exigindo-se, cumulativamente, a infração, o dano e o nexo causal, e afastou a possibilidade de o direito nacional condicionar a reparação a um patamar mínimo de gravidade do dano imaterial (União Europeia, 2023a). Em dezembro

de 2023, no caso Natsionalna agentsia za prihodite, que envolvia ataque cibernético à agência tributária búlgara, a Corte admitiu que o receio de utilização abusiva dos dados após o vazamento pode, por si, constituir dano imaterial, cabendo ao juiz nacional verificar se esse receio é fundado nas circunstâncias do caso (União Europeia, 2023b). No mesmo dia, no caso Gemeinde Ummendorf, reafirmou a inexistência de limiar mínimo de gravidade, mas exigiu que o titular demonstre ter efetivamente sofrido dano, ainda que reduzido, admitindo que a perda de controle sobre os dados, mesmo por curto período, pode configurá-lo (União Europeia, 2023c).

A solução europeia não é a da presunção absoluta nem a da exigência de prova de prejuízo material. Ela reconhece que a perda de controle sobre os dados e o temor fundado de seu mau uso são danos reais, mas exige que sejam demonstrados a partir das circunstâncias concretas do incidente. Essa via intermediária é especialmente útil para o direito brasileiro, cuja jurisprudência, como se verá, oscila entre os dois extremos.

## 5. A DIVERGÊNCIA JURISPRUDENCIAL NO SUPERIOR TRIBUNAL DE JUSTIÇA

A análise dos precedentes revela que o Superior Tribunal de Justiça ainda não uniformizou sua orientação sobre o dano decorrente da exposição indevida de dados. As decisões foram proferidas por turmas diferentes, em contextos fáticos distintos, e apontam em direções que nem sempre se conciliam. O Quadro 1 sintetiza os julgados examinados, distinguindo os casos de vazamento por incidente de segurança dos casos de compartilhamento sem base legal.

**Quadro 1.** Síntese dos precedentes do STJ analisados

| Julgado | Órgão e data | Hipótese | Dados envolvidos | Solução quanto ao dano |
|---|---|---|---|---|
| AREsp 2.130.619/SP | 2ª Turma, 7/3/2023 | Vazamento: ataque aos sistemas de concessionária de energia | Comuns (cadastrais e de consumo) | Exige prova do dano |
| REsp 2.133.261/SP | 3ª Turma, 8/10/2024 | Compartilhamento sem base legal por gestor de banco de dados | Comuns (cadastrais) | Dano presumido |
| REsp 2.147.374/SP | 3ª Turma, 3/12/2024 | Vazamento: ataque hacker | Comuns | Não examina a presunção; afasta a excludente de culpa exclusiva de terceiro |
| REsp 2.121.904/SP | 3ª Turma, 11/2/2025 | Vazamento: incidente de segurança em seguradora | Sensíveis (saúde) e patrimoniais | Dano presumido |
| REsp 2.201.694/SP | 3ª Turma, 5/8/2025 | Compartilhamento sem base legal por birô de crédito | Comuns (cadastrais e de adimplemento) | Dano presumido (por maioria) |
| REsp 2.221.650/SP | 4ª Turma, 4/11/2025 | Compartilhamento sem base legal | Comuns (cadastrais) | Exige prova do dano; falta de prova do próprio |

| | | | | |
|---|---|---|---|---|
| | | por birô de crédito | | compartilhamento (Súmula 7) |

**Fonte:** elaborado pelas autoras (2026), com base nos acórdãos indicados.

### 5.1. A Exigência de Prova do Dano na Segunda Turma

O precedente mais citado sobre o tema foi julgado pela Segunda Turma em 7 de março de 2023, sob relatoria do Ministro Francisco Falcão, no AREsp 2.130.619/SP (BRASIL, 2023). Na origem, uma consumidora idosa ajuizou ação contra a concessionária de energia elétrica Eletropaulo depois que criminosos invadiram os sistemas da empresa e copiaram dados de usuários. Entre as informações expostas estavam nome completo, RG, gênero, data de nascimento, idade, telefones e endereço, além de dados do contrato de fornecimento, como carga instalada e consumo estimado (BRASIL, 2023).

A sentença julgou o pedido improcedente. O Tribunal de Justiça de São Paulo reformou a decisão e fixou indenização de R$ 5.000,00, considerando tratar-se de dados de pessoa idosa. O STJ, por unanimidade, restabeleceu a sentença. A ementa resume o fundamento central:

> *V - O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações. (BRASIL, 2023).*

O acórdão também afirmou que o rol de dados sensíveis do art. 5º, II, da LGPD é taxativo e que os dados de natureza comum, pessoais, mas não íntimos, não podem ser assim classificados. O relator ressalvou expressamente a hipótese diversa: "Diferente seria se, de fato, estivéssemos diante de vazamento de dados sensíveis, que dizem respeito à intimidade da pessoa natural" (BRASIL, 2023). Dessa ressalva extraiu-se a distinção que passou a orientar parte da jurisprudência: o vazamento de dados comuns exige prova do dano, ao passo que o de dados sensíveis autorizaria a presunção. A Quarta Turma transcreveu a ementa do julgado como fundamento do REsp 2.221.650/SP (BRASIL, 2025c).

Dois aspectos do julgado merecem atenção. O primeiro é processual: a tese de culpa exclusiva de terceiro não foi examinada, por falta de prequestionamento (Súmula 211 do STJ), de modo que a responsabilidade da concessionária pelo incidente não chegou a ser discutida em seus contornos (BRASIL, 2023). O segundo é de fundo: o acórdão foi proferido por turma de direito público, ao passo que as questões de responsabilidade civil entre particulares são, em regra, julgadas pela Terceira e pela Quarta Turmas. Couto (2023, p. 180) aponta que o próprio tribunal já contava com julgados em sentidos opostos, o que contraria o dever de manter a jurisprudência estável,

íntegra e coerente imposto pelo art. 926 do Código de Processo Civil (BRASIL, 2015).

### 5.2. O Dano Presumido na Terceira Turma

A Terceira Turma reconheceu, já antes da vigência da LGPD, que a disponibilização de dados pessoais em banco de dados de fácil acesso por terceiros enseja indenização por danos morais, considerando sobretudo o sentimento de insegurança experimentado pelo titular (BRASIL, 2019). Em 2024 e 2025, essa orientação foi aplicada a novos contextos.

No REsp 2.133.261/SP, julgado por unanimidade em 8 de outubro de 2024, sob relatoria da Ministra Nancy Andrighi, a Turma assentou que o gestor de banco de dados que disponibiliza a terceiros consulentes informações que só poderiam ser compartilhadas entre bancos de dados responde objetivamente pelos danos morais, que se presumem diante da forte sensação de insegurança experimentada pelo titular (BRASIL, 2024a).

Em 3 de dezembro de 2024, no REsp 2.147.374/SP, relatado pelo Ministro Ricardo Villas Bôas Cueva, a Turma enfrentou vazamento de dados não sensíveis atribuído a ataque hacker e rejeitou a excludente do art. 43, III, da LGPD, por não ter sido demonstrada a culpa exclusiva do terceiro (BRASIL, 2024b). O acórdão não se pronunciou sobre a presunção do dano: sua relevância para este estudo está em afastar a ideia de que o ataque externo, por si só, exonera o agente de tratamento.

Em 11 de fevereiro de 2025, no REsp 2.121.904/SP, a Turma examinou o vazamento de propostas de seguro de vida, que continham dados de saúde, bens e beneficiários. A Ministra Nancy Andrighi, relatora,

afirmou que o vazamento de dados pessoais sensíveis fornecidos para a contratação do seguro, “por si só, submete o consumidor a riscos em diversos aspectos de sua vida, como em sua honra, imagem, intimidade, patrimônio, integridade física e segurança pessoal” (BRASIL, 2025a). Reconheceu-se, por unanimidade, a responsabilidade objetiva da seguradora e o dano moral presumido.

Por fim, em 5 de agosto de 2025, no REsp 2.201.694/SP, a Turma decidiu, por maioria, que o gestor de banco de dados para formação de histórico de crédito que disponibiliza a terceiros consulentes informações cadastrais e de adimplemento, sem prévia autorização do cadastrado, responde objetivamente pelos danos morais, que são presumidos (BRASIL, 2025b). Prevaleceu o voto da Ministra Nancy Andrighi, acompanhada pelos Ministros Moura Ribeiro e Daniela Teixeira, ficando vencidos o relator originário, Ministro Ricardo Villas Bôas Cueva, e o Ministro Humberto Martins. O caso chama atenção porque os dados envolvidos, como o número de telefone, não eram sensíveis, e o Tribunal de Justiça de São Paulo havia negado a indenização justamente por esse motivo.

### 5.3. A Posição da Quarta Turma

Em 4 de novembro de 2025, a Quarta Turma julgou o REsp 2.221.650/SP, de relatoria da Ministra Maria Isabel Gallotti, em que o autor alegava a comercialização de seus dados pessoais por empresa gestora de banco de dados de proteção ao crédito (BRASIL, 2025c). O acórdão, unânime, partiu de premissa coincidente com a da Terceira Turma: a LGPD autoriza o tratamento de dados para a proteção do crédito (art. 7º, X), mas remete à Lei do Cadastro Positivo, que permite ao gestor compartilhar informações cadastrais e de adimplemento apenas com outros bancos de dados e

disponibilizar a consulentes somente a nota de crédito e, mediante autorização específica, o histórico de crédito (BRASIL, 2011, art. 4º, III e IV). Concluiu, assim, que os gestores "não estão autorizados a disponibilizar dados pessoais e histórico de crédito sem o consentimento prévio de seus titulares" (BRASIL, 2025c).

A divergência está no passo seguinte. Para a Quarta Turma, "a disponibilização de dados pessoais, por si só, não configura dano moral presumido (in re ipsa)", sendo imprescindível comprovar "abalo significativo aos direitos de personalidade do titular" (BRASIL, 2025c). A relatora fundamentou essa conclusão na distinção entre dados sensíveis e dados comuns, estes últimos tratados como "informações ordinárias, frequentemente fornecidas em cadastros diversos", e invocou o AREsp 2.130.619/SP como precedente.

É preciso, contudo, qualificar o alcance do julgado. No caso concreto, o Tribunal de origem havia concluído que o autor não comprovou sequer a efetiva disponibilização de seus dados a terceiros, e a revisão dessa premissa esbarrou na Súmula 7 do STJ (BRASIL, 2025c). A divergência com a Terceira Turma é real quanto à tese, pois ambas reputam ilícita a disponibilização sem consentimento e divergem sobre a presunção do dano, mas o resultado do caso também decorreu da ausência de prova do próprio fato.

### 5.4. A Afetação do Tema Repetitivo 1.404

A divergência entre a Terceira e a Quarta Turmas, que compõem a Segunda Seção, levou à afetação da controvérsia ao rito dos recursos especiais repetitivos. No Tema 1.404, afetado nos REsp 2.226.946/SP e REsp 2.226.097/SP, de relatoria do Ministro Raul Araújo, a Segunda Seção definirá se é lícita a disponibilização ou comercialização a

terceiros de dados pessoais não sensíveis, por gestor de banco de dados de entidades de proteção ao crédito, sem prévia comunicação ou consentimento do cadastrado, e se há dano moral *in re ipsa* na hipótese de ilicitude da conduta, com suspensão dos processos que versem sobre a matéria (BRASIL, 2026).

O recorte do tema é relevante para este estudo. A tese a ser fixada alcançará a disponibilização de dados por gestores de bancos de dados de proteção ao crédito, mas não, ao menos diretamente, os vazamentos decorrentes de incidentes de segurança, como os examinados no AREsp 2.130.619/SP e no REsp 2.121.904/SP. Para essa segunda hipótese, não há precedente uniformizador, e a orientação da Segunda Turma convive com a abertura da Terceira Turma para o dano presumido nos casos de dados sensíveis, o que reforça a utilidade de critérios de aferição do dano que não dependam exclusivamente da natureza do dado.

## 6. CRITÉRIOS PARA A AFERIÇÃO DO DANO INDENIZÁVEL

A análise dos precedentes demonstra que a natureza do dado é relevante, mas não pode ser utilizada isoladamente. O sistema jurídico da proteção de dados oferece outros parâmetros para avaliar a gravidade do incidente e a existência de dano indenizável.

O primeiro critério é a **natureza e o volume dos dados expostos.** Dados referentes à saúde, à vida sexual, à origem racial, à biometria, à situação financeira ou às credenciais de autenticação possuem, em regra, maior potencial lesivo. A exposição de grande quantidade de dados também pode aumentar o risco de identificação, fraude e criação de perfis comportamentais. Foi esse o elemento destacado pela Terceira Turma no REsp 2.121.904/SP, em que o vazamento

envolvia dados de saúde, bens e beneficiários (BRASIL, 2025a). Por outro lado, como observa Bioni (2019), dados triviais podem adquirir caráter sensível quando correlacionados a outros, de modo que o volume e a combinação das informações também devem ser considerados.

O segundo critério é o **contexto e a finalidade da relação jurídica.** A expectativa de proteção deve ser analisada conforme a relação estabelecida entre o titular e o agente de tratamento. Informações fornecidas a uma seguradora, instituição financeira ou serviço de saúde são tratadas em contexto de confiança qualificada. No REsp 2.121.904/SP, a circunstância de os dados terem sido fornecidos para a contratação do seguro integrou a própria fundamentação do dano (BRASIL, 2025a).

O terceiro critério é a **origem do incidente.** Deve-se distinguir o acesso não autorizado decorrente de ataque externo da disponibilização voluntária de dados a terceiros sem base legal ou sem observância dos deveres de informação. A origem do evento influencia a análise da ilicitude e da responsabilidade. A comparação entre os precedentes evidencia esse ponto: no AREsp 2.130.619/SP, que tratava de invasão dos sistemas por terceiros, exigiu-se a prova do dano (BRASIL, 2023), ao passo que, nos REsp 2.133.261/SP e 2.201.694/SP, a disponibilização voluntária pelo próprio gestor levou a Terceira Turma a presumir o dano mesmo diante de dados comuns (BRASIL, 2024a; BRASIL, 2025b). O ataque externo, contudo, não exonera por si só o agente de tratamento, como decidido no REsp 2.147.374/SP (BRASIL, 2024b).

O quarto critério é o **uso efetivo ou o risco concreto de utilização indevida das informações.** A ocorrência de fraude, golpe,

contratação indevida ou contatos abusivos demonstra repercussão concreta. Mesmo sem fraude consumada, a exposição de informações em ambiente destinado à comercialização de dados pode revelar risco relevante. A Terceira Turma já considerava, antes da LGPD, o sentimento de insegurança decorrente da disponibilização de dados em banco de fácil acesso (BRASIL, 2019), e o Tribunal de Justiça da União Europeia admitiu que o receio fundado de utilização abusiva das informações pode, por si, constituir dano imaterial (União Europeia, 2023b).

O quinto critério é a **conduta posterior do agente de tratamento.** A comunicação tempestiva do incidente, a contenção do evento, a orientação dos titulares e a adoção de medidas de segurança devem ser consideradas na avaliação da gravidade da situação. Esse critério relaciona-se ao dever de comunicação previsto no art. 48 da LGPD e, embora possa influenciar a própria caracterização do dano, repercute sobretudo na fixação do valor da indenização, que se mede pela extensão do dano (BRASIL, 2002, art. 944).

Esses critérios encontram fundamento na própria LGPD, especialmente nos princípios da segurança, prevenção e responsabilização, bem como nas regras sobre tratamento irregular, comunicação de incidentes e medidas de mitigação. A Resolução CD/ANPD nº 15/2024 reforça esses parâmetros ao considerar que o incidente pode acarretar risco ou dano relevante quando puder afetar significativamente interesses e direitos fundamentais dos titulares e envolver, entre outros, dados sensíveis, dados de crianças, adolescentes ou idosos, dados financeiros, dados de autenticação em sistemas, dados protegidos por sigilo ou dados em larga escala (BRASIL, 2024c, art. 5º).

**Quadro 2.** Critérios para a aferição do dano indenizável

| Critério | Fundamento normativo | Indica maior gravidade | Indica menor gravidade |
|---|---|---|---|
| Natureza e volume dos dados expostos | LGPD, arts. 5º, II, e 11; Resolução CD/ANPD nº 15/2024, art. 5º | Dados sensíveis, financeiros, de autenticação, de crianças ou idosos; grande volume ou combinação de dados que permite fraude | Dado isolado de baixo potencial lesivo, já amplamente público |
| Contexto e finalidade da relação jurídica | LGPD, arts. 6º, I e II, e 44, I e II; CDC, art. 14, § 1º | Relação de confiança qualificada (saúde, seguro, finanças) | Cadastro de uso corriqueiro, sem expectativa especial de reserva |
| Origem do incidente | LGPD, arts. 6º, VII, 7º, 43, III, e 46; Lei nº 12.414/2011, art. 4º | Disponibilização voluntária sem base legal; falha de segurança evitável | Ataque externo apesar de medidas de segurança adequadas e comprovadas |
| Uso efetivo ou risco concreto de uso dos dados | LGPD, art. 48, § 1º, IV; Resolução CD/ANPD nº 15/2024 | Fraude, golpe ou contato abusivo comprovados; dados expostos em ambientes de comercialização | Ausência de indícios de circulação ou de uso das informações |
| Conduta do agente de tratamento após o incidente | LGPD, arts. 6º, X, 48 e 52, § 1º; Código Civil, art. 944 | Omissão ou demora na comunicação; ausência de mitigação | Comunicação tempestiva, bloqueio de acessos e orientação aos titulares |

**Fonte:** elaborado pelas autoras (2026).

## 7. CONSIDERAÇÕES FINAIS

A pesquisa demonstrou que o vazamento de dados pessoais e o compartilhamento indevido de informações são fenômenos relacionados, mas não idênticos. O primeiro normalmente decorre de acesso não autorizado ou falha de segurança; o segundo resulta da disponibilização ou utilização dos dados em desconformidade com a finalidade ou com os limites legais.

A jurisprudência do Superior Tribunal de Justiça ainda não consolidou uma resposta única. O AREsp 2.130.619/SP afastou o dano moral presumido em relação a dados comuns vazados. Em sentido diverso, a Terceira Turma reconheceu a presunção em casos envolvendo dados sensíveis e disponibilização indevida de dados cadastrais. A afetação do Tema 1.404 do STJ demonstra que a controvérsia permanece pendente de uniformização, ao menos quanto aos gestores de bancos de dados de proteção ao crédito.

A resposta ao problema de pesquisa é que o vazamento pode configurar dano moral indenizável sem prova de prejuízo material, mas a presunção não deve decorrer automaticamente da simples ocorrência do incidente. A solução mais adequada exige a análise conjunta de cinco critérios: natureza e volume dos dados expostos; contexto e finalidade da relação jurídica; origem do incidente; uso efetivo ou risco concreto de utilização das informações; e conduta posterior do agente de tratamento.

A principal contribuição do estudo consiste em demonstrar que a distinção entre dados comuns e sensíveis é necessária, mas insuficiente. Dados comuns podem adquirir elevado potencial lesivo quando combinados, utilizados para fraude ou compartilhados com

terceiros sem fundamento legal. Da mesma forma, a presença de dados sensíveis não elimina a necessidade de examinar o nexo causal e as circunstâncias concretas do caso.

A pesquisa também apresenta como limitação a rápida evolução jurisprudencial do tema. A afetação do Tema 1.404 do STJ poderá modificar a compreensão atualmente extraída dos precedentes.

## REFERÊNCIAS BIBLIOGRÁFICAS


ALEMANHA. Bundesverfassungsgericht (Primeiro Senado). **BVerfGE 65, 1.** Volkszählungsurteil (julgamento da lei do recenseamento). Karlsruhe, 15 dez. 1983.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com,** Rio de Janeiro, a. 9, n. 3, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/download/662/506. Acesso em: 8 out. 2026.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 8 out. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 15, de 24 de abril de 2024. Aprova o Regulamento de

Comunicação de Incidente de Segurança. **Diário Oficial da União,** Brasília, DF, 26 abr. 2024c. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 8 out. 2026.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Congresso Nacional, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 8 out. 2026.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilado.htm. Acesso em: 8 out. 2026.

BRASIL. Lei nº 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 8 out. 2026.

BRASIL. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. Brasília, DF: Presidência da República, 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 8 out. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 8 out. 2026.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 8 out. 2026.

BRASIL. Superior Tribunal de Justiça (2. Seção). **Tema Repetitivo nº 1.404.** Recursos Especiais nº 2.226.946/SP e nº 2.226.097/SP. Relator: Min. Raul Araújo. Brasília, DF: STJ, 2026. Disponível em: https://processo.stj.jus.br/repetitivos/temas_repetitivos/pesquisa.jsp?novaConsulta=true&tipo_pesquisa=T&cod_tema_inicial=1404&cod_tema_final=1404. Acesso em: 8 out. 2026.

BRASIL. Superior Tribunal de Justiça (2. Turma). **Agravo em Recurso Especial nº 2.130.619/SP.** Relator: Min. Francisco Falcão, 7 mar. 2023. DJe 10 mar. 2023. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumeroRegistro&termo=202201522622. Acesso em: 8 out. 2026.

BRASIL. Superior Tribunal de Justiça (3. Turma). **Recurso Especial nº 1.758.799/MG.** Relatora: Min. Nancy Andrighi, 12 nov. 2019. DJe 19 nov. 2019. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1888267&tipo=0&nreg=201700065219&SeqCgrmaSessao=&CodO

rgaoJgdr=&dt=20191119&formato=HTML&salvar=false. Acesso em: 8 out. 2026.

BRASIL. Superior Tribunal de Justiça (3. Turma). **Recurso Especial nº 2.121.904/SP.** Relatora: Min. Nancy Andrighi, 11 fev. 2025a. DJEN 17 fev. 2025. Disponível em: https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?i=1&b=ACOR&livre=(('RESP'.clas. e @num='2121904') ou ('RESP' adj '2121904'.suce.))&thesaurus=JURIDICO. Acesso em: 8 out. 2026.

BRASIL. Superior Tribunal de Justiça (3. Turma). **Recurso Especial nº 2.133.261/SP.** Relatora: Min. Nancy Andrighi, 8 out. 2024a. DJe 10 out. 2024. Disponível em: https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?i=1&b=ACOR&livre=(('RESP'.clas. e @num='2133261') ou ('RESP' adj '2133261'.suce.))&thesaurus=JURIDICO. Acesso em: 8 out. 2026.

BRASIL. Superior Tribunal de Justiça (3. Turma). **Recurso Especial nº 2.147.374/SP.** Relator: Min. Ricardo Villas Bôas Cueva, 3 dez. 2024b. DJEN 6 dez. 2024. Disponível em: https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?i=1&b=ACOR&livre=(('RESP'.clas. e @num='2147374') ou ('RESP' adj '2147374'.suce.))&thesaurus=JURIDICO. Acesso em: 8 out. 2026.

BRASIL. Superior Tribunal de Justiça (3. Turma). **Recurso Especial nº 2.201.694/SP.** Relatora para o acórdão: Min. Nancy Andrighi, 5 ago. 2025b. DJEN 15 ago. 2025. Disponível em: https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=329011149&registr

o_numero=202500811342&peticao_numero=&publicacao_data=20250815&formato=PDF. Acesso em: 8 out. 2026.

BRASIL. Superior Tribunal de Justiça (4. Turma). **Recurso Especial nº 2.221.650/SP.** Relatora: Min. Maria Isabel Gallotti, 4 nov. 2025c. DJEN 14 nov. 2025. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumeroRegistro&termo=202502428366. Acesso em: 8 out. 2026.

BRASIL. Superior Tribunal de Justiça. **Súmula nº 385.** Da anotação irregular em cadastro de proteção ao crédito, não cabe indenização por dano moral, quando preexistente legítima inscrição, ressalvado o direito ao cancelamento. Brasília, DF: STJ, 2009a.

BRASIL. Superior Tribunal de Justiça. **Súmula nº 403.** Independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais. Brasília, DF: STJ, 2009b.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387/DF.** Relatora: Min. Rosa Weber, 7 maio 2020. DJe 12 nov. 2020.

COUTO, José Henrique de Oliveira. Vazamentos de dados e dano moral 'in re ipsa': comentários ao Agravo em Recurso Especial nº 2.130.619/SP. **Revista IBERC,** Belo Horizonte, v. 6, n. 2, p. 171-188, maio/ago. 2023. Disponível em: https://revistaiberc.emnuvens.com.br/iberc/article/download/258/220/1524. Acesso em: 8 out. 2026.

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

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson; BRAGA NETTO, Felipe Peixoto. **Curso de direito civil:** responsabilidade civil. 7. ed. Salvador: JusPodivm, 2022.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do tratamento de dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** São Paulo: Thomson Reuters Brasil, 2019.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** São Paulo: Thomson Reuters Brasil, 2019.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor,** São Paulo, v. 120, p. 469-483, nov./dez. 2018.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. **Cadernos Adenauer,** Rio de Janeiro, a. 20, n. 3, p. 113-135, 2019.

MORAES, Maria Celina Bodin de. **Danos à pessoa humana:** uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2003.

MORAES, Maria Celina Bodin de. LGPD: um novo regime de responsabilização civil dito "proativo". **Civilistica.com,** Rio de Janeiro, a. 8, n. 3, 2019. Editorial. Disponível em: https://civilistica.emnuvens.com.br/redc/article/download/448/377. Acesso em: 8 out. 2026.

MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018). **Revista IBERC,** Belo Horizonte, 2020. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf. Acesso em: 8 out. 2026.

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

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: MENDES, Laura Schertel et al. (coord.). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021.

SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil:** da erosão dos filtros da reparação à diluição dos danos. 6. ed. São Paulo: Atlas, 2015.

UNIÃO EUROPEIA. Tribunal de Justiça (Terceira Secção). **Acórdão de 14 de dezembro de 2023.** Processo C-340/21, VB c. Natsionalna

agentsia za prihodite. ECLI:EU:C:2023:986. 2023b. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62021CJ0340. Acesso em: 8 out. 2026.

UNIÃO EUROPEIA. Tribunal de Justiça (Terceira Secção). **Acórdão de 14 de dezembro de 2023.** Processo C-456/22, VX e AT c. Gemeinde Ummendorf. ECLI:EU:C:2023:988. 2023c. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62022CJ0456. Acesso em: 8 out. 2026.

UNIÃO EUROPEIA. Tribunal de Justiça (Terceira Secção). **Acórdão de 4 de maio de 2023.** Processo C-300/21, UI c. Österreichische Post AG. ECLI:EU:C:2023:370. 2023a. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62021CJ0300. Acesso em: 8 out. 2026.

---

[1] Acadêmica do curso de Direito do Centro Universitário UniBRAS Rio Verde.

[2] Especialista. Advogada. Professora do curso de Direito e Coordenadora do Núcleo de Prática Jurídica do Centro Universitário UniBRAS Rio Verde. Orientadora. E-mail: acesse o artigo original para visualizar o e-mail.