

**FACULDADE DE ADMINISTRAÇÃO, NEGÓCIOS E SAÚDE DE SERGIPE -
FANESE
CURSO DE DIREITO**

JOSIMAR DAS VIRGENS DOS SANTOS

**A Responsabilidade Civil no Vazamento de Dados Pessoais: uma análise à luz da LGPD
e do entendimento do STJ**

ARACAJU

2026

S237r

SANTOS, Josimar das Virgens dos

A responsabilidade civil no vazamento de dados pessoais : uma análise à luz da LGPD e do entendimento do STJ / Josimar das Virgens dos Santos. - Aracaju, 2026.

22 f.

Trabalho de Conclusão de Curso (Artigo) Faculdade de Administração, Negócios e Saúde de Sergipe. Coordenação de Direito.

Orientador (a): Prof. Me. Thiago de Menezes Ramos

1. Direito 2. Dano moral – LGPD
3. Dados pessoais – Vazamento I. Título

CDU 34 (045)

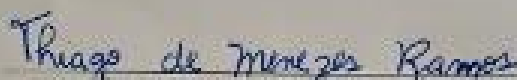
Elaborada pela Bibliotecária Edla de Fatima S. Evangelista CRB-5/1029

JOSIMAR DAS VIRGENS DOS SANTOS

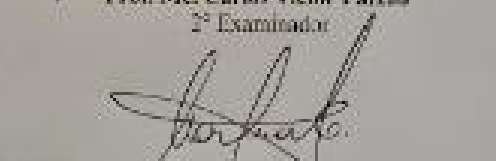
**RESPONSABILIDADE CIVIL NO VAZAMENTO DE DADOS PESSOAIS:
UMA ANÁLISE À LUZ DA LGPD E DO ENTENDIMENTO DO STJ**

Artigo Científico apresentado à Faculdade de Administração e Negócios de Sergipe - FANESE,
como requisito parcial e elemento obrigatório para a obtenção do grau bacharel em Direito no
período de 2026.1.

Aprovado (a) com média: **10,0**


Prof. Me. Thiago de Menezes Ramos
1º Examinador (Orientador)


Prof. Me. Carlos Vieira Paixão
2º Examinador


Prof. Me. Marilanny Sales Guimarães Poderosa
3º Examinadora

Aracaju, 18 de Junho de 2026

A Responsabilidade Civil no Vazamento de Dados Pessoais: uma análise à luz da LGPD e do entendimento do STJ

Josimar das Virgens dos Santos

RESUMO

O presente trabalho analisa a responsabilidade civil no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD), com foco no entendimento jurídico acerca do dano moral decorrente do vazamento de dados. O objetivo central é investigar se o incidente de segurança envolvendo dados pessoais comuns gera o dever de indenizar de forma presumida (*In Re Ipsa*) ou se exige a comprovação de prejuízo efetivo pelo titular. A metodologia adotada fundamenta-se na pesquisa bibliográfica e na análise documental, bem como na jurisprudência do Superior Tribunal de Justiça (STJ). Os resultados indicam que, embora a proteção de dados seja um direito fundamental, o entendimento pretoriano atual, consolidado pelo STJ, afasta a presunção do dano moral em casos de vazamento de dados biográficos, privilegiando a necessidade de prova do dano e do nexo de causalidade para a configuração da responsabilidade civil, o que, embora busque evitar a banalização do dano moral, pode restringir, na prática, a efetividade da tutela conferida ao titular em um ambiente marcado por forte assimetria informacional.

Palavras-chave: Dano Moral; LGPD; Responsabilidade Civil; Vazamento de Dados Pessoais.

1 INTRODUÇÃO

A centralidade econômica dos dados pessoais ampliou os riscos de lesão à esfera privada do titular, mas o problema jurídico central não está apenas no valor econômico da informação. Está, sobretudo, na dificuldade de o indivíduo controlar a circulação e o uso de seus próprios dados. No Brasil, esse cenário impulsionou a criação da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), que estabeleceu um novo paradigma jurídico para o tratamento de informações. O foco do debate atual reside na responsabilidade civil decorrente de incidentes de segurança, especificamente o vazamento de dados.

Embora a LGPD preveja a reparação de danos patrimoniais e morais (BRASIL, 2018), a aplicação prática desses dispositivos nos tribunais brasileiros tem gerado controvérsias. A grande questão jurídica que se impõe é: o simples vazamento de dados comuns é suficiente para gerar um dano moral presumido (*in re ipsa*), ou exige-se que o titular demonstre um prejuízo concreto?

Este trabalho justifica-se pela necessidade de analisar a segurança jurídica nas relações digitais, especialmente após a inclusão da proteção de dados como direito fundamental na Constituição Federal (EC nº 115/2022). O objetivo geral é investigar o regime de responsabilidade civil dos agentes de tratamento. Dentre os objetivos específicos visa-se diferenciar a responsabilidade subjetiva da objetiva no contexto da LGPD e analisar o posicionamento atual do Superior Tribunal de Justiça (STJ) sobre o tema.

A relevância deste projeto decorre, sobretudo, da importância jurídica que a proteção de dados pessoais passou a ocupar no ordenamento brasileiro, especialmente após seu reconhecimento como direito fundamental pela Emenda Constitucional nº 115/2022. Nesse contexto, torna-se necessário compreender de que maneira o Poder Judiciário vem aplicando a responsabilidade civil em situações de vazamento de dados, já que essa interpretação influencia diretamente a segurança jurídica de titulares e agentes de tratamento (SURIS; BRASIL DIAS, 2024).

Além disso, o tema se mostra atual diante do aumento dos incidentes de segurança cibernética e da frequência com que informações pessoais são expostas ou utilizadas indevidamente, o que desafia o Direito Civil a repensar a noção tradicional de dano em uma realidade cada vez mais digital (SCHREIBER, 2024). Soma-se a isso a dimensão social e econômica da questão, uma vez que a definição dos deveres de cuidado de controladores e operadores impacta não apenas a atuação das empresas, mas também o nível de proteção efetivamente assegurado à privacidade dos cidadãos.

A metodologia adotada é a pesquisa bibliográfica e documental, com abordagem qualitativa, focando na análise da legislação vigente e da jurisprudência recente. Estrutura-se a pesquisa em capítulos que abordam desde os fundamentos históricos da responsabilidade civil até a análise crítica dos precedentes judiciais sobre o dano moral digital.

A presente pesquisa adota abordagem qualitativa, de natureza exploratória e descritiva, por meio do método hipotético-dedutivo. Parte-se da análise das normas gerais de responsabilidade civil (Código Civil) e das regras específicas da LGPD para compreender sua aplicação prática. A pesquisa bibliográfica compreende a revisão doutrinária em obras e artigos de autores como Danilo Doneda, Bruno Bioni e Anderson Schreiber. A pesquisa documental e jurisprudencial abrange o levantamento de acórdãos do STJ e notas técnicas da ANPD. A técnica de análise consiste no confronto das correntes doutrinárias sobre a natureza do dano — presumido ou comprovado — e no exame crítico dos precedentes judiciais sobre o dano moral digital.

2 FUNDAMENTOS DA RESPONSABILIDADE CIVIL E PROTEÇÃO DE DADOS PESSOAIS

A compreensão da responsabilidade civil em matéria de proteção de dados pessoais exige, inicialmente, um retorno aos seus fundamentos históricos e dogmáticos. Não é possível analisar o vazamento de dados e os deveres impostos pela LGPD sem considerar como o instituto da responsabilidade civil se desenvolveu no direito brasileiro, quais funções passou a exercer e de que modo se aproximou da tutela dos direitos da personalidade. Ao mesmo tempo, a própria proteção de dados só pode ser corretamente entendida se for situada no contexto mais amplo da evolução da privacidade e dos direitos fundamentais. Por essa razão, antes de enfrentar diretamente o regime jurídico da LGPD e o tratamento jurisprudencial do dano moral decorrente de vazamentos, é necessário examinar os elementos estruturantes da responsabilidade civil e da proteção da pessoa humana no ordenamento

2.1 Evolução Histórica da Responsabilidade Civil no Brasil

A responsabilidade civil, no direito brasileiro, passou por significativa transformação ao longo do tempo. Em sua configuração mais tradicional, influenciada pelo liberalismo clássico, prevalecia a ideia de que a obrigação de indenizar estava diretamente vinculada à demonstração da culpa do agente causador do dano. Nesse modelo, o foco recaía sobre a reparação patrimonial, dentro de uma lógica individualista e repressiva, em que a responsabilidade civil era vista principalmente como consequência do ato ilícito praticado contra o patrimônio ou contra interesses juridicamente protegidos.

Com a evolução da sociedade e a ampliação dos riscos inerentes à vida moderna, esse entendimento mostrou-se insuficiente para responder a lesões mais complexas, especialmente aquelas relacionadas à personalidade, à dignidade e à esfera existencial do indivíduo. A doutrina contemporânea reconhece, nesse processo, um deslocamento da responsabilidade civil para uma função mais ampla de proteção da pessoa humana, como se percebe em Schreiber (2024) e Tepedino (2024).

No Brasil, essa mudança ganhou força com a constitucionalização do direito civil a partir da Constituição de 1988. A responsabilidade civil deixou de ser compreendida apenas como mecanismo técnico de recomposição econômica e passou a ser interpretada à luz dos valores constitucionais, especialmente a dignidade da pessoa humana, a solidariedade social e

a tutela dos direitos fundamentais. Com isso, o instituto passou a exercer também funções preventivas e protetivas, voltadas não só à reparação do dano já consumado, mas também à contenção de práticas lesivas e à promoção de maior cuidado nas relações privadas. Essa releitura se mostra particularmente importante em uma sociedade marcada pelo avanço tecnológico e pela circulação massiva de informações pessoais.

Nesse novo cenário, a responsabilidade civil passa a dialogar diretamente com os danos produzidos no ambiente digital. O uso intensivo de tecnologias de coleta, armazenamento e compartilhamento de dados revelou que muitas violações não se traduzem imediatamente em perdas econômicas visíveis, mas afetam a autonomia, a liberdade e a segurança do indivíduo. Doneda (2020) observa que a sociedade da informação alterou a própria natureza da tutela jurídica da pessoa, pois os dados pessoais se tornaram elementos centrais da vida social, econômica e institucional. Em linha semelhante, estudos recentes sobre a vulnerabilidade do titular de dados reforçam que a assimetria informacional e a circulação massiva de informações exigem um redesenho dos mecanismos de responsabilidade civil, aproximando-os de um modelo mais protetivo e compatível com os riscos estruturais da era digital (SURIS; BRASIL DIAS, 2024; SCHREIBER, 2024).

Assim, a evolução histórica da responsabilidade civil no Brasil demonstra a passagem de um modelo centrado quase exclusivamente na culpa e no patrimônio para outro orientado pela tutela integral da pessoa humana. É a partir dessa transformação que se torna possível compreender a proteção de dados pessoais como tema legítimo da responsabilidade civil contemporânea, sobretudo quando o tratamento indevido ou o vazamento de dados atinge direitos da personalidade e compromete a dignidade do titular.

2.2 A Proteção da Privacidade como Direito Fundamental à luz da Constituição Federal de 1988 em seu Art. 5º

A Constituição Federal de 1988 conferiu posição central à tutela da pessoa humana e estruturou, no art. 5º, um amplo sistema de direitos e garantias fundamentais. Quanto à privacidade, destacam-se especialmente os incisos X e XII. O inciso X estabelece que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação. Já o inciso XII protege o sigilo da correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas. Esses dispositivos revelam que a Constituição não apenas reconhece a existência

de uma esfera privada merecedora de tutela, mas também admite expressamente a reparação civil quando essa esfera é indevidamente atingida.

Ainda que a proteção de dados pessoais só tenha sido expressamente inserida no texto constitucional em 2022, a doutrina já identificava, antes disso, fundamento constitucional para sua tutela a partir da proteção da intimidade, da vida privada e do sigilo de dados. Doneda (2020) sustenta que a proteção de dados pessoais tem origem na privacidade, mas não se esgota nela. Para o autor, a noção clássica de privacidade, entendida apenas como um espaço de reserva ou de não intromissão, tornou-se insuficiente diante da realidade tecnológica atual, em que os dados são coletados, processados e compartilhados continuamente. Surge, então, a necessidade de proteger não apenas o segredo, mas também o controle sobre a própria informação.

É justamente nesse ponto que se destaca a ideia de autodeterminação informativa, entendida como a possibilidade de o indivíduo participar e influenciar o modo como seus dados são utilizados por terceiros. Essa concepção amplia o conteúdo jurídico da privacidade e a aproxima de uma perspectiva mais dinâmica e compatível com a sociedade digital. Em vez de limitar a proteção à proibição de invasões externas, passa-se a exigir transparência, finalidade legítima, controle e respeito à pessoa no tratamento de suas informações. Nessa linha, Schreiber (2024) e Tepedino (2020) contribuem para uma leitura civil-constitucional segundo a qual os direitos da personalidade devem ser reinterpretados de forma evolutiva, de modo a alcançar novas formas de lesão produzidas pelo desenvolvimento tecnológico e pela exploração econômica de dados pessoais.

No ambiente digital, a privacidade ganha contornos ainda mais sensíveis. O tratamento de dados pode ocorrer de forma invisível, automatizada e em larga escala, gerando riscos que nem sempre são imediatamente perceptíveis ao titular. A exposição indevida de dados, a formação de perfis, a circulação não autorizada de informações e a facilitação de fraudes demonstram que a proteção da privacidade, hoje, não pode ser dissociada da proteção da identidade e da liberdade informacional. Desse modo, o art. 5º da Constituição continua sendo o alicerce da tutela da pessoa humana também no contexto digital, servindo de fundamento para a interpretação da LGPD e para a análise da responsabilidade civil decorrente do uso indevido de dados pessoais.

2.3 Emenda Constitucional nº 115/2022

A Emenda Constitucional nº 115, promulgada em 10 de fevereiro de 2022, representa um marco normativo fundamental para a proteção de dados pessoais no Brasil. A emenda

acrescentou ao art. 5º da Constituição o inciso LXXIX, segundo o qual é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. Além disso, inseriu o inciso XXVI no art. 21, atribuindo à União a competência para organizar e fiscalizar a proteção e o tratamento de dados pessoais, e o inciso XXX no art. 22, estabelecendo a competência privativa da União para legislar sobre a matéria. Com isso, a proteção de dados passou a integrar expressamente o catálogo de direitos e garantias fundamentais.

A importância da Emenda Constitucional nº 115/2022 está em reconhecer, de forma clara, que a proteção de dados pessoais não constitui mera decorrência secundária da privacidade, mas sim um direito fundamental autônomo. Essa mudança acompanha a evolução doutrinária já defendida por Doneda (2020), para quem a proteção de dados exige tutela própria, adequada aos riscos da sociedade informacional e à crescente centralidade das informações pessoais nas relações sociais e econômicas. Ao constitucionalizar esse direito, o ordenamento brasileiro reforça a ideia de que o tratamento de dados não pode ser analisado apenas sob critérios econômicos ou empresariais, mas deve ser submetido a parâmetros de proteção da dignidade, da liberdade e da personalidade do titular.

Do ponto de vista da responsabilidade civil, a emenda fortalece a leitura constitucional da LGPD e amplia a densidade jurídica dos deveres impostos aos agentes de tratamento. A partir do reconhecimento expresso da proteção de dados como direito fundamental, o vazamento ou o tratamento indevido de dados pessoais deixa de ser visto apenas como falha técnica ou irregularidade operacional, podendo configurar lesão à posição jurídica de estatura constitucional. Isso não significa, por si só, que todo incidente gere automaticamente indenização, mas impõe ao intérprete uma análise mais sensível à gravidade da violação e aos impactos concretos sofridos pelo titular. A responsabilidade civil, nesse contexto, reafirma sua função de tutela da pessoa humana, especialmente em ambientes marcados por forte assimetria técnica e informacional.

Além disso, a Emenda Constitucional nº 115/2022 contribui para maior segurança jurídica ao concentrar na União a competência legislativa e administrativa sobre proteção de dados pessoais. Essa centralização evita fragmentações normativas e favorece a construção de um sistema mais uniforme, coerente e compatível com a natureza transversal dos fluxos informacionais na era digital. Dessa forma a emenda consolida a proteção de dados como valor constitucional expresso e reforça a necessidade de interpretar a responsabilidade civil por vazamento de dados à luz da dignidade da pessoa humana, da privacidade e da tutela dos direitos fundamentais.

3 O REGIME DE RESPONSABILIDADE NA LGPD COMO PROBLEMA JURÍDICO

É imperiosa a necessidade de abordagem dos limites e possibilidades da responsabilidade civil no ordenamento jurídico brasileiro. As tecnologias possibilitam disseminar dados, fomentar a democratização de informações e democratizar relações humanas a partir da informação como capital humano, econômico e social. Contudo, ao mesmo tempo que proporciona aludidas vantagens, cria, de modo direto, a necessidade de responsabilidade civil. Em razão disso, a LGPD se destaca como norma central de análise de tal regime de responsabilização.

3.1 O Surgimento da LGPD

A Lei Geral de Proteção de Dados Pessoais, instituída pela Lei nº 13.709/2018, surgiu em um contexto de profundas transformações tecnológicas e sociais, marcado pela intensificação da coleta, do armazenamento, do compartilhamento e da monetização de informações pessoais. A ampliação da economia digital, o uso crescente de plataformas eletrônicas, a automatização de decisões e a formação de bancos de dados em larga escala evidenciaram a insuficiência dos instrumentos jurídicos tradicionais para disciplinar o tratamento de dados pessoais. Nesse cenário, tornou-se necessário construir uma legislação específica, capaz de estabelecer parâmetros claros para a atuação de agentes públicos e privados, bem como de assegurar proteção efetiva aos titulares de dados.

O art. 1º da LGPD já revela a dimensão constitucional e existencial da lei ao dispor que ela regula o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Isso demonstra que a lei não se limita a organizar procedimentos técnicos de tratamento informacional, mas pretende resguardar valores centrais da ordem jurídica, diretamente vinculados à dignidade da pessoa humana (Brasil, 2018).

Nessa perspectiva, os dados pessoais deixam de ser vistos como meras informações economicamente exploráveis e passam a ser compreendidos como projeções da própria personalidade do indivíduo.

A doutrina de Doneda (2020) é fundamental para compreender esse processo. O autor sustenta que a proteção de dados pessoais não se resume à tutela clássica da privacidade, pois a sociedade informacional criou riscos e novas formas de vulnerabilidade. O problema jurídico

deixou de estar restrito à intromissão indevida na esfera privada e passou a envolver o controle sobre o fluxo de informações pessoais, sua circulação, reutilização e exploração econômica. A LGPD surge, portanto, como resposta normativa à necessidade de conferir ao titular maior controle sobre seus dados e maior proteção diante da assimetria informacional que caracteriza o ambiente digital.

Além disso, a lei brasileira se insere em um movimento internacional mais amplo de fortalecimento da proteção de dados, impulsionado por legislações estrangeiras e pela consolidação do tema como direito fundamental. No plano interno, a LGPD representa um marco regulatório essencial para a construção de uma cultura de responsabilidade no tratamento de dados pessoais. A partir dela, passam a coexistir direitos dos titulares, deveres dos agentes de tratamento, sanções administrativas e um regime próprio de responsabilidade civil, voltado à prevenção e reparação dos danos decorrentes do tratamento irregular de dados.

3.2 Princípios Norteadores: Prevenção, Segurança e Transparência

A LGPD estrutura-se sobre princípios que orientam toda a atividade de tratamento de dados pessoais. Esses princípios, previstos no art. 6º, cumprem função interpretativa e normativa, servindo como critério para aferir a licitude das condutas dos agentes de tratamento. Entre eles, assumem especial relevância para o presente trabalho os princípios da prevenção, da segurança e da transparência, justamente porque se relacionam diretamente com a lógica de responsabilização civil prevista na lei (Brasil, 2018).

O princípio da transparência impõe aos agentes de tratamento o dever de fornecer ao titular informações claras, precisas e facilmente acessíveis sobre a realização do tratamento, suas finalidades e os sujeitos envolvidos. Trata-se de exigência que busca reduzir a opacidade típica das relações informacionais contemporâneas, nas quais o titular, muitas vezes, desconhece quem trata seus dados, com qual finalidade e por quanto tempo. A transparência fortalece a autonomia do indivíduo e viabiliza o exercício consciente de seus direitos, sendo elemento indispensável para a legitimidade do tratamento de dados.

O princípio da segurança, por sua vez, exige a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Isso significa que a proteção dos dados não pode ficar restrita ao plano declaratório ou à intenção genérica de conformidade, devendo se traduzir em mecanismos concretos de prevenção de incidentes. A

segurança, nesse ponto, revela-se como verdadeiro dever jurídico de cuidado, cuja inobservância pode repercutir diretamente na caracterização da responsabilidade civil.

Já o princípio da prevenção projeta a proteção para um momento anterior ao dano, impondo aos agentes de tratamento o dever de adotar medidas destinadas a evitar a ocorrência de lesões aos titulares. Essa diretriz é especialmente importante porque afasta a compreensão de que a tutela jurídica dos dados pessoais se esgota na reparação posterior. Ao contrário, a LGPD privilegia uma lógica de atuação diligente, responsável e antecipatória, exigindo dos agentes uma postura ativa na administração dos riscos decorrentes do tratamento. Nessa linha, Tepedino (2020) ressalta que a circulação de dados pessoais deve ser lida à luz da dignidade da pessoa humana e da tutela das situações existenciais, o que reforça a ideia de que a atividade de tratamento não pode ser desvinculada de deveres robustos de cuidado e lealdade.

Esses princípios não funcionam de maneira isolada (Brasil, 2018). Prevenção, segurança e transparência integram um mesmo núcleo protetivo e revelam que a responsabilidade na LGPD não se limita à apuração de um dano consumado, mas está ligada à própria estrutura de deveres que recai sobre quem trata dados pessoais. Em outras palavras, o regime jurídico da lei não é apenas repressivo; ele é também preventivo, organizacional e protetivo.

3.3 Sujeitos: Controlador, Operador e Encarregado

A compreensão do regime de responsabilidade da LGPD exige, inicialmente, a identificação dos sujeitos envolvidos no tratamento de dados pessoais. O art. 5º da lei distingue três figuras principais: o controlador, o operador e o encarregado. O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. É ele, portanto, quem define as finalidades do tratamento e os meios essenciais para sua realização (Brasil, 2018).

O operador, por sua vez, é a pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador. Sua atuação decorre das diretrizes estabelecidas por quem ocupa a posição de controle decisório. Embora o operador não seja, em regra, o definidor das finalidades do tratamento, isso não significa ausência de relevância jurídica. Ao contrário, sua atuação pode gerar responsabilidade quando houver tratamento em desconformidade com a lei ou com as instruções legitimamente recebidas.

O encarregado, também previsto no art. 5º, exerce a função de canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados. Sua

função está relacionada à governança, à transparência e ao acompanhamento da conformidade institucional. Ainda que o encarregado não ocupe a mesma posição de centralidade decisória do controlador, sua presença reforça a estrutura de accountability introduzida pela LGPD, baseada na ideia de que o tratamento de dados deve ser rastreável, justificável e compatível com os direitos do titular.

A distinção entre esses sujeitos é relevante porque a imputação de deveres e responsabilidades depende do papel desempenhado por cada um na cadeia de tratamento. O controlador, por decidir sobre o tratamento, ocupa posição central e, por isso, assume deveres mais amplos de conformidade. O operador, embora atue em nome do controlador, também pode ser responsabilizado quando contribui para a violação da legislação. Já o encarregado se insere no sistema como figura de ligação institucional, favorecendo a transparência e a efetividade dos direitos previstos na lei. Essa delimitação evita a diluição indevida de responsabilidades e permite melhor identificação dos deveres jurídicos de cada agente.

3.4 Natureza da Responsabilidade: Objetiva vs. Subjetiva

A natureza da responsabilidade civil prevista na LGPD é tema que ainda provoca intenso debate doutrinário. O art. 42 dispõe que 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. A redação legal, porém, não afirma de maneira expressa se a responsabilidade é objetiva ou subjetiva, o que abriu espaço para interpretações distintas.

Uma parte significativa da doutrina sustenta que a responsabilidade civil na LGPD deve ser compreendida como objetiva, ou ao menos fortemente objetivada. Essa leitura se apoia em diferentes fundamentos: a atividade de tratamento de dados envolve risco, o titular se encontra em posição de vulnerabilidade técnica e informacional, e a exigência de prova da culpa poderia tornar excessivamente difícil a obtenção de tutela efetiva. Nessa linha, o estudo acerca da vulnerabilidade do titular de dados e da responsabilidade civil na LGPD aponta que a lógica protetiva da lei se harmoniza com a teoria objetiva, especialmente em razão da assimetria existente entre o titular e os agentes de tratamento (VIEIRA; NICOLETTI; SILVA, [s.d.]).

Por outro lado, Vieira, Nicoletti e Silva (s. d.) sustentam a existência de elementos subjetivos no regime da lei, argumentando que a ausência da expressão “independentemente de culpa” no art. 42 exige cautela na afirmação de uma responsabilidade objetiva em sentido pleno.

As autoras defendem que a responsabilidade civil na LGPD não pode ser lida como puramente objetiva, pois a imputação depende, ao menos, da demonstração de violação concreta aos deveres legais impostos aos agentes de tratamento, o que evidencia certa aproximação com modelos tradicionais de imputação civil. A controvérsia revela que o texto legal não eliminou inteiramente o debate, deixando margem para construção doutrinária e jurisprudencial.

Apesar disso, parece mais coerente com a finalidade da LGPD reconhecer que a lei adota um regime protetivo de responsabilidade que se aproxima da objetivação. Schreiber (2024), ao tratar da responsabilidade civil contemporânea, destaca que a proteção eficaz da vítima exige modelos compatíveis com a complexidade dos danos modernos e com a vulnerabilidade dos sujeitos expostos a riscos estruturais. Em matéria de dados pessoais, essa observação é especialmente pertinente, pois o titular raramente dispõe de informações suficientes para demonstrar, em detalhes, a culpa do agente de tratamento. Desse modo, ainda que a controvérsia doutrinária permaneça, a interpretação mais adequada a lógica da lei é aquela que privilegia a proteção efetiva da pessoa humana diante dos riscos informacionais.

3.5 Hipóteses excludentes de responsabilização

A LGPD também disciplina as hipóteses em que os agentes de tratamento poderão afastar a responsabilidade civil. O art. 43 estabelece que controlador e operador somente não serão responsabilizados quando provarem: que não realizaram o tratamento de dados pessoais que lhes é atribuído; que, embora tenham realizado o tratamento, não houve violação à legislação de proteção de dados pessoais; ou que o dano decorreu de culpa exclusiva do titular dos dados ou de terceiros.

Essas excludentes revelam que a lei não institui um dever absoluto de indenizar, mas também não adotou um sistema permissivo de exoneração. Ao contrário, o dispositivo exige prova concreta por parte do agente de tratamento, o que reforça a ideia de que a carga argumentativa e demonstrativa recai de forma relevante sobre quem exerce a atividade de tratamento. Não basta alegar genericamente que houve ataque externo, falha sistêmica ou participação de terceiro. É necessário demonstrar, de maneira consistente, que o caso se enquadra em uma das hipóteses legais aptas a romper o nexo de responsabilidade.

A interpretação dessas excludentes deve ser feita cautelosamente, sobretudo porque a proteção de dados pessoais está ligada à tutela de direitos fundamentais. Se interpretadas de forma excessivamente ampla, as excludentes podem esvaziar a efetividade da própria lei. Por

isso, o reconhecimento de culpa exclusiva do titular ou de terceiros, por exemplo, exige análise rigorosa das circunstâncias concretas e do cumprimento, pelo agente, de seus deveres de prevenção, segurança e conformidade. Em um ambiente de alto risco informacional, não se pode admitir que a mera ocorrência de incidente externo sirva, por si só, como justificativa automática para afastar a responsabilização.

3.6 Inversão do Ônus da Prova

No plano processual, a LGPD prevê importante mecanismo de proteção ao titular dos dados. O art. 42, § 2º, dispõe que o juiz, no processo civil, poderá inverter o ônus da prova em favor do titular quando for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção da prova pelo titular lhe resultar excessivamente onerosa. Trata-se de regra expressa, que demonstra a preocupação do legislador com a desigualdade informacional presente nos litígios envolvendo tratamento de dados.

Essa previsão é especialmente relevante porque, na maioria dos casos, o titular não possui acesso aos elementos técnicos e internos necessários para demonstrar exatamente como ocorreu o tratamento, em que ponto houve a falha, quais medidas de segurança existiam e se a conduta do agente observou ou não os deveres legais. Já o controlador e o operador, em regra, detêm melhores condições de acesso às informações, registros, logs, políticas internas e demais elementos de prova. A inversão do ônus da prova funciona, assim, como instrumento de equilíbrio processual e de concretização da proteção jurídica assegurada pela LGPD.

A previsão legal dialoga diretamente com a noção de vulnerabilidade do titular de dados. Em termos práticos, sem esse mecanismo, a tutela indenizatória poderia se tornar ineficaz, já que o titular frequentemente enfrentaria obstáculos quase intransponíveis para comprovar a origem e a extensão da falha no tratamento. Por essa razão, a inversão do ônus da prova não deve ser compreendida como exceção arbitrária, mas como consequência lógica de um regime jurídico voltado à proteção da pessoa em ambiente de intensa assimetria técnica e informacional.

Desse modo, a LGPD articula responsabilidade material e proteção processual de forma coerente. Ao mesmo tempo em que estabelece deveres de prevenção, segurança e conformidade para os agentes de tratamento, também reconhece que o titular necessita de instrumentos processuais adequados para obter tutela efetiva em juízo. Suris e Brasil Dias (2024) ressaltam que a efetividade do regime de responsabilidade civil na LGPD depende da conjugação entre deveres substanciais de cuidado e mecanismos processuais que reduzam as barreiras de acesso

à justiça impostas pela assimetria informacional. Nessa perspectiva, a inversão do ônus da prova ocupa papel central no sistema, pois contribui para transformar a proteção legal em proteção concretamente exigível pelo titular de dados.

4 O DANO MORAL NO VAZAMENTO DE DADOS: ANÁLISE JURISPRUDENCIAL

Os danos morais podem ser compensados a partir da existência de conduta e nexo de causalidade. Nesse viés, é preciso analisar a extensão dos danos morais no contexto digital.

4.1 Caracterização do dano moral no âmbito digital

O avanço da tecnologia alterou de forma significativa a maneira como os direitos da personalidade podem ser violados (SCHREIBER, 2024). No ambiente digital, a lesão à intimidade, à privacidade, à honra e à imagem pode ocorrer de forma mais rápida, ampla e duradoura, já que os dados circulam com facilidade e, muitas vezes, sem controle efetivo do titular.

Nesse contexto, o dano moral digital pode ser compreendido como a lesão extrapatrimonial decorrente do uso indevido, da exposição não autorizada ou da circulação ilícita de dados pessoais, quando isso afeta a esfera existencial da pessoa (SCHREIBER, 2024). Não se trata de uma categoria totalmente desvinculada do dano moral tradicional, mas de um desdobramento da tutela clássica dos direitos da personalidade diante das novas formas de lesão surgidas na sociedade da informação (DONEDA, 2020).

As novas tecnologias ampliaram o potencial lesivo das condutas humanas, exigindo do direito uma resposta mais atenta à proteção da pessoa (SCHREIBER, 2024; SURIS; BRASIL DIAS, 2024). Por isso, o dano moral no ambiente digital não se limita à publicação ofensiva ou à exposição de conteúdos íntimos, podendo também decorrer da perda de controle sobre informações pessoais, da utilização indevida de dados por terceiros e da quebra da autodeterminação informativa.

Nesse sentido, a proteção de dados pessoais não se resume à privacidade, entendida apenas como segredo ou reserva (DONEDA, 2020). A questão central está no controle que o indivíduo deve possuir sobre a obtenção, o tratamento e a circulação de seus dados. Quando esse controle é rompido por vazamento ou compartilhamento indevido, a violação pode atingir

diretamente a dignidade da pessoa natural, gerando consequências jurídicas no campo da responsabilidade civil (SCHREIBER, 2024).

4.2 A Tese do Dano *In Re Ipsa* no contexto digital

Em regra, o dano moral deve ser demonstrado por quem pleiteia a indenização. Contudo, em situações excepcionais, a jurisprudência admite o chamado dano *in re ipsa*, em que o prejuízo é presumido em razão da própria gravidade do fato. Nesses casos, a ocorrência do ilícito já revela, por si só, a existência de lesão moral, dispensando prova específica do sofrimento experimentado pela vítima.

Essa tese é particularmente relevante em matéria de proteção de dados, pois muitas vezes a vítima não consegue comprovar de forma imediata todos os efeitos concretos da exposição indevida de suas informações. O dano pode se projetar no tempo, manifestar-se de forma indireta ou surgir na forma de insegurança, medo de fraude e perda de controle sobre dados relevantes da vida privada.

Ainda assim, o reconhecimento do dano *in re ipsa* exige cautela. O Superior Tribunal de Justiça tem entendido que essa modalidade de dano não pode ser aplicada automaticamente em toda hipótese de vazamento de dados, sob pena de banalização da responsabilidade civil (STJ, 2022; STJ, 2023). A presunção do dano deve ficar reservada às situações em que a gravidade da ofensa à personalidade seja evidente e juridicamente qualificada.

Assim, a jurisprudência vem demonstrando que o dano presumido não é afastado da proteção de dados, mas sua incidência depende das circunstâncias do caso concreto, da natureza dos dados envolvidos e da intensidade da lesão provocada ao titular.

4.3 Distinção entre Dados Comuns e Sensíveis

A distinção entre dados pessoais comuns e dados pessoais sensíveis é essencial para a compreensão da responsabilidade civil em casos de vazamento. A Lei Geral de Proteção de Dados define dado pessoal como toda informação relacionada a pessoa natural identificada ou identificável. Já os dados sensíveis correspondem àqueles relacionados à origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, saúde, vida sexual, dados genéticos e biométricos (BRASIL, 2018, art. 5º, II).

Essa diferenciação possui relevante consequência jurídica. A própria LGPD estabelece proteção reforçada para os dados sensíveis, especialmente por reconhecer que tais informações possuem maior potencial discriminatório e invasivo, podendo gerar danos mais intensos à intimidade, à liberdade e à dignidade do titular. Em razão disso, o vazamento de dados sensíveis tende a ser tratado com maior severidade pelo ordenamento jurídico.

No plano doutrinário, compreende-se que a proteção de dados deve considerar não apenas o conteúdo da informação, mas também os riscos decorrentes de sua circulação, compartilhamento e uso indevido. Por isso, a exposição de dados sensíveis justifica uma resposta mais intensa do sistema jurídico, sobretudo quando há ameaça concreta à personalidade e à segurança do titular.

No campo jurisprudencial, essa distinção se tornou decisiva. O Superior Tribunal de Justiça vem entendendo que, em casos de dados comuns, a indenização por dano moral normalmente exige demonstração de prejuízo concreto. Já nas hipóteses que envolvem dados sensíveis, ou situações de risco acentuado à esfera da personalidade, torna-se mais viável o reconhecimento do dano moral presumido (STJ, 2025).

4.4 O Entendimento Atual do STJ com base em julgados

A jurisprudência recente do Superior Tribunal de Justiça demonstra que o tribunal não adota uma posição automática sobre o dano moral em casos de vazamento de dados (STJ, 2024). De maneira geral, a corte tem entendido que o simples vazamento de dados pessoais comuns não gera, por si só, indenização. Por outro lado, quando a exposição envolve dados sensíveis, compartilhamento indevido relevante ou utilização fraudulenta das informações, o dever de indenizar tende a ser reconhecido com maior facilidade.

Um dos precedentes mais importantes sobre o tema é o AREsp 2.130.619/SP. Nesse caso, houve vazamento de nome, data de nascimento, endereço e número de documento de identificação. O STJ concluiu que se tratava de dados pessoais comuns, e não de dados sensíveis, razão pela qual o dano moral não poderia ser presumido. Conforme registrado no julgado: **“PROCESSUAL CIVIL E CONSUMIDOR. RECURSO ESPECIAL. AÇÃO REVISIONAL DE FINANCIAMENTO COM ALIENAÇÃO FIDUCIÁRIA. CAPITALIZAÇÃO DIÁRIA DE JUROS. DEVER DE INFORMAÇÃO. AUSÊNCIA DE TAXA DIÁRIA. ABUSIVIDADE E NULIDADE PARCIAL DA CLÁUSULA. RECÁLCULO. SEGURO PRESTAMISTA. VENDA CASADA. TEMA 972/STJ. NECESSIDADE DE PROVA DE IMPOSIÇÃO. ÓBICES DAS SÚMULAS 5 E 7/STJ.**

LGPD. COMPARTILHAMENTO DE DADOS. CONSENTIMENTO E BASES LEGAIS. DANO MORAL NÃO PRESUMIDO. NECESSIDADE DE DANO CONCRETO. RECURSO CONHECIDO EM PARTE E PARCIALMENTE PROVIDO.

5. Sobre a LGPD, havendo consentimento e demais bases legais de tratamento, e ausente prova de dano concreto, o dano moral não é presumido; o acolhimento da pretensão exigiria reinterpretação de cláusulas e revolvimento probatório (Súmulas 5 e 7/STJ)”.

Assim, para haver indenização, seria necessária a comprovação de prejuízo efetivo sofrido pela titular.

Em linha semelhante, o REsp 2.221.650 reafirmou que a mera disponibilização não autorizada de dados pessoais não sensíveis em cadastro positivo não gera automaticamente dano moral presumido. Conforme ementa e nas palavras do acórdão: **“RECURSO ESPECIAL. AÇÃO DE OBRIGAÇÃO DE FAZER CUMULADA COM INDENIZAÇÃO POR DANOS MORAIS. DISPONIBILIZAÇÃO DE DADOS PESSOAIS NÃO SENSÍVEIS. LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). LEI DO CADASTRO POSITIVO. AUSÊNCIA DE CONSENTIMENTO PRÉVIO. AUSÊNCIA DE DANO MORAL PRESUMIDO (IN RE IPSA). NECESSIDADE DE COMPROVAÇÃO DO DANO. RECURSO NÃO PROVIDO** e Vistos e relatados estes autos em que são partes as acima indicadas, acordam os Ministros da QUARTA TURMA, por unanimidade, negar provimento ao recurso, nos termos do voto da Sra. Ministra Relatora. Os Srs. Ministros Antonio Carlos Ferreira, Marco Buzzi, João Otávio de Noronha e Raul Araújo votaram com a Sra. Ministra Relatora”.

O entendimento foi no sentido de que a reparação exige prova de abalo significativo, afastando a presunção automática do dano em hipóteses envolvendo dados comuns.

Por outro lado, o STJ tem decidido de forma diversa quando a situação revela lesão mais intensa à personalidade. No REsp 2.201.694, a Terceira Turma reconheceu que a disponibilização indevida de informações pessoais em banco de dados a terceiros, sem comunicação prévia ao titular e sem consentimento, configura violação aos direitos da personalidade e gera dano moral presumido. (STJ, 2025). Conforme o julgado: **“DIREITO DO CONSUMIDOR E PROCESSUAL CIVIL. RECURSO ESPECIAL. OBRIGAÇÃO DE FAZER E INDENIZAÇÃO POR DANOS MORAIS. TRATAMENTO E COMERCIALIZAÇÃO DE DADOS PESSOAIS. CADASTRO POSITIVO. LEI N. 12.414/2011. LEI GERAL DE PROTEÇÃO DE DADOS (LEI N. 13.709/2018). CREDIT SCORING (TEMA 710/STJ E SÚMULA 550/STJ). DISTINÇÃO DE INSTITUTOS.**

DISPONIBILIZAÇÃO INDEVIDA DE DADOS CADASTRAIS A TERCEIROS. VIOLAÇÃO DO DEVER DE INFORMAÇÃO E CONSENTIMENTO. DANO MORAL IN RE IPSA. LEGITIMIDADE PASSIVA DO GESTOR DE BANCO DE DADOS. RESPONSABILIDADE OBJETIVA. RECURSO ESPECIAL PROVIDO.

4. Conforme precedentes desta Corte, a comercialização e o compartilhamento de dados pessoais como nome da mãe, data de nascimento, endereço, telefones, sexo, título de eleitor e renda presumida, por gestores de bancos de dados a terceiros consulentes, sem o consentimento prévio e específico do titular, configura violação do direito à privacidade e intimidade, conforme o art. 5º, X, da Constituição Federal, o art. 21 do Código Civil, os arts. 7º, I e X, 8º e parágrafos da Lei n. 13.709/2018, e os arts. 3º, §§ 1º e 3º, I e 4º e 5º, VII, da Lei n. 12.414/2011, caracterizando-se como ato ilícito.

5. A disponibilização indevida de dados pessoais pelo gestor de banco de dados a terceiros gera dano moral in re ipsa, presumido pela forte sensação de insegurança e descontrole sobre as próprias informações, sendo desnecessária a comprovação do prejuízo concreto”.

Nesse caso, prevaleceu a ideia de que a forte sensação de insegurança provocada pela divulgação indevida já seria suficiente para justificar a indenização.

Situação ainda mais expressiva aparece no REsp 2.121.904/SP, relativo ao vazamento de dados pessoais sensíveis em contrato de seguro de vida. Nesse precedente, o STJ reconheceu a responsabilidade objetiva da seguradora e admitiu o dano moral presumido, justamente porque a natureza dos dados expostos elevava consideravelmente o risco de discriminação, constrangimento e violação à intimidade. (STJ, Informativo de Jurisprudência n. 842). Nos termos do acórdão: **“Vistos e relatados estes autos em que são partes as acima indicadas, acordam os Ministros da TERCEIRA TURMA do Superior Tribunal de Justiça, em Sessão Virtual de 28/04/2026 a 04/05/2026, por unanimidade, conhecer parcialmente do recurso e, nessa parte, dar-lhe parcial provimento, nos termos do voto do Sr. Ministro Relator.**

Os Srs. Ministros Daniela Teixeira, Nancy Andrigli, Humberto Martins e Ricardo Villas Bôas Cueva votaram com o Sr. Ministro Relator”.

Além disso, quando o vazamento se conecta a fraude ou dano material concreto, a tendência do tribunal também é reconhecer a responsabilidade. O próprio levantamento institucional do STJ sobre os primeiros quatro anos da LGPD menciona o REsp 2.077.278, em que instituição financeira foi responsabilizada pelo tratamento indevido de dados bancários utilizados em golpe contra o consumidor. (STJ, 2024). Conforme ementa e acórdão:

“DIREITO DO CONSUMIDOR. RECURSO ESPECIAL. FRAUDE BANCÁRIA. ATUAÇÃO CRIMINOSA. VAZAMENTO PRÉVIO DE DADOS PESSOAIS. DANOS EXTRAPATRIMONIAIS. PRESUMIDOS. SENSACÃO DE INSEGURANÇA. REFORMA DO ACÓRDÃO.

3. Embora a fraude bancária, por si só, não configure o dano moral indenizável, nos termos da jurisprudência desta Corte, quando o referido ilícito estiver associado ao prévio vazamento de dados pessoais - que possibilitaram aos falsários o conhecimento de informações privilegiadas sobre o titular da conta - caracteriza-se o dano extrapatrimonial, com o consequente dever de compensá-lo.

4. A configuração do dano moral decorre do evidente sentimento de insegurança experimentado pela parte ao perceber que seus dados foram disponibilizados indevidamente para terceiros, favorecendo a prática de atos ilícitos ou contratações fraudulentas por eventuais terceiros de má-fé.

Vistos e relatados estes autos em que são partes as acima indicadas, acordam os Ministros da TERCEIRA TURMA, por unanimidade, conhecer do recurso especial e lhe dar provimento, nos termos do voto da Sra. Ministra Relatora.

Os Srs. Ministros Humberto Martins, Ricardo Villas Bôas Cueva, Moura Ribeiro e Daniela Teixeira votaram com a Sra. Ministra Relatora”

Em síntese, o entendimento atual do STJ pode ser resumido da seguinte forma: o mero vazamento de dados comuns não gera automaticamente dano moral; porém, quando há dados sensíveis, compartilhamento indevido relevante ou prejuízo concreto decorrente do tratamento irregular, a indenização passa a ser juridicamente mais consistente (STJ, 2024).

Essa linha jurisprudencial demonstra que o tribunal vem buscando um ponto de equilíbrio entre evitar a banalização do dano moral e assegurar tutela efetiva à pessoa natural quando a violação informacional afeta de forma relevante sua dignidade e sua segurança.

5 CONSIDERAÇÕES FINAIS

A análise desenvolvida neste trabalho permite concluir que a responsabilidade civil por vazamento de dados pessoais, no contexto da LGPD, não pode ser tratada de forma automática nem simplificada. Embora a proteção de dados tenha sido reconhecida como direito fundamental e represente hoje uma das expressões mais relevantes da tutela da personalidade no ambiente digital, isso não significa que todo incidente de segurança produza, por si só, o dever de indenizar. A prática jurisprudencial, especialmente no âmbito do Superior Tribunal de

Justiça, revela uma tendência de maior cautela: nos casos envolvendo dados pessoais comuns, tem prevalecido o entendimento de que o dano moral não se presume, sendo necessária a demonstração de prejuízo efetivo e do nexo entre a falha no tratamento e a lesão alegada.

Esse posicionamento, de um lado, busca evitar a banalização da responsabilidade civil e impedir que a mera ocorrência formal de um vazamento seja suficiente para gerar indenização em qualquer hipótese. De outro lado, essa mesma orientação não está livre de críticas. Em um cenário marcado por forte assimetria técnica e informacional, exigir do titular prova concreta do dano pode significar, em muitos casos, impor um ônus excessivo justamente à parte mais vulnerável da relação. O problema se torna ainda mais sensível quando se considera que os efeitos do vazamento de dados nem sempre são imediatos, visíveis ou facilmente demonstráveis, podendo surgir de forma posterior, difusa ou cumulativa.

A pesquisa também evidencia que a natureza dos dados expostos exerce papel decisivo na resposta jurídica. Quando estão em jogo dados sensíveis, informações capazes de gerar discriminação ou situações em que o vazamento se conecta a fraude, constrangimento ou risco relevante à esfera existencial do titular, a solução não pode ser a mesma aplicada indistintamente aos casos de menor gravidade. Nesses contextos, mostra-se mais coerente admitir uma tutela reparatória mais intensa, compatível com a dimensão da lesão e com a função protetiva da própria LGPD.

Assim, a hipótese central do trabalho se confirma: o atual entendimento do STJ, de modo geral, afasta o reconhecimento automático do dano moral nos casos de vazamento de dados pessoais comuns, exigindo a comprovação do prejuízo concreto. Ainda assim, essa orientação não encerra o debate. Ao contrário, demonstra que o direito brasileiro ainda está em processo de construção de critérios mais seguros para lidar com danos produzidos em ambiente digital, especialmente quando a violação informacional atinge direitos da personalidade de maneira menos tangível, mas nem por isso menos relevante.

Em conclusão, parece mais adequado compreender que a responsabilidade civil na LGPD deve ser aplicada com equilíbrio, sem reduzir o vazamento de dados a um mero aborrecimento cotidiano, mas também sem transformar toda falha de segurança em dano presumido. O desafio jurídico está justamente em encontrar um ponto de convergência entre segurança jurídica e proteção efetiva da pessoa humana. É nesse espaço de tensão que se insere a importância da interpretação jurisprudencial e doutrinária do tema, bem como a necessidade de constante aperfeiçoamento dos mecanismos de tutela do titular de dados na sociedade informacional.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [1988].

BRASIL. **Emenda Constitucional n.º 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: Presidência da República, 2022.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Thomson Reuters Brasil, 2020.

SCHREIBER, Anderson. **Manual de direito civil contemporâneo**. 7. ed. São Paulo: SaraivaJur, 2024.

SCHREIBER, Anderson. **Os direitos da personalidade e o Código Civil de 2002**. [S. l.], [s. d.].

SUPERIOR TRIBUNAL DE JUSTIÇA. **Disponibilização indevida de informações pessoais em banco de dados gera dano moral presumido**. Brasília, DF: STJ, 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. In re ipsa: os entendimentos mais recentes do STJ sobre a configuração do dano presumido. Brasília, DF: STJ, 2022.

SUPERIOR TRIBUNAL DE JUSTIÇA. Os precedentes do STJ nos primeiros quatro anos de vigência da Lei Geral de Proteção de Dados Pessoais. Brasília, DF: STJ, 2024.

SUPERIOR TRIBUNAL DE JUSTIÇA. REsp 2.121.904/SP. Informativo de Jurisprudência n. 842. Brasília, DF: STJ, [s. d.].

SUPERIOR TRIBUNAL DE JUSTIÇA. REsp 2.221.650. Acórdão. Brasília, DF: STJ, [s. d.].

SUPERIOR TRIBUNAL DE JUSTIÇA. Titular de dados vazados deve comprovar dano efetivo ao buscar indenização, decide Segunda Turma. Brasília, DF: STJ, 2023.

SURIS, Jéssica; BRASIL DIAS, Ádamo. Uma análise crítica acerca do regime de responsabilidade civil dos agentes de tratamento da Lei Geral de Proteção de Dados. Revista da Defensoria Pública do Estado do Rio Grande do Sul, Porto Alegre, v. 1, n. 34, p. 286-305, 2024.

TEFFÉ, Chiara Antonia Spadaccini de; TEPEDINO, Gustavo. O consentimento na circulação de dados pessoais. **Revista Brasileira de Direito Civil – RBDCivil**, Belo Horizonte, v. 25, n. 3, p. 83-104, 2020.

TEPEDINO, Gustavo. **Fundamentos do direito civil: responsabilidade civil**. v. 4. 5. ed. Rio de Janeiro: Forense, 2024.

VIEIRA, Tatiana Malta; NICOLETTI, Camilla Guimarães; SILVA, Beatriz Ferreira da. A vulnerabilidade do titular de dados e a responsabilidade civil na Lei Geral de Proteção de Dados. **Civilistica.com**, [s. l.], [s. d.].