Revista Educação, Meio Ambiente e Saúde
REMAS
ISSN: 1983-0173

# Proteção de dados pessoais e responsabilidade civil no Brasil: limites da reparação por tratamento irregular

# Protection of personal data and civil liability in Brazil: limits of compensation for unlawful processing

# Protección de datos personales y responsabilidad civil en Brasil: límites de la reparación por tratamiento irregular

Tipo de artigo: Artigo de pesquisa | Recebido: 07/10/2026 | Aceito: 03/11/2026

**Gustavo Tameirão Junker**

Acadêmico do Curso de Direito Instituição de Formação: Faculdade de Ensino Superior de Linhares

Endereço: Linhares, Espírito Santo, Brasil E-mail: gustavoojunker@gmail.com

ORCID: https://orcid.org/0009-0006-8986-7760

**Jakeline Martins Silva Rocha**

Mestra em Direito Privado Instituição de Formação: Faculdade Vitória em Cristo Endereço: São Mateus, Espírito Santo, Brasil

E-mail: jakeline.rocha@faceli.edu.br

ORCID: https://orcid.org/0000-0002-6867-6272

**RESUMO**

**Objetivo:** com o status de direito fundamental no Brasil, a proteção de dados pessoais impõe hoje uma nova leitura dos critérios clássicos de responsabilização civil. O artigo investiga em que condições controladores e operadores respondem por tratamento irregular de dados, com foco em vazamentos, falhas de segurança, dano moral e relações de consumo. **Metodologia:** utilizou-se pesquisa qualitativa de cunho bibliográfico, documental e jurisprudencial, com base na Constituição Federal, na LGPD, em atos da ANPD, em doutrina especializada e em julgados do STJ. **Resultados:** constatou-se que a LGPD não impõe indenização automática a todo vazamento, mas tampouco aceita, sem comprovação, que um ataque externo isente o agente de responsabilidade: a reparação exige prova do tratamento irregular, do nexo causal e do dano concreto, sem prejuízo de medidas inibitórias e dos direitos de acesso e informação do titular. **Conclusão:** o modelo brasileiro, conclui-se, combina prevenção, responsabilidade ligada ao risco da atividade e apreciação concreta da lesão à personalidade.

**DESCRITORES:** Proteção de dados; Responsabilidade civil; Privacidade; Vazamento de dados; Lei Geral de Proteção de Dados.

**ABSTRACT**

**Objective:** now recognized as a fundamental right in Brazil, personal data protection calls for a fresh reading of the traditional standards of civil liability. This article examines the conditions under which controllers and processors may be held liable for unlawful data processing, focusing on breaches, security failures, moral damages and consumer relations. **Methodology:** a qualitative study was carried out through bibliographical, documentary and case-law research, drawing on the Federal Constitution, the Brazilian data protection statute (LGPD), guidance issued by the National Data Protection Authority, specialized scholarship and Superior Court of Justice rulings. **Results:** the findings show that the LGPD neither imposes automatic liability for every breach nor allows an external attack to be accepted, without proof, as grounds for exemption: compensation requires evidence of unlawful processing, causation and actual harm, alongside injunctive remedies and the

data subject's rights to access and information. **Conclusion:** the Brazilian model, the study concludes, blends prevention, risk-based liability and a case-by-case assessment of harm to personality rights.
**DESCRIPTORS:** Data protection; Civil liability; Privacy; Data breach; General Data Protection Law.

**RESUMEN**
**Objetivo:** reconocida como derecho fundamental en Brasil, la protección de datos personales exige hoy una nueva lectura de los criterios clásicos de responsabilidad civil. El artículo examina en qué condiciones responsables y encargados del tratamiento responden por un manejo irregular de los datos, centrándose en filtraciones, fallas de seguridad, daño moral y relaciones de consumo. **Metodología:** se realizó una investigación cualitativa de tipo bibliográfico, documental y jurisprudencial, con base en la Constitución Federal, la LGPD, actos de la Autoridad Nacional de Protección de Datos, doctrina especializada y fallos del Superior Tribunal de Justicia. **Resultados:** se constató que la LGPD no impone indemnización automática por cada filtración, pero tampoco acepta, sin prueba, que un ataque externo exima de responsabilidad al agente: la reparación exige demostrar el tratamiento irregular, el nexo causal y el daño concreto, sin perjuicio de medidas inhibitorias y de los derechos de acceso e información del titular. **Conclusión:** el modelo brasileño combina, así, prevención, responsabilidad basada en el riesgo y evaluación concreta de la lesión a la personalidad.
**DESCRIPTORES:** Protección de datos; Responsabilidad civil; Privacidad; Filtración de datos; Ley General de Protección de Datos.

## INTRODUÇÃO

A digitalização mudou a forma como pessoas, empresas e órgãos públicos coletam, guardam e usam informações. Dados pessoais hoje atravessam contratação, consumo, crédito, saúde, educação, trabalho e prestação de serviços — o que amplia a capacidade das organizações de conhecer e influenciar indivíduos, mas também os riscos de acesso indevido, de compartilhamento fora da finalidade original e de uso abusivo.

No Brasil, a proteção de dados deixou de ser tratada apenas como faceta da privacidade e ganhou status constitucional próprio: a Emenda Constitucional nº 115/2022 inseriu no art. 5º, LXXIX, da Constituição o direito à proteção de dados pessoais, inclusive em meios digitais, além de atribuir à União competência legislativa e administrativa sobre a matéria. Com isso, o titular deixa de ser mero objeto do fluxo informacional e passa a ser sujeito de direitos, com autodeterminação informativa e proteção de sua personalidade.

A Lei nº 13.709/2018 (LGPD), em seu art. 1º, protege os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade, definindo princípios, bases legais, direitos dos titulares, deveres de controladores e operadores, medidas de segurança e regras de responsabilização civil. A dúvida central é saber em que condições o tratamento irregular gera dever de indenizar e se o simples vazamento já basta para configurar dano moral.

O tema ganhou destaque diante de decisões do STJ que, à primeira vista, parecem apontar em direções diferentes. Em 2023, a Segunda Turma decidiu, no AREsp 2.130.619, que o vazamento de dados pessoais comuns não gera, por si só, dano moral indenizável, sendo necessária prova do prejuízo efetivo. Já no REsp 2.147.374/SP, julgado em 2024 e divulgado no Informativo nº 838, a Corte entendeu que um ataque hacker não funciona automaticamente como excludente de responsabilidade, cabendo ao agente comprovar que adotou as medidas de segurança esperadas.

Este artigo tem como objetivo geral analisar o regime jurídico brasileiro de proteção de dados pessoais e os critérios de responsabilização civil dos agentes de tratamento. Especificamente, busca-se: examinar os fundamentos constitucionais e legais da matéria; identificar as hipóteses de responsabilidade em vazamentos e incidentes de segurança; discutir a configuração do dano moral; e avaliar os mecanismos de reparação e prevenção previstos na LGPD e lidos pelo STJ.

A relevância é tripla. No plano social, a exposição de dados facilita fraudes, discriminações e violações da esfera privada. No plano jurídico, aplicar a LGPD exige equilibrar proteção efetiva do titular e vedação de indenizações automáticas sem prova de lesão. No plano acadêmico, o tema mostra como a responsabilidade civil se conecta cada vez mais à governança, à segurança da informação e à tutela da personalidade.

**MÉTODO**

Trata-se de pesquisa qualitativa, exploratória e descritiva, construída por revisão bibliográfica, pesquisa documental e análise jurisprudencial. O estudo não envolve seres humanos, questionários, entrevistas ou coleta de dados pessoais, razão pela qual dispensou submissão ao Comitê de Ética em Pesquisa. Seu objeto é o regime normativo e interpretativo brasileiro sobre responsabilidade civil por tratamento irregular de dados pessoais.

A revisão bibliográfica abrangeu obras e artigos sobre privacidade, proteção de dados, direito do consumidor e responsabilidade civil, com destaque para Doneda, Mendes e Capanema. A pesquisa documental examinou a Constituição Federal, a EC nº 115/2022, a LGPD e orientações normativas da ANPD. A análise jurisprudencial concentrou-se em decisões e informativos do STJ publicados entre 2023 e 2026, selecionados por sua relação direta com vazamento, dano moral, ataque hacker e deveres dos agentes de tratamento.

O procedimento seguiu três etapas: identificação dos fundamentos constitucionais, princípios e categorias da LGPD; sistematização dos dispositivos sobre tratamento irregular, segurança, excludentes e reparação; e comparação dos precedentes para

apontar critérios comuns e eventuais tensões entre a exigência de prova do dano e a proteção da legítima expectativa de segurança. Por se tratar de matéria em desenvolvimento, os resultados podem ser impactados por novos casos, regulamentações e julgamentos futuros.

**RESULTADOS**

**Proteção de dados como direito fundamental e proteção da personalidade**

A EC nº 115/2022 alterou o parâmetro constitucional ao incluir a proteção de dados pessoais no catálogo de direitos fundamentais, o que orienta a interpretação da LGPD, impõe deveres de proteção ao Estado e reforça a necessidade de considerar autonomia, dignidade, liberdade e privacidade do titular na avaliação do tratamento.

A LGPD confirma essa orientação: seu art. 2º traz fundamentos que vão além de uma visão puramente patrimonial da informação, combinando privacidade, autodeterminação informativa e inviolabilidade da intimidade, da honra e da imagem com liberdade de expressão, desenvolvimento tecnológico, defesa do consumidor e livre desenvolvimento da personalidade. A lei não proíbe a circulação de dados, mas a condiciona a finalidades legítimas, bases jurídicas adequadas, transparência, segurança e respeito aos direitos do titular.

Autodeterminação informativa não equivale a controle absoluto do titular sobre cada operação feita com seus dados. Além do consentimento, a LGPD prevê bases legais como cumprimento de obrigação legal, execução de contrato, exercício regular de direitos e legítimo interesse, dentro dos limites legais. O essencial é que o tratamento seja previsível, justificável e proporcional, e que o titular possa conhecer e questionar práticas incompatíveis com a finalidade informada.

**Deveres dos agentes de tratamento e tratamento irregular**

O controlador decide sobre o tratamento; o operador o executa em nome do controlador. Isso não impede que ambos respondam quando suas condutas contribuírem para o dano. Pelo art. 44 da LGPD, é irregular o tratamento que desrespeita a lei ou não oferece a segurança esperada pelo titular, consideradas as circunstâncias e as técnicas disponíveis à época.

O art. 46 exige medidas técnicas e administrativas capazes de proteger os dados contra acesso não autorizado, destruição, perda, alteração, comunicação ou uso inadequado — obrigação que acompanha o produto ou serviço desde a concepção até a execução. Segurança, aqui, não é promessa de risco zero, mas dever de prevenção

proporcional à natureza dos dados, ao volume tratado, à finalidade, à tecnologia disponível e à vulnerabilidade dos titulares.

Segundo a ANPD, incidentes capazes de gerar risco ou dano relevante devem ser comunicados ao órgão e aos titulares — comunicação que não é mera formalidade, pois permite que as pessoas afetadas tomem providências. A Autoridade também esclarece que informar apenas a ANPD, sem comunicar os titulares, não satisfaz o art. 48 quando há risco ou dano relevante, evidenciando que a LGPD combina reparação e governança preventiva.

**Responsabilidade civil e solidariedade**

Pelo art. 42 da LGPD, controlador ou operador que causar dano patrimonial, moral, individual ou coletivo em violação à lei deve repará-lo — regra que deve ser lida junto com os arts. 44 e 46: não basta o incidente, é preciso avaliar se o tratamento foi irregular, se houve prejuízo e se existe nexo causal entre a falha e a lesão alegada.

A solidariedade do art. 42, §1º, permite que o titular cobre a reparação de qualquer responsável pelo tratamento, sem discutir de início quem foi o principal causador. O operador responde quando descumpre suas obrigações legais ou deixa de seguir instruções lícitas do controlador, sendo nesse caso equiparado a responsável pelo tratamento danoso; havendo mais de um controlador, todos podem responder solidariamente. Quem indeniza o titular pode depois cobrar dos demais a parcela correspondente à participação de cada um — a solidariedade facilita a reparação da vítima, mas não implica divisão automática igualitária do prejuízo entre os agentes.

Solidariedade não é sinônimo de responsabilidade automática de qualquer pessoa remotamente ligada ao fluxo de dados: é preciso identificar a posição jurídica do agente, a atividade que efetivamente exerce, seus deveres, a falha ocorrida e sua contribuição causal. Em relações de consumo, o art. 45 da LGPD preserva a aplicação do Código de Defesa do Consumidor, sem dispensar a análise do defeito do serviço, do dano e do nexo causal.

A doutrina destaca que o tratamento de dados pode se inserir na cadeia de fornecimento e envolver vulnerabilidade técnica e informacional do consumidor, o que justifica interpretação rigorosa dos deveres de segurança — sem, contudo, presumir dano moral em toda exposição. A reparação permanece vinculada às funções compensatória, preventiva e, quando cabível, inibitória da responsabilidade civil.

**Excludentes e ataques de terceiros**

O art. 43 da LGPD afasta a responsabilização em três hipóteses: ausência de realização do tratamento atribuído, inexistência de violação legal e dano decorrente de

culpa exclusiva do titular ou de terceiro. A excludente exige prova efetiva — alegar que o vazamento decorreu de ataque hacker não comprova, por si só, que o agente adotou as medidas de segurança exigíveis nem que a conduta de terceiro foi exclusiva e inevitável.

O STJ reforçou essa leitura no REsp 2.147.374/SP (Informativo nº 838), ao entender que o agente pode ser obrigado a cumprir deveres de informação da LGPD mesmo diante de vazamento de dados não sensíveis originado de ataque hacker, associando o caso à legítima expectativa de proteção, à responsabilidade civil proativa e à necessidade de gestão de riscos. O precedente não torna todo ataque cibernético gerador de indenização automática, mas confirma que a segurança da informação integra o dever jurídico do agente — que, para invocar culpa exclusiva de terceiro, precisa demonstrar de forma consistente que o evento não resultou de falha de governança, configuração insegura, ausência de atualização, controle de acesso insuficiente ou resposta inadequada ao incidente.

**Dano moral e necessidade de prova da lesão**

O dano moral decorrente do tratamento de dados deve ser avaliado conforme a natureza da informação, a extensão da exposição, o contexto, a finalidade do tratamento, a identificabilidade do titular, os riscos concretos e as consequências demonstradas. A proteção constitucional não converte todo descumprimento formal em dano presumido, mas também não reduz a lesão a uma simples perda econômica mensurável.

No AREsp 2.130.619, a Segunda Turma do STJ concluiu que o vazamento de dados comuns — nome, data de nascimento, endereço, documento — não gera, isoladamente, dano moral indenizável, exigindo prova do prejuízo efetivo e distinguindo dados comuns de dados sensíveis ligados à intimidade. Já o Informativo nº 871 registrou que a mera disponibilização de dados pessoais não configura dano moral presumido, sendo indispensável comprovar lesão concreta e relevante à personalidade. A jurisprudência, porém, não é uniforme: no REsp 2.201.694, de setembro de 2025, a Terceira Turma reconheceu dano moral presumido em caso específico, no qual informações cadastrais foram repassadas indevidamente a terceiros, sem comunicação prévia nem consentimento, por gestor de banco de dados regido pela Lei nº 12.414/2011.

Essa exigência de prova não deve ser lida de forma excessivamente restritiva: a lesão pode ser demonstrada por fraudes, tentativas de golpe, contatos abusivos, discriminação, exposição de dados íntimos, restrição de crédito, uso indevido de identidade, repercussão pública ou risco concretamente materializado. O titular não precisa comprovar prejuízo patrimonial para caracterizar dano moral, mas deve apresentar

circunstâncias que revelem afetação relevante de sua personalidade. Dados sensíveis exigem avaliação mais rigorosa, por seu potencial discriminatório e maior proximidade com a intimidade, mas a classificação como sensível, isoladamente, não gera regra automática de indenização — o julgador deve sempre considerar o conjunto probatório e a gravidade da lesão, o que preserva a coerência do sistema e evita tanto a banalização do dano moral quanto a insuficiência de tutela em casos graves.

**Direitos do titular e mecanismos de reparação**

A reparação civil é apenas uma entre várias respostas possíveis. Conforme o caso, o titular pode exercer direitos de confirmação, acesso, correção, eliminação, informação sobre compartilhamento e revisão de decisões automatizadas — no REsp 2.147.374/SP, o STJ reconheceu a possibilidade de impor ao agente o dever de informar entidades com as quais houve compartilhamento, origem, critérios e finalidade do tratamento.

A tutela também pode ser preventiva e inibitória: se a atividade continua gerando risco, cabe ordem judicial determinando adequações, bloqueio, eliminação de dados, prestação de informações ou implementação de medidas de segurança. Em incidentes coletivos, o art. 42, §3º, da LGPD permite ações coletivas para tutelar interesses transindividuais. A ANPD tem papel relevante na prevenção e fiscalização, mas sua atuação não substitui a responsabilidade civil perante o titular, nem a comunicação do incidente elimina automaticamente o dever de reparar — ainda que a rapidez da resposta, a cooperação com a Autoridade e as medidas de mitigação possam influenciar a avaliação da conduta e da extensão dos danos.

**DISCUSSÃO**

Os resultados mostram que a responsabilidade civil por tratamento irregular de dados não se encaixa bem numa simples oposição entre responsabilidade objetiva e subjetiva. A LGPD cria deveres de prevenção, segurança, transparência e cooperação que tornam a análise fortemente orientada pelo risco da atividade: quem explora economicamente o tratamento deve estruturar sua operação para reduzir riscos previsíveis e comprovar a efetividade de seus controles.

Ao mesmo tempo, o STJ rejeita a indenização automática por qualquer vazamento — posição que protege a racionalidade do sistema ao exigir dano concreto e relevante. Ausência de dano moral presumido não equivale à ausência de ilicitude: pode haver infração administrativa, dever de informação, direito de acesso, ordem de adequação ou responsabilidade por dano material sem que todo titular tenha direito automático à compensação moral.

A aparente tensão entre o AREsp 2.130.619, o REsp 2.147.374/SP, o Informativo nº 871 e o REsp 2.201.694 se resolve pela análise do contexto concreto: primeiro, se o agente cumpriu os deveres de segurança, finalidade, transparência e informação; depois, se o titular sofreu dano indenizável. O ataque hacker pode não bastar para afastar o dever de segurança e os direitos de informação, mas a indenização moral depende da gravidade da lesão e do nexo causal — já em casos de disponibilização indevida a terceiros, sem comunicação nem consentimento e em violação a regime específico de bancos de dados, o STJ admitiu que a própria situação de insegurança pode caracterizar dano presumido. Não existe, portanto, regra abstrata única para todo incidente: a natureza do ato, o contexto regulatório, a previsibilidade da exposição e a intensidade da lesão orientam a solução.

Essa distinção também evita reduzir o debate à mera existência ou ausência de consentimento. Como a LGPD prevê múltiplas bases legais, o tratamento sem consentimento não é necessariamente ilícito — a irregularidade pode nascer de finalidade incompatível, falta de transparência, excesso de dados, ausência de segurança, compartilhamento indevido ou violação dos direitos do titular. O consentimento não substitui a governança nem autoriza genericamente qualquer uso futuro.

A efetividade do sistema depende de documentação: controladores e operadores devem registrar decisões, avaliações de risco, políticas de acesso, treinamentos, contratos, respostas a incidentes e medidas corretivas, sem que essa prova de conformidade seja meramente formal — programas de observância precisam ser proporcionais ao porte da organização, ao tipo de dado e ao risco da atividade, já que a ausência de documentação pode dificultar a demonstração das excludentes do art. 43.

Por rigor metodológico, este artigo não utiliza como fundamento conclusivo a estatística inicialmente cogitada de mais de 8,5 mil reclamações em São Paulo em 2025, cuja fonte não permitia confirmar com segurança o órgão responsável, o universo das reclamações e a metodologia de contagem — em pesquisa jurídica, a atualidade da notícia não substitui a confiabilidade metodológica da fonte.

Como limitação, o estudo não realizou levantamento quantitativo de decisões nem análise exaustiva de todos os tribunais, tendo se concentrado em fontes oficiais diretamente relacionadas ao problema. Pesquisas futuras podem ampliar o corpus, comparar decisões de Tribunais de Justiça, examinar a aplicação do CDC em setores específicos e investigar como a ANPD e o Judiciário avaliam programas de segurança e governança.

## CONSIDERAÇÕES FINAIS

A proteção de dados pessoais é hoje direito fundamental no Brasil e impõe nova compreensão da responsabilidade civil: a LGPD não trata os dados como simples ativo econômico, mas como elemento ligado à liberdade, à privacidade, à autodeterminação informativa e ao livre desenvolvimento da personalidade.

Responsabilizar alguém por tratamento irregular exige análise conjunta da conduta, da violação de deveres legais, do dano e do nexo causal. O vazamento, isoladamente, não gera dano moral automático, segundo a orientação do STJ para dados comuns; mas a simples participação de terceiro em ataque cibernético também não afasta automaticamente a responsabilidade do agente, sendo indispensável verificar se houve medidas de segurança compatíveis com a atividade e se o evento decorreu exclusivamente de causa externa.

O modelo mais adequado combina prevenção, governança, transparência e reparação concreta — a atuação da ANPD, os direitos de informação e acesso, às medidas inibitórias e as ações coletivas complementam a indenização, sem que nenhum desses planos (ilicitude do tratamento, violação dos deveres de segurança e existência de dano moral) seja esvaziado.

A efetividade da LGPD depende menos de fórmulas abstratas e mais da avaliação documentada do risco, da conduta do agente, da natureza dos dados, da extensão da exposição e das consequências para o titular — abordagem que favorece a segurança jurídica, evita indenizações automáticas sem lesão comprovada e, ao mesmo tempo, garante tutela rigorosa quando o tratamento irregular efetivamente atinge direitos da personalidade.

## AGRADECIMENTOS, APOIO, CONFLITO DE INTERESSES E AFILIAÇÕES

O artigo foi elaborado no âmbito do curso de Direito da Faculdade de Ensino Superior de Linhares — FACELI. Não houve financiamento externo informado. Os autores declaram, até o momento, não possuir conflito de interesses relacionado ao estudo. A declaração deverá ser confirmada e ajustada pela autoria antes da submissão.

## REFERÊNCIAS

BRASIL. Autoridade Nacional de Proteção de Dados. Comunicação de incidente de segurança. Brasília, DF, 2022. Atualizado em 4 ago. 2026. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/comunicacao-de-incidentes-de-seguranca-c is. Acessado em: 20 de agosto de 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. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acessado em: 20 de agosto de 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Texto compilado. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acessado em: 20 de agosto de 2026.

BRASIL. Superior Tribunal de Justiça. Disponibilização indevida de informações pessoais em banco de dados gera dano moral presumido. Brasília, DF, 5 set. 2025. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2025/05092025-Disponibilizacao-indevida-de-informacoes-pessoais-em-banco-de-dados-gera-dano-m oral-presumido.aspx. Acessado em: 20 de agosto de 2026.

BRASIL. Superior Tribunal de Justiça. Informativo de Jurisprudência nº 838: REsp 2.147.374-SP. Brasília, DF, 4 fev. 2025. Disponível em: https://scon.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisar&aplicac ao=informativo&livre=%40CNOT%3D%27021293%27. Acessado em: 20 de agosto de 2026.

BRASIL. Superior Tribunal de Justiça. Informativo de Jurisprudência nº 871. Brasília, DF, 18 nov. 2025. Disponível em: https://scon.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedic ao&livre='0871'.cod. Acessado em: 20 de agosto de 2026.

BRASIL. Superior Tribunal de Justiça. Titular de dados vazados deve comprovar dano efetivo ao buscar indenização, decide Segunda Turma. Brasília, DF, 17 mar. 2023. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/17032023-Titular-de-dados-vazados-deve-comprovar-dano-efetivo-ao-buscar-indenizacao--deci de-Segunda-Turma.aspx. Acessado em: 20 de agosto de 2026.

CAPANEMA WA. A responsabilidade civil na Lei Geral de Proteção de Dados. Cadernos Jurídicos, São Paulo, 2020;21(53):163-170.

DONEDA D. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Revista dos Tribunais, 2021.

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