

A RESPONSABILIDADE CIVIL DECORRENTE DO USO INDEVIDO DE DADOS PESSOAIS

CIVIL LIABILITY ARISING FROM THE MISUSE OF PERSONAL DATA

Ciências Sociais Aplicadas • 01/11/2026

REGISTRO DOI: [10.70773/revistatopicos/793388366](https://doi.org/10.70773/revistatopicos/793388366)

Maria Fabíola da Fonseca Silva¹

Andressa Costenaro de Alencar²

RESUMO

Esta pesquisa tem como assunto a responsabilidade civil decorrente do uso indevido de dados pessoais, e como objetivo geral analisar quais são os justificadores capazes de gerar o direito à indenização em relação à violação de dados pessoais. A problemática que orienta o estudo é: simples violação de dados pessoais é suficiente para gerar o dever de indenizar, configurando o dano *in re ipsa*, ou se a reparação exige a demonstração de prejuízo concreto. Para tanto, adota-se abordagem qualitativa, de natureza exploratória e descritiva, desenvolvida mediante pesquisa bibliográfica e documental, com fundamento na Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), no Código Civil de 2002 e na jurisprudência brasileira. A investigação parte da análise dos fundamentos da responsabilidade civil aplicáveis à proteção de dados, examina os dispositivos da LGPD relativos à responsabilidade decorrente do tratamento e da violação de dados pessoais e identifica os elementos e circunstâncias capazes de caracterizar o dano indenizável, distinguindo o mero incidente de segurança da efetiva ocorrência de dano. Em seguida, analisa o entendimento da jurisprudência nacional acerca da configuração do dano moral presumido nas hipóteses de violação de dados pessoais. Os resultados indicam que o ordenamento brasileiro adota responsabilidade civil de natureza objetiva, fundada na teoria do risco, com base no art. 42 da LGPD e no art. 927, parágrafo único, do Código Civil, mas não sanciona o mero risco: o dever de reparar surge apenas quando o incidente de segurança se converte em prejuízo efetivo. Conclui-se que a simples violação de dados pessoais não é suficiente, por si só, para gerar o dever de indenizar, prevalecendo na jurisprudência orientação restritiva quanto ao dano *in re ipsa*, admitido apenas em hipóteses qualificadas, como a exposição de dados sensíveis, o uso fraudulento dos dados e a

violação de dados de crianças e adolescentes.

Palavras-chave: Responsabilidade civil; Proteção de dados pessoais; LGPD; Dano moral; Dano in re ipsa.

ABSTRACT

This research addresses civil liability arising from the misuse of personal data, with the general objective of analyzing the grounds that give rise to a right to compensation for personal data breaches. The central question guiding the study is whether a mere personal data breach is sufficient to trigger a duty to compensate—constituting “in re ipsa” damage—or whether reparation requires proof of actual harm. To this end, a qualitative approach of an exploratory and descriptive nature is adopted, utilizing bibliographic and documentary research based on the General Personal Data Protection Law (LGPD – Law No. 13.709/2018), the 2002 Civil Code, and Brazilian case law. The investigation begins by analyzing the foundations of civil liability applicable to data protection, examines LGPD provisions regarding liability arising from data processing and breaches, and identifies the elements and circumstances that characterize compensable harm, distinguishing between a mere security incident and the actual occurrence of damage. Subsequently, it analyzes the stance of national courts regarding the recognition of presumed non-pecuniary damage (“dano moral”) in cases of personal data breaches. The results indicate that the Brazilian legal system adopts a strict liability regime based on risk theory—grounded in Article 42 of the LGPD and Article 927, sole paragraph, of the Civil Code—but does not sanction mere risk; the duty to compensate arises only when a security incident results in actual harm. The study concludes that a simple personal data breach is not, in itself, sufficient to trigger a duty to compensate; a restrictive view regarding “in re ipsa” damage prevails in case law,

with such damage being recognized only in specific, qualified scenarios, such as the exposure of sensitive data, fraudulent use of data, and breaches involving the data of children and adolescents.

Keywords: Civil liability; Personal data protection; LGPD; Non-pecuniary damage; “In re ipsa” damage.

1. INTRODUÇÃO

A proteção de dados pessoais no Brasil está passando por um momento de consolidação teórica e prática. Isso é impulsionado pela elevação dessa garantia a um direito fundamental pela Emenda Constitucional nº 115/2022. Esse movimento legislativo reforça a ideia de que os dados não são apenas um ativo econômico ou um registro burocrático; eles são uma parte essencial da personalidade humana. Isso exige que a responsabilidade civil sirva como uma ferramenta para preservar a dignidade digital.

Diante da crescente utilização e circulação de dados pessoais, surgem questionamentos acerca da responsabilidade civil decorrente de sua violação. Nesse contexto, a presente pesquisa parte da seguinte problemática: a simples violação de dados pessoais é suficiente para gerar o dever de indenizar, configurando o dano *in re ipsa*? Busca-se, portanto, compreender se a ocorrência da violação, por si só, caracteriza dano indenizável ou se é necessária a demonstração de prejuízo efetivamente suportado pelo titular dos dados.

A presente pesquisa tem como objetivo geral analisar quais são os justificadores capazes de gerar o direito à indenização em relação à violação de dados pessoais. Para alcançar esse propósito, estabelecem-se como objetivos específicos: compreender os

fundamentos da responsabilidade civil aplicáveis à proteção de dados pessoais no ordenamento jurídico brasileiro; examinar as disposições da Lei Geral de Proteção de Dados Pessoais (LGPD) relacionadas à responsabilidade civil decorrente do tratamento e da violação de dados pessoais; identificar os elementos e circunstâncias capazes de caracterizar o dano indenizável decorrente da violação de dados pessoais, distinguindo o mero incidente de segurança da efetiva ocorrência de dano; e analisar o entendimento da jurisprudência brasileira acerca da configuração do dano moral presumido (*in re ipsa*) nas hipóteses de violação de dados pessoais.

A pesquisa adota foi de abordagem qualitativa, de natureza exploratória e descritiva, desenvolvida mediante pesquisa bibliográfica e documental. A pesquisa bibliográfica foi realizada a partir de livros, artigos científicos, dissertações, teses e demais produções acadêmicas relacionadas à responsabilidade civil, à proteção de dados pessoais e ao dano moral. A pesquisa documental compreendeu a análise da Constituição Federal, do Código Civil, da Lei nº 13.709/2018 (LGPD) e de outros diplomas normativos pertinentes, bem como de decisões judiciais e entendimentos jurisprudenciais dos tribunais brasileiros, especialmente aqueles que discutam a necessidade de demonstração do dano e a possibilidade de sua configuração *in re ipsa*. Quanto aos procedimentos, foi empregado o método dedutivo, partindo-se dos fundamentos gerais da responsabilidade civil e da proteção jurídica dos dados pessoais para examinar, especificamente, em que circunstâncias a violação de dados pode gerar o dever de indenizar.

A escolha do tema justifica-se, no âmbito acadêmico, pela crescente relevância da proteção de dados pessoais no Direito brasileiro e

pelos debates ainda existentes acerca dos limites da responsabilidade civil decorrente de incidentes envolvendo dados. A entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD) ampliou a necessidade de estudos sobre os pressupostos do dever de indenizar, especialmente quanto à distinção entre a mera violação de dados e a efetiva configuração de dano. Nesse contexto, investigar a possibilidade de reconhecimento do dano *in re ipsa* contribui para o aprofundamento da discussão doutrinária e jurisprudencial sobre a aplicação da responsabilidade civil às novas situações decorrentes do tratamento de informações pessoais.

No âmbito social, a relevância da pesquisa decorre da crescente utilização de dados pessoais por empresas, instituições públicas e plataformas digitais, aumentando a exposição dos indivíduos a incidentes de segurança e ao uso inadequado de suas informações. A discussão sobre a necessidade de comprovação do dano possui impacto direto tanto na proteção dos titulares de dados quanto na definição dos limites da responsabilização dos agentes de tratamento. Assim, compreender quais circunstâncias efetivamente justificam a indenização permite contribuir para uma tutela mais adequada dos direitos da personalidade, sem transformar toda ocorrência de violação de dados, por si só, em hipótese automática de reparação civil.

2. DISPOSIÇÕES DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) RELACIONADAS À RESPONSABILIDADE CIVIL DECORRENTE DO TRATAMENTO E DA VIOLAÇÃO DE DADOS PESSOAIS

No plano constitucional, o direito à proteção de dados pessoais foi expressamente erigido a direito fundamental pela Emenda

Constitucional 115/2022 (Brasil, 2022), que inseriu o inciso LXXIX ao art. 5º: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

A LGPD dedica o Capítulo VI do Título III à responsabilidade civil, sistematizando no Artigo 42 e seguintes as hipóteses de reparação pelos danos decorrentes do tratamento de dados pessoais. O ponto de partida normativo é o caput do 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). A norma adota, portanto, a responsabilidade de natureza objetiva, dispensando a prova de culpa do agente, dispensando-se a comprovação de culpa do agente, bastando a demonstração do dano, da atividade de tratamento e do nexo causal.

A esse modelo soma-se a cláusula geral de responsabilidade objetiva do Artigo 927, parágrafo único, do Código Civil, que impõe o dever de reparar "quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem" (Brasil, 2002). É nesse campo da responsabilidade objetiva, fundada no risco da atividade, que a proteção de dados pessoais se insere, dado o caráter intrinsecamente arriscado da atividade de tratamento de dados em larga escala.

A responsabilidade civil, no ordenamento brasileiro, estrutura-se a partir do Artigo 186 do Código Civil, segundo a qual "aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito" (Brasil, 2002). O dispositivo consagra a chamada

responsabilidade subjetiva, que se perfaz mediante a conjugação de conduta, culpa, nexo causal e dano.

Os incisos I e II do § 1º do Artigo 42 disciplina a hipótese de responsabilidade solidária entre operadores e controladores:

“I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador [...]

II- os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente. (Brasil, 2018).

Já o Artigo 43 exclui a responsabilidade do operador "não realizaram o tratamento de dados pessoais que lhes é atribuído. II- que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros. (Brasil, 2018).

Para afastar sua responsabilidade, o controlador precisa demonstrar que cumpriu de maneira efetiva as obrigações previstas na legislação, especialmente aquelas relacionadas à adoção de medidas de segurança capazes de proteger os dados pessoais. O problema é que essa demonstração nem sempre é simples. Na prática, pode recair sobre o controlador a tarefa de comprovar que determinado fato não ocorreu, transformando a produção da prova em uma questão particularmente difícil, sobretudo quando o titular

dos dados não possui acesso às informações e aos mecanismos internos utilizados no tratamento (Costa, 2019).

O Artigo 45 orienta que em caso de a violação de dados envolver relações de consumo, deve-se aplicar as regras da legislação pertinente, ou seja, o Código de Defesa do Consumidor.

No campo das relações de consumo, existe uma premissa que orienta boa parte da proteção jurídica: o consumidor ocupa uma posição de vulnerabilidade diante do fornecedor. É justamente esse desequilíbrio que ajuda a explicar a adoção da responsabilidade objetiva em determinadas situações. Quando essa lógica é transportada para as relações que envolvem o tratamento de dados pessoais, percebe-se que o titular dos dados também pode se encontrar em uma posição de vulnerabilidade, sobretudo diante do domínio técnico e informacional daqueles que coletam, armazenam e utilizam essas informações.

Essa condição encontra respaldo na própria Lei Geral de Proteção de Dados. O Artigo 42, § 2º, da LGPD permite que o juiz determine a inversão do ônus da prova quando estiver presente a hipossuficiência do titular para a produção da prova, reconhecendo que nem sempre ele terá condições de demonstrar, por seus próprios meios, como ocorreu o tratamento ou eventual violação de seus dados (Brasil, 2018). É nesse ponto que a discussão sobre a vulnerabilidade deixa de ser apenas teórica e passa a produzir efeitos concretos no processo, como destaca Gabriel Araújo Souto:

Desse modo, quando se tratar de uma relação de consumo, o mero vazamento dos dados caracteriza defeito no produto ou serviço contratado, configurando-se a responsabilidade objetiva, nos termos dos art. 12, §1º e art. 14, §1º do CDC (LGL\1990\40), por não fornecer a segurança que o consumidor pode dele esperar, através do resultado e os riscos que razoavelmente dele se esperam, consonante como art. 44, II da LGPD. Assim, em ambos os casos, demanda-se a gestão de riscos para isenção de ilicitude na gestão de dados de terceiros (Souto, 2020, p. 375).

Merece destaque também o Artigo 52, que arrola as sanções administrativas aplicáveis pela Autoridade Nacional de Proteção de Dados (ANPD), entre elas a advertência e a multa "de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 por infração" (Brasil, 2018).

É essencial distinguir que as sanções do Artigo 52 têm natureza administrativa e são aplicadas pela ANPD, enquanto a reparação do Artigo 42 tem natureza civil e depende de ação judicial.

3. ELEMENTOS E CIRCUNSTÂNCIAS CAPAZES DE CARACTERIZAR O DANO INDENIZÁVEL DECORRENTE DA VIOLAÇÃO DE DADOS PESSOAIS

A reparação civil pressupõe a existência de dano, e o ordenamento brasileiro não admite indenização por mero risco ou por abstrata possibilidade de prejuízo. O **Artigo 944 do Código Civil** consagra que "a indenização mede-se pela extensão do dano" (Brasil, 2002),

princípio que vincula o dever de reparar à efetiva materialização do prejuízo.

No âmbito da LGPD, o Artigo 42 condiciona o dever de reparar à causação de "dano patrimonial, moral, individual ou coletivo" (Brasil, 2018). A literalidade do dispositivo exige, portanto, um dano concreto, e não a mera irregularidade no tratamento. Daí a distinção central deste capítulo: o incidente de segurança não se confunde com o dano indenizável.

Define-se incidente de segurança como todo acesso, aquisição, perda ou alteração não autorizada de dados pessoais, tal como o § 1º do art. 46 da LGPD sinaliza ao impor aos agentes de tratamento a adoção de medidas de segurança aptas a proteger os dados "de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (Brasil, 2018). O art. 48 da LGPD impõe a comunicação à ANPD e ao titular quando o incidente "possa acarretar risco ou dano relevante aos titulares", o que revela que o próprio legislador reconhece a possibilidade de incidentes sem dano relevante, já que a notificação só é exigível na hipótese de risco significativo.

Extraí-se, daí, uma escala de gravidade: (i) o incidente sem risco; (ii) o incidente com risco ou dano relevante, sujeito a comunicação obrigatória; e (iii) o incidente que efetivamente se converte em dano indenizável. Apenas o último gera o dever de reparação do art. 42, pois a norma exige que se tenha "causado" dano.

A doutrina é convergente nesse sentido. Carpena (2020, p. 158) e outros autores sustentam que "a responsabilidade civil não decorre do mero vazamento, mas da demonstração de que o incidente se

converteu em prejuízo concreto ao titular". No entanto, observa a dificuldade de se provar o nexo causal entre o incidente e um prejuízo individualizado (Menke, 2021).

Elementos capazes de caracterizar o dano indenizável incluem: a exposição de dados sensíveis (Artigo 5º, II, da LGPD), a utilização indevida ou o vazamento de dados que permitam a identificação e o uso fraudulento por terceiros, a materialização de prejuízo econômico (fraudes financeiras, fraudes de identidade), e a alteração substancial da esfera existencial do titular (dano moral). O art. 5º, II define dados sensíveis como aqueles relativos à "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado eferente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (Brasil, 2018). A exposição dessas categorias tende a caracterizar dano indenizável com maior facilidade, dada a aptidão da divulgação para atingir a esfera mais íntima da personalidade.

São circunstâncias agravantes que reforçam a configuração do dano: (i) reincidência específica (mesma infração ao mesmo dispositivo legal): acréscimo de 10% por caso, limitado a 40%; (ii) ampla difusão da infração ou dano a grupos vulneráveis (crianças, idosos, portadores de deficiência); (iii) alto volume de dados pessoais envolvidos; (iv) vantagem econômica obtida com a prática ilícita; (v) não cessação da infração após notificação (Confidata, 2026).

Por outro lado, não configuram, por si sós, dano indenizável: o mero temor subjetivo de futura utilização indevida, o cadastro em listas de vazamentos sem qualquer consequência demonstrada, e a simples irregularidade formal no tratamento sem repercussão concreta;

A doutrina sustenta que a distinção entre incidente e dano se apoia no princípio da reparação integral do Artigo 944 do Código Civil, segundo o qual só há dever de reparar na medida do prejuízo efetivamente sofrido. Assim, o incidente de segurança é o fato gerador potencial; o dano indenizável é a concretização do prejuízo no patrimônio ou na esfera moral do titular.

Em síntese, a caracterização do dano indenizável decorrente da violação de dados pessoais exige a comprovação de que o incidente de segurança se converteu em prejuízo concreto, não bastando a mera irregularidade ou o vazamento em abstrato. Essa é a premissa que o próximo capítulo examina sob a ótica jurisprudencial do dano moral presumido.

4. ENTENDIMENTO DA JURISPRUDÊNCIA BRASILEIRA ACERCA DA CONFIGURAÇÃO DO DANO MORAL PRESUMIDO (IN RE IPSA) NAS HIPÓTESES DE VIOLAÇÃO DE DADOS PESSOAIS

A configuração do dano moral presumido nas hipóteses de violação de dados pessoais constitui um dos pontos mais controvertidos da aplicação da LGPD no Brasil. O tema gira em torno de uma tensão fundamental: de um lado, a responsabilidade civil objetiva adotada pelo Artigo 42 da LGPD, que dispensa a prova de culpa; de outro, a necessidade de demonstração do dano como pressuposto da reparação, conforme o Artigo 944 do Código Civil. O ponto de maior divergência reside justamente em definir se o dano moral pode ser presumido a partir do vazamento, ou se deve ser provado pelo titular.

A dogmática do dano moral *in re ipsa* remonta a uma construção jurisprudencial consolidada em hipóteses dotadas de elevada carga

ofensiva à dignidade. O Desembargador Ramon Mateo Júnior, em precedente do Superior Tribunal de Justiça observou que "o dano moral não se presume; o que se presume, em determinadas hipóteses, é o seu caráter contrário ao direito, quando a própria conduta ofensiva já revela, de forma inequívoca, a lesão à personalidade" (STJ, 2018). A distinção é relevante: o dano *in re ipsa* não afasta o dano, apenas dispensa a prova do prejuízo quando este se extrai da própria natureza do ato ilícito.

No caso específico do vazamento de dados, o Superior Tribunal de Justiça firmou orientação restritiva. No julgamento do REsp 1.737.467/SC (Primeira Turma, Rel. Min. Napoleão Nunes Maia Filho), entendeu-se o “dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações” (STJ, 2018).

A orientação foi reiterada em outros julgados da mesma Corte, que passaram a exigir, além do vazamento, a comprovação “eventual dano decorrente da exposição dessas informações”, ou seja, é necessário que se prove de que os dados foram efetivamente utilizados de forma indevida ou de que houve exposição concreta do titular a riscos (Acórdão AResp. 2.130.619) (STJ, 2022). Nesse sentido, a jurisprudência exige uma "ponte" entre o incidente e o dano, não bastando a constatação de insegurança no tratamento.

No âmbito do Supremo Tribunal Federal, o RE 1.010.606/RJ (2017), julgado sob a sistemática da repercussão geral ao analisar a presunção do dano moral em contexto de violação a direitos da personalidade envolvendo uso não autorizado da imagem de um irmão de uma falecida, fixou balizas importantes sobre os limites do

arbitramento e sobre a necessidade de lesão efetiva, contribuindo para a leitura restritiva da presunção.

Danilo Doneda (2018), acompanham essa leitura e adverte que a proteção de dados exige equilíbrio entre a tutela preventiva e a reparatória, de modo a não transformar o vazamento em fonte automática de enriquecimento de modo a não transformar o vazamento em fonte automática de enriquecimento sem causa, mas também sem deixar o titular desamparado diante de lesões efetivas.

Há, contudo, hipóteses em que a jurisprudência admite a configuração do dano moral *in re ipsa* na violação de dados pessoais. A primeira delas é a exposição de dados sensíveis (art. 5º, II, da LGPD), como dados de saúde, origem racial ou convicção religiosa, cuja divulgação atinge de modo manifesto a esfera mais íntima da personalidade (Brasil, 2018). A segunda é a utilização fraudulenta dos dados, com materialização de prejuízo, como fraudes bancárias ou de identidade. A terceira envolve a violação de dados de crianças e adolescentes, dada a proteção especial do Artigo 14 da LGPD. Nessas hipóteses, sustenta-se que o dano se extrai da própria natureza do ilícito, dispensando prova específica do prejuízo.

Em sentido inverso, a jurisprudência rejeita o dano *in re ipsa* quando se trata de mero vazamento sem consequência demonstrada, de dados de baixa sensibilidade, ou de mero temor subjetivo de futura utilização indevida, como já informado. Nesses casos, o titular que pretende reparação deve comprovar o nexo causal entre o incidente e o prejuízo concreto, à luz do Artigo 944 do Código Civil.

A síntese que se extrai da jurisprudência é a seguinte: (i) o entendimento majoritário rejeita a presunção automática do dano moral apenas pelo vazamento, exigindo prova do prejuízo; (ii) admite-se o dano *in re ipsa* quando a violação atinge dados sensíveis, quando há uso fraudulento ou quando a exposição coloca o titular em risco concreto e relevante; e (iii) reconhece-se que a inversão do ônus da prova, autorizada pelo Artigo 42, § 2º, da LGPD, mitiga a dificuldade probatória do titular sem, contudo, dispensar a demonstração do dano.

Conclui-se que a configuração do dano moral presumido na violação de dados pessoais não é automática, mas depende da conjugação entre a natureza dos dados atingidos, a repercussão concreta do incidente e a demonstração, ainda que por presunções, da lesão à esfera jurídica do titular.

5. RESULTADOS E ANÁLISE

A análise dos capítulos precedentes permite extrair resultados convergentes sobre o regime brasileiro de responsabilidade civil por violação de dados pessoais. O primeiro resultado é a consolidação da responsabilidade objetiva como eixo do sistema, firmada pelo Artigo 42 da LGPD, que dispensa a comprovação de culpa e se ancora na teoria do risco da atividade de tratamento. Esse dado normativo é reforçado pelo Artigo 927, parágrafo único, do Código Civil, que impõe a reparação quando a atividade normalmente desenvolvida implicar risco para direitos de outrem.

O segundo resultado concerne à distinção entre incidente de segurança e dano indenizável. A análise revelou que o ordenamento não sanciona o mero risco: os Artigos 46 e 48 da LGPD tratam do

dever de segurança e do dever de comunicação, e a própria exigibilidade da notificação apenas na hipótese de "risco ou dano relevante" evidencia que o legislador admitiu a existência de incidentes sem dano. Daí decorre que o dever de reparar do Artigo 42 surge somente quando o incidente se converte em prejuízo concreto, à luz do Artigo 944 do Código Civil. A análise confirma, portanto, que a cadeia reparatória exige três elos: conduta de tratamento, violação à legislação e dano efetivo.

O terceiro resultado diz respeito ao dano moral presumido. A jurisprudência analisada aponta para uma orientação majoritariamente restritiva: o mero vazamento não gera dano moral *in re ipsa*, exigindo-se a demonstração da repercussão lesiva; admite-se a presunção, contudo, em hipóteses de exposição a dados sensíveis, uso fraudulento e violação de dados de crianças e adolescentes, todos dotados de proteção reforçada pela LGPD (Artigos. 5º, II, e 14). Esse resultado revela uma tensão metodológica: embora o Artigo 42 adote a responsabilidade objetiva, a exigência probatória do dano aproxima, na prática, o regime da vítima da prova que se buscava dispensar.

Um quarto resultado, de natureza sistêmica, é a coexistência de regimes: civil (Artigo 42), administrativo (Artigo 52) e consumerista (Artigo 14 do CDC), este último aplicável quando houver relação de consumo. A análise demonstra que a integração entre esses regimes, embora coerente em tese, produz zonas de incerteza quanto ao foro, ao fundamento e aos critérios de quantificação, especialmente diante da falta de parâmetros consolidados de arbitramento e do reduzido número de decisões definitivas em matéria de vazamento de dados.

Em termos analíticos, o que se verifica é que o sistema brasileiro se caracteriza por uma responsabilidade objetiva quanto ao fundamento, mas efetiva quanto ao dano. A objetividade do Artigo 42 desloca o debate da culpa para o dano, mas a exigência de comprovação do prejuízo reintroduz, no plano probatório, uma barreira que a responsabilidade objetiva pretendia eliminar. É nesse ponto que a inversão do ônus da prova autorizada pelo Artigo 42, § 2º, assume papel central: ela mitiga a hipossuficiência do titular, mas não substitui a demonstração do dano.

A análise também evidencia que a natureza dos dados funciona como critério operacional relevante. Dados sensíveis, dados de crianças e adolescentes e dados financeiros tendem a produzir presunção mais robusta de lesão, ao passo que dados de baixa sensibilidade raramente sustentam, isoladamente, dever de reparar. A conclusão parcial é que a jurisprudência, ainda que rejeite a presunção genérica, opera com uma presunção graduada conforme a gravidade e a natureza do dado atingido.

Outro resultado relevante é a função preventiva do regime. A reparação civil não esgota a tutela: as sanções administrativas do Artigo 52 da LGPD e a atuação fiscalizatória da ANPD operam como instrumentos dissuasórios complementares, de modo que o sistema combina prevenção (Artigos 46 e 48) e reparação (Artigo 42). Essa combinação é coerente com o caráter multifacetado da proteção de dados, simultaneamente direito fundamental, direito da personalidade e objeto de tutela coletiva

6. CONSIDERAÇÕES FINAIS

A presente produção científica demonstrou que a responsabilidade civil aplicável à proteção de dados pessoais no Brasil se funda em um regime de natureza objetiva, ancorado no Artigo 42 da LGPD e na teoria do risco da atividade, reforçado pela elevação constitucional da proteção de dados a direito fundamental. A análise evidenciou que o sistema não sanciona o mero risco: a distinção entre incidente de segurança e dano indenizável, extraída da lógica dos Artigos 46, 48 e 42, que revela que apenas a concretização do prejuízo gera o dever de reparar, exigindo do intérprete a identificação dos elementos que convertem o vazamento em lesão efetiva à esfera jurídica do titular.

Ademais, que a configuração do dano moral presumido na violação de dados pessoais não é automática, prevalecendo na jurisprudência brasileira a orientação restritiva segundo a qual o mero vazamento, por si só, não gera dever de indenizar, sendo necessária a demonstração da repercussão lesiva na esfera jurídica do titular. Reconhece-se, contudo, a admissibilidade do dano *in re ipsa* em hipóteses qualificadas, exposição de dados sensíveis, uso fraudulento dos dados e violação de dados de crianças e adolescentes, nas quais a própria natureza do ilícito revela a lesão, dispensando prova específica do prejuízo. O regime, portanto, combina objetividade quanto ao fundamento com exigência de efetividade quanto ao dano, cabendo à inversão do ônus da prova prevista no art. 42, § 2º, da LGPD o papel de mitigar a hipossuficiência probatória do titular sem, todavia, dispensar a comprovação do prejuízo.

Por fim, ainda que o ordenamento brasileiro tenha avançado significativamente na tutela dos dados pessoais, a pesquisa evidenciou a necessidade de consolidação de parâmetros

jurisprudenciais estáveis para o arbitramento do dano moral e para a distinção entre incidente e dano, de modo a conferir segurança jurídica e efetividade à proteção.

Sugere-se, para trabalhos futuros, a realização de levantamento empírico sistemático de decisões dos tribunais brasileiros, a fim de mapear tendências concretas de quantificação e de reconhecimento do dano *in re ipsa*, superando a limitação metodológica aqui registrada. A proteção de dados, enquanto direito fundamental e instrumento de tutela da personalidade, exige, assim, um regime reparatório que concilie a vocação protetiva do artigo 42 da LGPD com a exigência de lesão efetiva, assegurando ao titular não apenas ressarcimento, mas também prevenção e segurança no tratamento de suas informações.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. *Emenda Constitucional nº 115, de 10 de fevereiro de 2022*. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm . Acesso em: 17 de setembro de 2026.

BRASIL. *Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil)*. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 08 de setembro de 2026.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018 (LGPD)*. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

CAPANEMA, Walter Aranha. *A responsabilidade civil na Lei Geral de Proteção de Dados*. Cadernos Jurídicos, n. 53, vol. 21. São Paulo: Escola Paulista da Magistratura, jan.-mar./2020.

CONFIDATA. As multas da LGPD: valores reais, critérios de cálculos e casos aplicados. 2026. Disponível em: <https://confidata.com.br/blog/multas-lgpd-valores-criterios-casos>. Acesso em: 23 de setembro de 2026.

COSTA, Tiago Branco da. *A responsabilidade civil decorrente da violação do Regulamento Geral sobre a Proteção de Dados*, 2019. Disponível em: http://repositorium.sdum.uminho.pt/bitstream/1822/61446/3/UNIO_EBOOK_INTEROP_2019.pdf. Acesso em: 26 setembro 2026.

DONEDA, Danilo. *Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados*. Revista de Direito do Consumidor. Vol. 27, n. 120. São Paulo: Revista dos Tribunais, nov./dez. 2018, p. 476-477.

FERREIRA, Lucia Maria T; GARCIA, Matheus. *Responsabilidade civil por vazamento de dados pessoais: análise da decisão proferida no AResp. N. 2.130.619/SP*. Civilista.com. 2024. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/1038/>. Acesso em: 18 de setembro de 2026.

MENKE, Fabiano; GOULART, Guilherme Damásio. Segurança da informação e vazamento de dados. In: DONEDA, Danilo; MENDES, Laura Schertel; RODRIGUES JR, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Coord.). *Tratado de proteção de dados pessoais*. 1. ed. Rio de Janeiro: Forense, 2021.

SOUTO, Gabriel Araújo. *Vazamento de dados no setor privado brasileiro: a gestão do risco como parâmetro para a responsabilidade empresarial*. Revista de Direito e as Novas Tecnologias, vol. 7/2020, Abr-Jun/2020, DTR\2020\7817.

SUPERIOR TRIBUNAL DE JUSTIÇA. AgI no Recurso Especial nº 1737467 – SC. 2018. In: Jusbrasil. *Superior Tribunal de Justiça – Agravo Interno no Recurso Especial*. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/stj/868166854/inteiro-teor-868166857>. Acesso em: 22 de setembro de 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA. *Agravo em Recurso Especial nº 2.130.619 – SP*. Supremo Tribunal De Justiça. 2022. Disponível em: https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=178204788&registro_numero=202201522622&peticao_numero=&publicacao_data=20230310&formato=PDF. Acesso em: 20 de setembro de 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA. *Ação indenizatória*. Vazamento de dados de usuários do bilhete único da SPTRANS. 2023.

SUPREMO TRIBUNAL FEDERAL. *Tema 786 – Aplicabilidade do direito ao esquecimento na esfera civil quando for invocado pela própria vítima ou pelos seus familiares*. 2017. Disponível em: <https://portal.stf.jus.br/jurisprudenciarepercussao/verAndamentoProcesso.asp?incidente=5091603&numeroProcesso=1010606&classeProcesso=RE&numeroTema=786>. Acesso em: 19 de setembro de 2026.

¹ Discente do curso de Direito da Faculdade de Educação Santa Terezinha (FEST). E-mail: [acesse o artigo original para visualizar o e-mail](#)

² Docente do curso de Direito da Faculdade de Educação Santa Terezinha (FEST). E-mail: [acesse o artigo original para visualizar o e-mail](#)