DOI: 10.33242/rbdc.2026.01.008

RESPONSABILIDADE CIVIL PELA DISPONIBILIZAÇÃO INDEVIDA DE DADOS PESSOAIS E DANO MORAL *IN RE IPSA*: ANÁLISE DO RESP 2.201.694/SP À LUZ DA LGPD E DO DIREITO COMPARADO

CIVIL LIABILITY FOR THE UNAUTHORIZED DISCLOSURE OF PERSONAL DATA AND MORAL DAMAGES *IN RE IPSA*: AN ANALYSIS OF RESP 2.201.694/SP IN LIGHT OF THE LGPD AND COMPARATIVE LAW

Lucas Melo Rodrigues de Sousa

Graduado em Direito pelo Centro Universitário Dom Helder. Especialista em Direito do Trabalho e Previdenciário e em Direito Processual Civil pela Pontifícia Universidade Católica de Minas Gerais. Desenvolve pesquisas nas áreas de direitos humanos, direitos sociais, tecnologia e diversidade, com produção acadêmica voltada à análise crítica das transformações sociais, institucionais e normativas contemporâneas. Possui experiência em ensino jurídico, produção de conteúdo didático, monitoria acadêmica e revisão de periódico científico. É colunista do portal Entreparágrafos, onde assina a coluna Direito em Plural, dedicada ao debate sobre direitos humanos, diversidade, inclusão e direitos fundamentais. Orcid: https://orcid.org/0000-0002-9718-8075
E-mail: lucasrmelo@yahoo.com

Resumo: O presente artigo analisa o julgamento do Recurso Especial nº 2.201.694/SP pelo Superior Tribunal de Justiça, que reconheceu a configuração de dano moral *in re ipsa* na hipótese de disponibilização indevida, a terceiros, de informações pessoais mantidas em banco de dados. O objetivo consiste em investigar os fundamentos jurídicos do precedente e sua inserção no contexto da responsabilidade civil contemporânea, à luz da Lei Geral de Proteção de Dados e do direito comparado. Adota-se metodologia qualitativa, de natureza bibliográfica e jurisprudencial, com abordagem dedutiva, articulando o exame do julgado com a doutrina especializada e decisões nacionais e estrangeiras. Os resultados indicam uma tendência de adoção de critérios objetivos na responsabilidade civil digital, com deslocamento do foco da prova do dano para a proteção da dignidade informacional e da autodeterminação do titular dos dados. Verifica-se, ainda, a convergência entre o ordenamento jurídico brasileiro e o modelo europeu de proteção de dados, embora com diferenças quanto à exigência de demonstração do dano. Como contribuição teórica, propõe-se a adoção de critérios multifatoriais para a aplicação do dano moral presumido, considerando a natureza dos dados, a extensão da violação, a

conduta do agente e o potencial de dano existencial. Conclui-se que o precedente analisado representa marco relevante na adaptação da responsabilidade civil à sociedade digital, ao mesmo tempo em que impõe desafios relacionados à segurança jurídica e à delimitação do dano moral.

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

Abstract: This article examines Special Appeal No. 2.201.694/SP, decided by the Brazilian Superior Court of Justice, which recognized presumed moral damages (*in re ipsa*) where personal information held in a database was unlawfully made available to third parties. The study analyzes the legal foundations of the precedent and its role within contemporary civil liability in light of the Brazilian General Data Protection Law and comparative law. It adopts a qualitative, bibliographical and case-law methodology, using a deductive approach to connect the judgment with specialized scholarship and national and foreign decisions. The findings indicate a trend toward objective standards in digital civil liability, shifting attention from proof of actual harm to the protection of informational dignity and the data subject's self-determination. The study also identifies convergence between Brazilian law and the European data-protection framework, although differences remain regarding the requirement to demonstrate damage. As a theoretical contribution, the article proposes a multifactorial framework for presumed moral damages, considering the nature of the data, the scope of the violation, the conduct of the agent and the potential for existential harm. It concludes that the precedent is a relevant milestone in adapting civil liability to the digital society, while raising challenges concerning legal certainty and the limits of moral damages.

Keywords: Civil liability. Personal data protection. Moral damages *in re ipsa*. LGPD. Informational self-determination.

Sumário: Introdução – **1** Identificação do julgado e delimitação da controvérsia jurídica – **2** Análise crítica da *ratio decidendi* e diálogo com o direito comparado – **3** Impactos econômicos, regulatórios e sistêmicos da responsabilidade civil digital – **4** Proposta de critérios para aplicação do dano moral *in re ipsa* em casos de disponibilização indevida de dados – Considerações finais – Referências

Introdução

A crescente digitalização das relações sociais e econômicas tem reconfigurado profundamente os contornos tradicionais do Direito Civil, impondo novos desafios à tutela dos direitos da personalidade. Em uma sociedade orientada pela circulação massiva de informações, os dados pessoais assumem centralidade não apenas como ativos econômicos, mas como extensões da própria identidade do indivíduo, vinculando-se diretamente à sua autonomia, liberdade e dignidade. Nesse contexto, a proteção de dados emerge como dimensão essencial dos direitos fundamentais, ultrapassando a lógica clássica da privacidade para afirmar-se como um verdadeiro direito à autodeterminação informativa.[1]

[1] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019.

A promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) inaugura, no ordenamento jurídico brasileiro, um paradigma normativo orientado pela responsabilização dos agentes de tratamento e pela centralidade do titular dos dados. Tal diploma legal incorpora princípios estruturantes, como a finalidade, a necessidade e a segurança, ao mesmo tempo em que estabelece mecanismos de responsabilização civil voltados à reparação de danos decorrentes do uso indevido de informações pessoais. Nesse cenário, a responsabilidade civil passa a desempenhar função não apenas reparatória, mas também preventiva e pedagógica, especialmente diante da natureza difusa e potencialmente irreversível dos danos informacionais.[2]

É nesse ambiente de transformação que se insere o julgamento do Recurso Especial nº 2.201.694/SP pelo Superior Tribunal de Justiça, o qual representa marco relevante na consolidação da responsabilidade civil digital no Brasil. Ao reconhecer a configuração do dano moral *in re ipsa* diante da disponibilização indevida de informações pessoais a terceiros, a Corte sinaliza uma inflexão interpretativa significativa, deslocando o eixo da análise jurídica da prova concreta do prejuízo para a própria violação do direito da personalidade. Tal entendimento reflete a percepção de que, na sociedade informacional, a simples perda do controle sobre os dados já constitui lesão juridicamente relevante, independentemente da demonstração de consequências materiais específicas.[3]

A decisão dialoga diretamente com a tendência de constitucionalização do Direito Civil, na medida em que reforça a centralidade da dignidade da pessoa humana como vetor interpretativo das relações privadas. Ademais, aproxima o ordenamento jurídico brasileiro dos modelos internacionais de proteção de dados, notadamente o europeu, no qual a tutela da personalidade assume caráter robusto e preventivo, com reconhecimento de danos morais mesmo na ausência de prejuízo econômico comprovado.[4]

Diante desse cenário, o presente artigo tem por objetivo analisar criticamente o REsp 2.201.694/SP, investigando seus fundamentos jurídicos, sua inserção no contexto normativo da LGPD e seus impactos para a evolução da responsabilidade civil contemporânea. Para tanto, adota-se metodologia qualitativa, de natureza bibliográfica e jurisprudencial, com abordagem dedutiva, buscando articular o precedente judicial com a doutrina especializada e com experiências comparadas no

[2] MIRAGEM, Bruno. *Responsabilidade civil*. São Paulo: Forense, 2021.

[3] BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 2.201.694/SP. Terceira Turma. Relator Ministro Ricardo Villas Bôas Cueva. Relatora para o acórdão Ministra Nancy Andrighi. Julgado em 5 ago. 2025. Diário da Justiça Eletrônico Nacional, 15 ago. 2025.

[4] MARTINS-COSTA, Judith. *A boa-fé no direito privado*: sistema e tópica no processo obrigacional. São Paulo: Revista dos Tribunais, 2018.

direito estrangeiro. Parte-se da hipótese de que o referido julgado contribui para a consolidação de um modelo de responsabilidade civil orientado pela proteção da dignidade informacional, ainda que suscite desafios quanto à delimitação do dano moral e à segurança jurídica.

1 Identificação do julgado e delimitação da controvérsia jurídica

O Recurso Especial nº 2.201.694/SP, julgado pelo Superior Tribunal de Justiça em 2025, insere-se no contexto de consolidação da responsabilidade civil no ambiente digital, especialmente no que se refere à proteção de dados pessoais enquanto dimensão dos direitos da personalidade. A controvérsia central submetida à apreciação da Corte consistiu em determinar se a divulgação indevida de dados pessoais seria suficiente, por si só, para ensejar a configuração de dano moral indenizável, ou se seria necessária a demonstração concreta de prejuízo experimentado pelo titular dos dados.

Do ponto de vista fático, a demanda originou-se da disponibilização, por agência de informações de crédito, de dados cadastrais e de adimplemento a terceiros, sem prévia comunicação e sem consentimento do titular. A discussão jurídica deslocou-se, portanto, para a extensão do dano e para a necessidade de sua comprovação, revelando a tensão entre os pressupostos tradicionais da responsabilidade civil e as novas exigências impostas pela sociedade informacional.

A decisão proferida pelo Superior Tribunal de Justiça firmou entendimento no sentido de que a disponibilização indevida de informações cadastrais ou de adimplemento mantidas em banco de dados, em desacordo com a legislação aplicável, configura dano moral *in re ipsa*, dispensando a comprovação específica do prejuízo. Tal posicionamento reconhece que, no ambiente digital, a perda de controle sobre informações pessoais pode produzir lesão autônoma aos direitos da personalidade.

Sob a perspectiva da teoria geral da responsabilidade civil, o julgado revela uma aproximação com modelos de objetivação da responsabilidade, nos quais o foco se desloca da culpa para o risco inerente à atividade desenvolvida. Como observa Miragem, a responsabilidade civil contemporânea tem se orientado por uma lógica de redistribuição dos riscos sociais, especialmente em contextos marcados por assimetrias informacionais e tecnológicas. Nesse sentido, a atividade de tratamento de dados pessoais, por sua própria natureza, envolve riscos elevados à esfera jurídica dos titulares, justificando a adoção de critérios mais protetivos.[5]

[5] MIRAGEM, Bruno. *Responsabilidade civil*. São Paulo: Forense, 2021.

Além disso, a decisão dialoga diretamente com a noção de autodeterminação informativa, concebida como o direito do indivíduo de controlar o fluxo de suas informações pessoais. Tal conceito, desenvolvido no âmbito do direito constitucional alemão e posteriormente incorporado à doutrina brasileira, reforça a ideia de que a simples perda de controle sobre os dados já configura lesão juridicamente relevante, independentemente da comprovação de danos materiais ou psicológicos concretos.[6]

A *ratio decidendi* do julgado, portanto, funda-se na compreensão de que a proteção de dados pessoais integra o núcleo essencial dos direitos da personalidade, de modo que sua violação implica, por si só, afronta à dignidade da pessoa humana. Essa perspectiva está em consonância com o movimento de constitucionalização do direito privado, no qual os institutos civis passam a ser reinterpretados à luz dos valores e princípios constitucionais, especialmente a dignidade, a liberdade e a igualdade.[7]

Importa destacar, ainda, que o entendimento adotado pelo Superior Tribunal de Justiça não representa ruptura isolada, mas sim a consolidação de uma tendência jurisprudencial mais ampla, já perceptível em decisões anteriores envolvendo danos morais presumidos em contextos de violação de direitos fundamentais. Contudo, sua aplicação ao campo da proteção de dados pessoais evidencia um avanço qualitativo, na medida em que reconhece as especificidades do dano informacional e a insuficiência dos modelos tradicionais para sua adequada tutela.

Nesse sentido, a controvérsia analisada no REsp 2.201.694/SP transcende o caso concreto, projetando efeitos estruturais sobre o sistema de responsabilidade civil brasileiro. Ao admitir a presunção do dano moral em hipóteses de disponibilização indevida de dados, o STJ contribui para a construção de um modelo jurídico mais sensível às dinâmicas da sociedade digital, ainda que tal avanço imponha desafios relevantes quanto à delimitação dos critérios de responsabilização e à prevenção de eventuais distorções, como a banalização do dano moral.

2 Análise crítica da *ratio decidendi* e diálogo com o direito comparado

A consolidação do entendimento do Superior Tribunal de Justiça no REsp 2.201.694/SP, ao admitir o dano moral *in re ipsa* em hipóteses de disponibilização

[6] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019.

[7] MARTINS-COSTA, Judith. *A boa-fé no direito privado*: sistema e tópica no processo obrigacional. São Paulo: Revista dos Tribunais, 2018.

indevida de dados pessoais, revela não apenas uma evolução interpretativa pontual, mas uma reconfiguração estrutural da responsabilidade civil brasileira diante das transformações impostas pela sociedade digital. Tal inflexão exige análise crítica que ultrapasse a mera descrição do precedente, situando-o no contexto mais amplo da teoria do dano, da função da responsabilidade civil e da convergência com experiências jurídicas estrangeiras.

Sob o prisma da teoria geral da responsabilidade civil, a decisão evidencia a superação progressiva do paradigma clássico centrado na comprovação empírica do dano, em favor de um modelo orientado pela tutela preventiva de direitos fundamentais. Tradicionalmente, a responsabilidade civil exigia a demonstração concreta do prejuízo como elemento indispensável à reparação. Contudo, em contextos marcados por riscos difusos e danos de difícil mensuração, como aqueles relacionados ao tratamento de dados pessoais, essa exigência revela-se insuficiente para assegurar proteção efetiva ao indivíduo.[8]

Nesse sentido, o reconhecimento do dano moral presumido encontra fundamento na própria natureza do bem jurídico tutelado. Os dados pessoais, enquanto projeções da personalidade, integram a esfera existencial do indivíduo, de modo que sua violação implica, necessariamente, uma lesão à dignidade, ainda que não se possa identificar de imediato consequências concretas ou quantificáveis. Como destaca Doneda, a proteção de dados pessoais não se limita à prevenção de danos econômicos, mas visa assegurar o controle do indivíduo sobre sua própria identidade informacional, o que justifica a adoção de mecanismos de tutela mais rigorosos.[9]

A decisão do STJ, portanto, alinha-se à concepção contemporânea de dano enquanto categoria jurídica autônoma em relação à sua manifestação empírica, aproximando-se da noção de dano existencial. Tal perspectiva tem sido amplamente desenvolvida na doutrina civil-constitucional brasileira, que enfatiza a centralidade da dignidade da pessoa humana como critério de interpretação dos institutos privados. Nessa linha, a simples violação de um direito fundamental já é suficiente para caracterizar o dano, independentemente da demonstração de repercussões externas.[10]

Todavia, essa ampliação do conceito de dano não está isenta de críticas. Um dos principais riscos associados à presunção do dano moral reside na possibilidade de sua banalização, com consequente enfraquecimento de sua função simbólica e

[8] MIRAGEM, Bruno. *Responsabilidade civil*. São Paulo: Forense, 2021.

[9] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019.

[10] MARTINS-COSTA, Judith. *A boa-fé no direito privado*: sistema e tópica no processo obrigacional. São Paulo: Revista dos Tribunais, 2018.

reparatória. A ausência de critérios objetivos para delimitar as hipóteses de aplicação do dano *in re ipsa* pode gerar insegurança jurídica, especialmente em contextos nos quais a gravidade da violação não é evidente. Nesse ponto, a doutrina alerta para a necessidade de construção de parâmetros normativos que permitam diferenciar situações de efetiva lesão à dignidade daquelas em que a irregularidade não ultrapassa o plano da ilicitude formal.[11]

A análise comparada revela que essa tensão não é exclusiva do ordenamento brasileiro. No âmbito da União Europeia, a aplicação do Regulamento Geral de Proteção de Dados tem enfrentado desafios semelhantes. O Tribunal de Justiça da União Europeia, no caso Österreichische Post, decidiu que a mera violação da norma de proteção de dados não é suficiente, por si só, para gerar direito à indenização, exigindo a demonstração de dano, ainda que de natureza não patrimonial. Entretanto, o Tribunal adotou interpretação flexível quanto à extensão desse dano, admitindo que ele pode ser mínimo ou de difícil comprovação, desde que não seja meramente hipotético.[12]

Essa posição europeia evidencia uma diferença relevante em relação ao entendimento do STJ. Enquanto o modelo europeu busca equilibrar a proteção do titular com a necessidade de evitar indenizações automáticas, o precedente brasileiro tende a reforçar a presunção do dano em determinadas hipóteses, especialmente quando envolvem dados sensíveis. Ainda assim, ambos os sistemas convergem quanto ao reconhecimento de que os danos informacionais não podem ser analisados segundo os parâmetros tradicionais da responsabilidade civil, exigindo adaptações metodológicas e conceituais.

No plano constitucional, a decisão do STJ também encontra respaldo na jurisprudência do Supremo Tribunal Federal, que tem reconhecido a proteção de dados pessoais como direito fundamental autônomo.[13] Tal entendimento reforça a ideia de que a tutela da personalidade no ambiente digital deve ser interpretada à luz da Constituição, o que legitima a adoção de soluções mais protetivas no âmbito infraconstitucional. Como observa Mendes, a incorporação da proteção de dados ao catálogo de direitos fundamentais implica a necessidade de revisão dos critérios tradicionais de responsabilidade civil, de modo a assegurar sua efetividade.[14]

---

11 MIRAGEM, Bruno. *Responsabilidade civil*. São Paulo: Forense, 2021.

12 UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Processo C-300/21, UI v. Österreichische Post AG. Julgado em 4 maio 2023.

13 BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6.387/DF. Relatora Ministra Rosa Weber. Medida cautelar julgada em 7 maio 2020.

14 MENDES, Laura Schertel; DONEDA, Danilo. *Proteção de dados pessoais*: privacidade, autodeterminação informativa e regulação. São Paulo: Saraiva, 2018.

Além disso, a decisão dialoga com a teoria do risco, ao reconhecer que determinadas atividades, por sua própria natureza, implicam exposição elevada a danos potenciais. O tratamento de dados pessoais, especialmente em larga escala, configura atividade de risco, na medida em que envolve a manipulação de informações sensíveis e a possibilidade de impactos amplos e irreversíveis. Nesse contexto, a responsabilização civil assume função de redistribuição dos riscos sociais, transferindo ao agente que se beneficia da atividade o ônus decorrente de eventuais danos.[15]

Em síntese, o REsp 2.201.694/SP representa um avanço significativo na adaptação da responsabilidade civil brasileira às exigências da sociedade digital, ao reconhecer a especificidade do dano informacional e a necessidade de mecanismos de tutela mais eficazes. Contudo, sua consolidação como paradigma interpretativo exige o desenvolvimento de critérios mais precisos para a aplicação do dano moral presumido, de modo a conciliar a proteção da dignidade com a segurança jurídica e a racionalidade do sistema.

3 Impactos econômicos, regulatórios e sistêmicos da responsabilidade civil digital

A consolidação do entendimento jurisprudencial que admite o dano moral *in re ipsa* em casos de disponibilização indevida de dados pessoais projeta efeitos que transcendem o plano estritamente jurídico, alcançando dimensões econômicas, regulatórias e estruturais do mercado digital. A responsabilidade civil, nesse contexto, deixa de operar apenas como mecanismo de reparação *ex post* e passa a desempenhar função regulatória indireta, influenciando comportamentos organizacionais e padrões de governança informacional.

Sob a perspectiva da análise econômica do direito, a ampliação da responsabilidade civil pode ser compreendida como instrumento de internalização de externalidades negativas. O tratamento de dados pessoais, especialmente em larga escala, gera riscos que, na ausência de mecanismos adequados de responsabilização, tendem a ser suportados exclusivamente pelos titulares dos dados. Ao impor ao agente de tratamento o dever de indenizar mesmo na ausência de prova concreta do dano, o sistema jurídico cria incentivos para a adoção de medidas preventivas, como investimentos em segurança da informação, programas de *compliance* e estruturas de governança de dados.[16]

[15] BECK, Ulrich. *Sociedade de risco*: rumo a uma outra modernidade. 2. ed. São Paulo: Editora 34, 2011.
[16] POSNER, Richard A. *Análise econômica do direito*. 9. ed. São Paulo: Atlas, 2014.

Nesse sentido, a Lei Geral de Proteção de Dados estabelece um modelo normativo orientado pela *accountability*, no qual os agentes de tratamento devem demonstrar a adoção de medidas eficazes para garantir a conformidade com a legislação. A responsabilidade civil atua, portanto, como mecanismo complementar de *enforcement*, reforçando a eficácia dos princípios previstos no art. 6º da LGPD, especialmente aqueles relacionados à segurança, prevenção e responsabilização.

Contudo, a objetivação do dano moral em hipóteses de vazamento de dados também suscita preocupações relevantes do ponto de vista econômico. A possibilidade de condenações automáticas pode gerar aumento significativo da litigiosidade, com impactos diretos sobre o custo de operação das empresas, sobretudo aquelas de menor porte. Esse cenário pode produzir efeitos indesejados, como a retração de investimentos em inovação ou a adoção de estratégias excessivamente defensivas, comprometendo a dinâmica do mercado digital.

A literatura econômica alerta que sistemas de responsabilidade civil excessivamente rigorosos podem gerar efeitos de sobreinclusão, nos quais agentes são responsabilizados mesmo em situações de baixo risco ou de dano mínimo, resultando em alocação ineficiente de recursos. Nesse contexto, a ausência de critérios claros para a quantificação do dano moral pode contribuir para a imprevisibilidade das decisões judiciais, afetando a segurança jurídica e a estabilidade das relações econômicas.[17]

Por outro lado, a experiência comparada demonstra que a adoção de modelos mais protetivos não necessariamente inviabiliza o desenvolvimento econômico. No âmbito da União Europeia, a aplicação do Regulamento Geral de Proteção de Dados tem promovido a elevação dos padrões de proteção sem impedir a expansão do mercado digital. Ao contrário, a previsibilidade normativa e a uniformização de critérios têm contribuído para a construção de um ambiente de confiança, essencial para a economia baseada em dados.

No Brasil, a consolidação de entendimentos jurisprudenciais como o firmado no REsp 2.201.694/SP pode desempenhar papel semelhante, desde que acompanhada da construção de parâmetros objetivos para a aplicação da responsabilidade civil. A definição de critérios como a natureza dos dados envolvidos, a gravidade da violação, a conduta do agente e a extensão do risco gerado pode contribuir para equilibrar a proteção do titular com a segurança jurídica dos agentes econômicos.

Além disso, a responsabilidade civil digital deve ser compreendida em articulação com outros mecanismos regulatórios previstos na LGPD, como as sanções administrativas aplicáveis pela Autoridade Nacional de Proteção de Dados. A coexistência de múltiplos instrumentos de *enforcement* exige coordenação institucional

[17] SHAVELL, Steven. *Foundations of economic analysis of law*. Cambridge: Harvard University Press, 2004.

e coerência interpretativa, a fim de evitar sobreposição de penalidades e garantir a proporcionalidade das medidas adotadas.

Outro aspecto relevante diz respeito à função pedagógica da responsabilidade civil. Ao reconhecer a presunção do dano moral em determinadas hipóteses, o Judiciário sinaliza a intolerância do ordenamento jurídico em relação a práticas negligentes no tratamento de dados pessoais. Esse efeito simbólico contribui para a formação de uma cultura de proteção de dados, na qual a privacidade e a segurança informacional são incorporadas como valores estruturantes das atividades econômicas.

Em síntese, os impactos decorrentes da ampliação da responsabilidade civil digital são ambivalentes. De um lado, promovem maior proteção aos titulares de dados e incentivam práticas mais responsáveis por parte dos agentes de tratamento. De outro, impõem desafios relacionados à previsibilidade, à proporcionalidade e à eficiência econômica do sistema. A consolidação desse modelo dependerá, em última análise, da capacidade do direito brasileiro de desenvolver critérios interpretativos que conciliem a tutela da dignidade com a racionalidade econômica e a segurança jurídica.

4 Proposta de critérios para aplicação do dano moral *in re ipsa* em casos de disponibilização indevida de dados

A consolidação jurisprudencial do dano moral presumido em hipóteses de violação de dados pessoais, embora represente avanço significativo na tutela da dignidade informacional, impõe a necessidade de construção de parâmetros interpretativos que assegurem coerência, proporcionalidade e segurança jurídica. A ausência de critérios objetivos pode conduzir à banalização do instituto, comprometendo sua função normativa e simbólica no sistema de responsabilidade civil.

Nesse contexto, propõe-se a adoção de um modelo estruturado de análise, capaz de orientar a aplicação do dano moral *in re ipsa* a partir de elementos normativos e fáticos relevantes.

4.1 Natureza dos dados envolvidos

A distinção entre dados pessoais comuns e dados sensíveis deve assumir papel central na aferição do dano. Informações relativas à saúde, orientação sexual, convicções religiosas ou dados biométricos apresentam maior potencial lesivo, justificando a presunção do dano de forma mais intensa. Tal diferenciação encontra respaldo na própria Lei Geral de Proteção de Dados, que atribui regime jurídico mais rigoroso aos dados sensíveis.

4.2 Extensão e alcance da divulgação

A amplitude da divulgação constitui critério relevante para a aferição da gravidade da violação. Divulgações massivas ou com ampla circulação pública tendem a gerar maior risco à esfera jurídica do titular, ao passo que exposições restritas podem demandar análise mais contextualizada.

4.3 Grau de culpa ou risco da atividade

Embora a responsabilidade civil em matéria de dados pessoais tenda à objetivação, o grau de diligência do agente não deve ser completamente desconsiderado. A existência de falhas estruturais, ausência de medidas de segurança ou descumprimento de deveres legais reforça a presunção do dano e justifica maior rigor na responsabilização. Por outro lado, situações de caso fortuito ou adoção comprovada de medidas adequadas podem influenciar a quantificação da indenização.

4.4 Potencial de dano existencial

A análise deve considerar não apenas o dano concreto, mas o potencial de impacto sobre a esfera existencial do indivíduo. A exposição de dados pode gerar riscos futuros indeterminados, como discriminação, fraudes ou restrições de acesso a oportunidades sociais e econômicas. Esse caráter prospectivo do dano informacional justifica a flexibilização da exigência probatória.

4.5 Conduta posterior do agente

A reação do agente após a violação também deve ser considerada. A adoção de medidas imediatas de contenção, comunicação transparente e mitigação dos danos pode atenuar a responsabilização, enquanto a omissão ou tentativa de ocultação agrava a ilicitude.

4.6 Função preventiva e pedagógica da indenização

A fixação do valor indenizatório deve observar não apenas a extensão do dano, mas também sua função preventiva. A responsabilidade civil, nesse contexto, deve atuar como instrumento de indução de condutas, incentivando a adoção

de padrões elevados de proteção de dados. Como destaca a doutrina, a indenização deve ser suficiente para desestimular práticas negligentes, sem, contudo, configurar enriquecimento sem causa.[18]

Assim, a aplicação do dano moral *in re ipsa* em matéria de proteção de dados deve ser orientada por um modelo multifatorial que combine: (i) natureza dos dados; (ii) extensão da divulgação; (iii) conduta do agente; (iv) potencial de dano; e (v) função preventiva.

Tal abordagem permite superar a dicotomia entre automatização e excessiva rigidez, promovendo um equilíbrio entre a proteção da dignidade e a segurança jurídica.

Considerações finais

A análise do REsp 2.201.694/SP evidencia que a responsabilidade civil brasileira se encontra em processo de reconfiguração estrutural diante das exigências impostas pela sociedade digital. Ao reconhecer a possibilidade de configuração do dano moral *in re ipsa* em hipóteses de disponibilização indevida de dados pessoais, o Superior Tribunal de Justiça não apenas resolve uma controvérsia pontual, mas sinaliza uma inflexão paradigmática na compreensão do dano e na função da responsabilidade civil contemporânea.

O precedente examinado revela a progressiva superação do modelo clássico centrado na comprovação empírica do prejuízo, em favor de uma lógica orientada pela proteção preventiva da dignidade da pessoa humana e pela tutela da autodeterminação informativa. Nesse novo cenário, o dano deixa de ser compreendido exclusivamente como resultado concreto e mensurável, passando a abranger também situações de risco, exposição e perda de controle sobre informações pessoais, cuja relevância jurídica decorre de sua própria potencialidade lesiva.

A decisão alinha-se ao movimento de constitucionalização do Direito Civil, ao reafirmar a centralidade dos direitos fundamentais na interpretação das relações privadas, e aproxima o ordenamento jurídico brasileiro de modelos internacionais, especialmente o europeu, nos quais a proteção de dados pessoais assume caráter robusto e preventivo. Ao mesmo tempo, evidencia a necessidade de adaptação dos institutos tradicionais da responsabilidade civil às especificidades do dano informacional, marcado por sua natureza difusa, imaterial e frequentemente prospectiva.

[18] MIRAGEM, Bruno. *Responsabilidade civil*. São Paulo: Forense, 2021.

Não obstante os avanços identificados, a consolidação desse entendimento jurisprudencial impõe desafios relevantes. A presunção do dano moral, se aplicada de forma indiscriminada, pode comprometer a segurança jurídica e favorecer a banalização do instituto, esvaziando sua função normativa. Nesse sentido, demonstrou-se ao longo do trabalho a importância da construção de critérios interpretativos capazes de orientar a aplicação do dano *in re ipsa*, garantindo equilíbrio entre a efetividade da tutela dos direitos da personalidade e a racionalidade do sistema jurídico.

A proposta de um modelo multifatorial, baseado na natureza dos dados, na extensão da violação, na conduta do agente e no potencial de dano existencial, apresenta-se como caminho possível para a harmonização desses interesses. Tal abordagem permite superar tanto o formalismo excessivo quanto a automatização da responsabilidade, promovendo decisões mais proporcionais, coerentes e sensíveis às particularidades do caso concreto.

Em termos mais amplos, o precedente analisado confirma a emergência de um novo paradigma de responsabilidade civil, no qual a função preventiva e regulatória assume protagonismo, especialmente em contextos de elevada complexidade tecnológica. A responsabilidade civil deixa, assim, de atuar apenas como instrumento de recomposição patrimonial para assumir papel ativo na conformação de comportamentos e na proteção de bens jurídicos fundamentais.

Conclui-se, portanto, que o REsp 2.201.694/SP constitui marco relevante na evolução do direito civil brasileiro, ao incorporar as demandas da sociedade da informação e ao reafirmar o compromisso do ordenamento jurídico com a proteção da dignidade humana em suas múltiplas dimensões. Sua consolidação como paradigma interpretativo dependerá, contudo, da capacidade da doutrina e da jurisprudência de desenvolver critérios consistentes que assegurem, simultaneamente, proteção efetiva e segurança jurídica.

Referências

BECK, Ulrich. *Sociedade de risco*: rumo a uma outra modernidade. 2. ed. São Paulo: Editora 34, 2011.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Senado Federal, 1988.

BRASIL. *Lei nº 12.414, de 9 de junho de 2011*. Disciplina a formação e consulta a bancos de dados com informações de adimplemento de pessoas naturais ou de pessoas jurídicas para formação de histórico de crédito. Brasília, DF: Presidência da República, 2011.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 2.201.694/SP. Terceira Turma. Relator Ministro Ricardo Villas Bôas Cueva. Relatora para o acórdão Ministra Nancy Andrighi. Julgado em 5 ago. 2025. *Diário da Justiça Eletrônico Nacional*, 15 ago. 2025.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade nº 6.387/DF*. Relatora Ministra Rosa Weber. Medida cautelar julgada em 7 maio 2020.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019.

MARTINS-COSTA, Judith. *A boa-fé no direito privado*: sistema e tópica no processo obrigacional. São Paulo: Revista dos Tribunais, 2018.

MENDES, Laura Schertel; DONEDA, Danilo. *Proteção de dados pessoais*: privacidade, autodeterminação informativa e regulação. São Paulo: Saraiva, 2018.

MIRAGEM, Bruno. *Responsabilidade civil*. São Paulo: Forense, 2021.

POSNER, Richard A. *Análise econômica do direito*. 9. ed. São Paulo: Atlas, 2014.

SHAVELL, Steven. *Foundations of economic analysis of law*. Cambridge: Harvard University Press, 2004.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Processo C-300/21, UI v. Österreichische Post AG. Julgado em 4 maio 2023.

Informação bibliográfica deste texto, conforme a NBR 6023:2025 da Associação Brasileira de Normas Técnicas (ABNT):

SOUSA, Lucas Melo Rodrigues de. Responsabilidade civil pela disponibilização indevida de dados pessoais e dano moral in re ipsa: análise do REsp 2.201.694/SP à luz da LGPD e do direito comparado. *Revista Brasileira de Direito Civil – RBDCivil*, Belo Horizonte, v. 35, n. 1, p. 197-210, jan./mar. 2026. DOI: 10.33242/rbdc.2026.01.008.

Recebido em: 31.03.2026
Aprovado em: 02.07.2026