Revista Iberoamericana de Derecho, Cultura y Ambiente

Edición Nº8 – Diciembre de 2025

Capítulo de Derecho Civil y Comercial

www.aidca.org/revista

RESPONSABILIDADE CIVIL POR DANO MORAL EM TRATAMENTO IRREGULAR DE DADOS PESSOAIS NÃO-SENSÍVEIS: UM ESTUDO A PARTIR DA JURISPRUDÊNCIA DO SUPERIOR TRIBUNAL DE JUSTIÇA (STJ)

RESPONSABILIDAD CIVIL POR DAÑO MORAL EN CASOS DE MANEJO INDEBIDO DE DATOS PERSONALES NO SENSIBLES: UN ESTUDIO CON BASE EN LA JURISPRUDENCIA DEL TRIBUNAL SUPERIOR DE JUSTICIA (STJ)

Alexandria dos Santos Alexim[1]

[1] Advogada. Doutora em Ciência Política – IUPERJ – Instituto de Pesquisas do Rio de Janeiro - Universidade Candido Mendes. Mestre em Relações Internacionais pelo Centro Brasileiro de Estudos Latino Americanos. Professora e Pesquisadora do Programa de Doutorado e Mestrado do IUPERJ - UCAM - Professora e Pesquisadora do Mestrado em Direito da Universidade Candido Mendes - UCAM, Professora de Direito Internacional e Direito Civil da graduação em Direito da Universidade Candido Mendes. Pesquisadora Líder do Grupo de Pesquisas em Direito Internacional da Universidade Candido Mendes. Professora da Pós Graduação da PUC Paraná, Professora visitante da Pós Graduação em Direito do CEPED UERJ – Universidade do Estado do Rio de Janeiro e da MLAW – Maritime Law Academy. Membro da ABDI – Associação Brasileira de Direito Internacional. Membro da AICDA – Associação Iberoamericana de Direito, Cultura e Ambiente na Argentina. Membro da LIMAA – Liga Mundial de Advogados Ambientalistas – México. Membro da FISAT – Fundação Sustentabilidade Ambiental e Territorial – África, América e Europa. E-mail: asalexim@uol.com.br.

[2]Advogada, formada pela Universidade Candido Mendes.

Beatriz Yasmin Gonçalves Jordy[2]

RESUMO: A proteção de dados pessoais foi incluída no rol das Garantias e Direitos fundamentais protegidos pela Constituição Federal de 1988, visto que os dados pessoais passaram a integrar os direitos de personalidade dos cidadãos. A partir de 2020, quando a Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/18) entrou em vigor, as violações às obrigações impostas pelo recente marco normativo se tornaram objeto de disputa judicial em ações de responsabilidade civil, visando discutir a possibilidade de reparação por dano moral em caso de tratamento irregular de dados pessoais. Sobre isso, num primeiro momento da tutela jurisdicional do tema, o STJ firmou o entendimento de que o dano moral seria cabível quando o dano verificado afeta os *dados pessoais sensíveis*, não abarcando as violações aos dados pessoais classificados como comuns ou *não-sensíveis* pela LGPD. Busca-se com esta pesquisa analisar em que medida o tratamento indevido de dados pessoais *não-sensíveis* pode gerar danos morais indenizáveis ao titular afetado. Conclui-se que, segundo atual entendimento do STJ, o tratamento irregular de dados pessoais *não-sensíveis* pode configurar dano moral presumido, visto seu reconhecido potencial de atingir a esfera íntima dos direitos de personalidade do titular.

Palavras-chave: LGPD; proteção de dados pessoais; dano moral; responsabilidade civil; dados pessoais comuns.

ABSTRACT: The protection of personal data was included in the list of guarantees and fundamental rights protected by the Federal Constitution of 1988, since personal data became part of citizens' personality rights. Since 2020, when the General Personal Data Protection Law (Law No. 13,709/18) came into force, violations of the obligations imposed by the recent regulatory framework have become the subject of legal disputes in civil liability actions, seeking to discuss the possibility of compensation for moral damage in the event of irregular processing of personal data. In this regard, the STJ has established the understanding that moral damage is only applicable when the damage affects sensitive personal data, and does not cover violations of personal data classified as common or non-

sensitive by the LGPD. The aim of this research is to analyze the extent to which the irregular processing of non-sensitive personal data can result in moral damage that can be compensated to the affected data subject. It concludes that, according to the STJ's current understanding, the irregular processing of non-sensitive personal data constitutes presumed moral damage, given its recognized potential to affect the intimate sphere of the data subject's personality rights.

Key-words: LGPD; personal data protection; dano moral; responsabilidade civil; dados pessoais comuns.

1. INTRODUÇÃO

Recentes casos emblemáticos de tratamento irregular de dados pessoais, tais como o incidente envolvendo a coleta massiva de dados de 87 milhões de usuários do Facebook pela empresa Cambridge Analytica, sem conhecimento dos titulares dos dados pessoais afetados, colocaram em pauta os potenciais riscos e impactos do tratamento de dados pessoais em ambientes não regulados.

No Brasil, a proteção de dados pessoais acabou sendo elevada à condição de direito fundamental autônomo e protegido por legislação específica, a Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/18), tendo em vista que os dados pessoais passaram a ser entendidos como parte constitutiva dos direitos de personalidade do titular.

Visando a regulamentação da temática, o marco normativo prevê duas categorias distintas de dados pessoais – os dados pessoais e os dados pessoais sensíveis. De um lado, o inciso I do artigo 5º da Lei classifica os dados pessoais, numa acepção ampla, como toda “informação relacionada a pessoa natural identificada ou identificável” (Brasil, 2018, art. 5º, inc. I). Estes são os dados pessoais que convencionou chamar-se de dados pessoais “comuns ou não-sensíveis”2, definidos de maneira residual.

De outro lado, é legalmente prevista uma segunda categoria de dado

[2] Não há uma nomenclatura específica para esses “tipos” de dados na LGPD, que os define como “dados pessoais”, visto se tratar do conceito amplo de dados pessoais. Visando destaca-los dos dados expressamente categorizados como sensíveis, a jurisprudência convencionou chamar esta categoria de dados pessoais “não-sensíveis” ou “comuns”. Adicionalmente, a ANPD, na Resolução CD/ANPD nº 15, de 24 de abril de 2024, intitula também esta categoria de “dados pessoais gerais” (ANPD, 2024).

pessoal, os dados pessoais sensíveis, agrupados expressamente no rol do artigo 5º, inciso II, da LGPD (Brasil, 2018, art. 5º, II). Dentre eles, estão as "informações referentes à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados biométricos ou genéticos e informações referentes à saúde ou à vida sexual de um indivíduo" (Brasil, 2018, art. 5º, inc. II).

Tal diferenciação legal concedida aos dados sensíveis teria ocorrido em virtude do caráter personalíssimo dessas informações e, por consequência, do potencial caráter discriminatório que o seu uso indevido pode gerar ao seu titular, visto que o "contexto do tratamento desses dados poderá implicar riscos significativos para o exercício dos direitos e liberdades fundamentais" da pessoa a quem se referem (Doneda, 2019).

Com o objetivo de coibir o tratamento irregular desses dados, um dos princípios regentes da LGPD é o regime legal de responsabilização dos agentes de tratamento, prevista nos artigos 6º, X e 42 da Lei (Brasil, 2018, art.6º, X e art. 42)3. Isso quer dizer que, desde a coleta até o fim do ciclo de vida da informação, as organizações possuem o dever de assegurar o cumprimento das obrigações legais e regulamentares. A não aplicação dessas medidas submete os agentes ao dever de reparar o dano eventualmente ocasionado durante o exercício do tratamento dos dados.

Neste contexto, um dos temas de destaque da tutela jurídica dos dados pessoais é o debate acerca da responsabilidade civil e dos danos morais decorrentes da não observância dos princípios e normas que versam sobre o adequado tratamento de tais informações. A partir de 2020, quando a LGPD entrou em vigor, passou a ocorrer a judicialização das violações aos direitos subjetivos dos titulares de dados pessoais. Pergunta-se: o tratamento irregular de dados gera danos morais indenizáveis em favor do titular afetado? Caso o entendimento seja positivo, qual é o bem jurídico protegido pelo dano moral, os dados pessoais em sentido ampliado, ou apenas os dados pessoais sensíveis?

Em julgamento do Agravo em Recurso Especial nº 2.130.619/SP (Brasil, 2023), de relatoria do Ministro Francisco Falcão, acerca do vazamento de dados pessoais de uma consumidora em face de concessionária de energia elétrica, o Superior Tribunal de Justiça restringe o cabimento de indenização

3 "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, art.42).

por danos morais somente às situações de exposição indevida de dados pessoais sensíveis (Brasil, 2023). A consumidora, no caso em tela, teve os seguintes dados vazados: data de nascimento, números de CPF e RG, gênero, endereço, números de telefones e celular, endereço, carga instalada, consumo estimado, tipo de instalação e leitura.

O argumento que fundamenta a decisão seria que, no caso analisado, a exposição teria atingido "[...]apenas dados de natureza comum, de cunho pessoal, mas não considerados de índole íntima, uma vez que passíveis apenas de identificação da pessoa natural, não sendo, por isso, classificados como sensíveis" (STJ, 2023). Isto porque, no entendimento do magistrado, os dados objeto da lide "[...]são aqueles que se fornece em qualquer cadastro, inclusive nos sites consultados no dia a dia, não sendo, portanto, acobertados por sigilo, e o conhecimento por terceiro em nada violaria o direito de personalidade da recorrida" (STJ, 2023).

Recentemente, no Recurso Especial n. 2.133.261/SP (Brasil, 2024), publicado em 08 de outubro de 2024, sob relatoria da Ministra Nancy Andrighi, é possível entrever uma divergência de entendimentos da Egrégia Corte. Analisando também um caso de tratamento irregular de dados pessoais, a ministra julgou que, mesmo se tratando da disponibilização indevida que atingiu dados pessoais de natureza não-sensível, verificou-se o dano moral presumido em virtude da forte "sensação de insegurança" experimenta pelo titular (Brasil, 2024).

De acordo com a Ministra (STJ, 2024), "a transferência dos dados pessoais a terceiro, sem base legal, originou a pretensão do titular quanto à indenização pelo dano causado e de "[...]fazer cessar a ofensa aos (seus) direitos de personalidade".

Isto posto, o objetivo deste trabalho é examinar, partindo-se da jurisprudência do Superior Tribunal de Justiça produzida entre os anos de 2023 e 2024, em que medida é cabível a reparação civil por danos morais em caso de tratamento indevido de dados pessoais não classificados como sensíveis pela legislação pátria, buscando-se apontamentos para uma efetiva tutela judicial dos direitos do titular.

1 RESPONSABILIDADE CIVIL E A LEI GERAL DE PROTEÇÃO DE DADOS (Lei n. 13.709/18)

A noção de *responsabilidade* está, sem dúvidas, enraizada na vida cotidiana. Ofender a honra de alguém; deixar de realizar manutenção em bens

imóveis e acabar cansando danos aos vizinhos; dar causa a acidentes de trânsito; incorrer em falhas durante a prestação de um serviço, ocasionando prejuízos à parte contratante; inadimplir com obrigações contratuais pactuadas. Todos estes fatos da vida social podem, aos olhos da legislação brasileira, gerar o dever de reparar o dano causado por aquele que praticou a conduta danosa.

Como observam os civilistas Nelson Rosenvald e Felipe Braga Netto (Rosenvald; Braga Netto 2024, p. 46,), a sociedade atual, pós-revolução industrial, é uma *sociedade de riscos*, cabendo assim ao Direito, através do instituto da responsabilidade civil, apresentar uma reação jurídica capaz de proteger os indivíduos de danos e ameaças injustificáveis.

Com efeito, a teoria mais recente da responsabilidade civil ganha um caráter preventivo, antecipatório dos riscos, danos e ameaças à esfera jurídica da pessoa. Passa-se assim de uma interpretação clássica pautada no ressarcimento de danos e nas sanções, a posteriori do evento danoso, para uma moderna teoria da responsabilidade civil, baseada na prevenção do dano, antecipatória de resultados.

É justamente no contexto desta moderna teoria geral da responsabilidade civil, pautada na dignidade da pessoa humana, solidariedade, reparação integral e prevenção (Rosenvald, p. 48), que tomaria forma o design normativo da Lei Geral de Proteção de Dados Pessoais.

1.1 RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS: A RESPONSABILIDADE CIVIL NA LGPD

Considerando os perigos que essa sociedade de riscos representa para a efetiva tutela dos direitos dos titulares de dados pessoais, a LGPD dedica uma seção ao tema da responsabilidade civil e ressarcimento de danos eventualmente decorrentes das atividades de tratamento de dados pessoais.

Um dos princípios fundamentais da Lei Geral de Proteção de Dados (LGPD) é o regime jurídico de responsabilização dos agentes de tratamento. Isso significa que, desde a coleta até a eliminação dos dados pessoais, as organizações possuem o dever de garantir o cumprimento das obrigações legais e regulatórias. O descumprimento dessas exigências pode ensejar a responsabilização dos agentes, os quais deverão reparar os danos que vierem a ser causados no curso do tratamento dos dados, inclusive aqueles de natureza moral. Tal diretriz se encontra nos artigos 6º, inciso X, e 42 da referida norma, abaixo destacadas:

> Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/18)
> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> (...) X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.
> (...) 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).

Inserida no contexto de uma responsabilidade civil preocupada com o risco intrínseco de determinadas atividades, a LGPD busca delimitar o escopo do comportamento antijurídico que objetiva combater, ou seja, o tratamento irregular de dados pessoais.

2.1.1 Tratamento irregular de dados pessoais

O tratamento irregular, de acordo com a Lei, é aquele em que os agentes de tratamento deixam de cumprir com o seu dever de cuidado no sentido de (i) observar as normas gerais de proteção de dados pessoais ou (ii) fornecer as medidas de segurança aptas a assegurar a proteção o dado pessoal, considerando as expectativas do titular:

> LGPD
> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
> I - o modo pelo qual é realizado;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado (Brasil, 2018).

A opção por este design legislativo encontra sua origem no Código de

Defesa do Consumidor Lei n. 8.078/90, que considera um produto ou serviço defeituoso quando houver falha na segurança que o consumidor pode esperar:

> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.
> § 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:
> I - o modo de seu fornecimento;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - a época em que foi fornecido. (Brasil, 1990).

Deste modo, entende-se que a responsabilidade do agente de tratamento decorre tanto da (i) violação da legislação de proteção de dados, quanto da (ii) violação da segurança dos dados pessoais, em virtude da ausência de adoção de medidas de proteção de dados esperadas pelo titular (art. 44, LGPD, 2018).

Acerca do primeiro critério, a legislação não se ateve à definição de requisitos objetivos que configuram o "não atendimento à legislação de proteção de dados", aproximando mais o conceito de tratamento irregular das violações de segurança. Entretanto, pode-se afirmar, de modo geral, que o tratamento será irregular quando o agente de tratamento descumprir as regras e princípios dispostos na LGPD, tais como o dever de transparência sobre o modo como realiza a atividade de tratamento, o enquadramento do tratamento na base legal adequada, ou até mesmo a falta de nomeação do Encarregado de Dados Pessoais, obrigações contidas nos artigos 7º, 11º, no inciso VI do artigo 6º e artigo 41 da LGPD (Brasil, 2018), respectivamente.

No que tange ao segundo critério do art. 44, "quando não fornecer a segurança que o titular dele pode esperar" (Brasil, 2018), a irregularidade do tratamento dos dados se configura pela não adoção das medidas de segurança que razoavelmente se poderia esperar que fossem adotadas pelo Controlador e Operador das informações pessoais, no decorrer de determinada atividade de processamento dos dados.

Neste escopo, a noção de "legítima expectativa do titular acerca das

medidas de segurança adotadas" (Brasil, 2018) é um dos elementos centrais do regime de responsabilidade civil da LGPD, levando-se também em consideração "o modo pelo qual o tratamento é realizado, o resultado e os riscos que dele se esperam e a técnicas de tratamento de dados pessoais disponíveis à época" (incisos I, II e III, art. 43, LGPD, 2018), circunstâncias previstas pelo legislador a fim de aferir o nível de segurança que o titular dos dados pode pressupor serem aplicadas.

Com efeito, o titular, ao compartilhar seus dados com os agentes de tratamento, para cumprimento de uma finalidade específica, legitimamente parte do pressuposto de que serão adotadas, de maneira preventiva, medidas de segurança, técnicas e administrativas capazes de proteger os seus dados pessoais de possíveis eventos que venham a comprometer o sigilo, a confidencialidade e a privacidade das informações.

O não fornecimento da segurança de dados que o titular espera serem implementadas, é violação de requisito fundamental da lei, e pode obrigar o agente de tratamento a responder pelos danos decorrentes, em caso de comprometimento da privacidade das informações:

> LGPD
> Art. 44 (...)
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano. (Brasil, 2018).

Neste sentido, a lei busca destacar a "violação da segurança dos dados", definindo-a como fato gerador da obrigação de indenizar, caso o tratamento indevido dos dados pessoais resulte em prejuízos ao titular.4

A esse respeito, as "violações de segurança dos dados" estão previstas no artigo 46 da Lei Geral de Proteção de Dados Pessoais. São descritas pelo legislador como (a) acessos não autorizados, (b) situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou (c) qualquer forma de tratamento inadequado ou ilícito (art. 46, LGPD), com o potencial de gerar risco para o exercício de direitos e liberdades do titular de dados pessoais. Cada um

4 As violações de segurança estão descritas no artigo 46 da LGPD: "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (Brasil, 2018).

desses efeitos adversos relacionados às violações de segurança dos dados pessoais, considerados de maneira isolada, configura um incidente de segurança.

O vazamento de dados pessoais, por exemplo, é um dos incidentes de segurança mais conhecidos e recorrentes, segundo a ANPD, e “ocorre quando dados são indevidamente acessados, coletados e divulgados ou repassados a terceiros”5. Como consequência, o titular pode ser exposto a diversos tipos de danos tais quais fraudes bancárias, tentativas de golpes financeiros, roubo de identidade, falsidade ideológica, venda dos dados, compartilhamento dos dados sem autorização, riscos reputacionais, violações ao direito de imagem, entre outros.

Com o fim de evitar a ocorrência de incidentes, a lei impõe ao Controlador e ao Operador dos dados o dever positivo de mitigar os riscos do tratamento, no Capítulo VII – Da Segurança e Boas Práticas. Adotar medidas de compliance de dados, implementar regras de governança e segurança da informação, além de mecanismos internos de prevenção das formas de tratamento irregular de dados pessoais é uma obrigação legal voltada para a prevenção da ocorrência de danos.

Essa série de condutas exigidas das organizações decorre do fato de que “o critério determinante para imputação da responsabilidade é a irregularidade do tratamento” (Bioni; Dias, 2021, p.413). Neste aspecto, o sistema regulatório de proteção de dados pessoais parte de uma abordagem de responsabilidade civil que objetiva induzir comportamentos meritórios e reduzir as potenciais consequências lesivas do tratamento de dados pessoais.

2 A TUTELA JURISDICIONAL DE DADOS PESSOAIS NÃO-SENSÍVEIS NO SUPERIOR TRIBUNAL DE JUSTIÇA (2023-2024)

Tão logo a LGPD entrou em vigor, em setembro de 2020, casos envolvendo a licitude do tratamento de dados pessoais vem sendo um tema enfrentado de forma crescente pelo Poder Judiciário. Neste cenário, discussões em torno da responsabilidade civil e da possibilidade de configuração dos danos morais decorrentes de incidentes de segurança com dados pessoais ocupam o primeiro plano das ações judicializadas, reiterando

5 ANPD. Incidentes de segurança com dados pessoais (ANPD, 2022).

a importância do assunto para a jurisprudência brasileira.

Não por acaso, a pesquisa Painel LGPD nos Tribunais, de iniciativa do saudoso Danilo Doneda, apontou a Seção III – Da Responsabilidade e do Ressarcimento de Danos – como um dos capítulos da LGPD mais mencionados nas decisões judiciais analisadas entre os anos de 2021 a 2023 (Mendes; Fujimoto, 2024, p.89).

A esse respeito, como fica evidente pela análise da jurisprudência recente, parece haver uma relação intrínseca entre o Art. 5º, II e do Art. 42, caput, ambos da LGPD. Quando considerados em conjunto, estes dispositivos revelam a crescente preocupação das decisões judiciais em relacionar diretamente a (a) classificação dos dados pessoais como dados sensíveis com a (b) possibilidade de caracterização do dano moral indenizável, em especial o dano moral presumido (LGPD, 2024, p. 17).

Nesta pesquisa, busca-se percorrer o caminho inverso. Partindo da análise qualitativa de dois acórdãos do STJ, emblemáticos na seara da tutela jurisdicional de casos envolvendo a LGPD, pretende-se analisar a relação entre, de um lado, (i) a classificação dos dados pessoais como dados comuns ou não-sensíveis e, de outro, (ii) a configuração do dano moral presumido.

Os referidos acórdãos são: (a) a decisão proferida pelo Superior Tribunal de Justiça (STJ) no Agravo em Recurso Especial nº 2.130.619/SP, de relatoria do Ministro Francisco Falcão, relativa a caso de grande impacto na esfera jurídica, se tornando um precedente das demandas de responsabilidade civil decorrentes de incidentes de segurança com dados pessoais; e (b) o acórdão proferido em sede de Recurso Especial nº 2.133.261/SP, de relatoria da Ministra Nancy Andrighi, que empreendeu uma verdadeira mudança de paradigmas quando o assunto é a o tratamento irregular que atinge dados pessoais não-sensíveis.

2.1 A IMPOSSIBILIDADE DE CONFIGURAÇÃO DO DANO MORAL NO INCIDENTE DE VAZAMENTO DE DADOS PESSOAIS: ANÁLISE DO ARESP 2.130.619/SP, DE RELATORIA DO MINISTRO FRANCISCO FALCÃO (SEGUNDA TURMA DO STJ)

Caso de grande repercussão num primeiro momento da tutela judicial da temática foi o vazamento de dados pessoais da então conhecida Eletropaulo Metropolitana Eletricidade de São Paulo S/A, atualmente ENEL, apreciado pelo STJ no Agravo em Recurso Especial 2.130.619/SP, de relatoria do Ministro

Francisco Falcão.

A controvérsia em questão teve sua origem em ação indenizatória ajuizada por uma consumidora em face da concessionária, pleiteando indenização por danos morais, em razão do vazamento e acesso indevido de seus dados pessoais e contratuais por terceiros alheios à relação jurídica entre as partes.

Os dados pessoais afetados no incidente de segurança foram: nome completo, RG, gênero, data de nascimento, idade, telefone fixo, telefone celular e endereço, além de dados relativos ao contrato de fornecimento de energia elétrica celebrado com a ré, como carga instalada, consumo estimado, tipo de instalação e leitura de consumo. Durante o processo, comprovou-se que tais dados foram acessados e compartilhados com terceiros não autorizados, expondo a demandante a potencial risco de fraude e importunação.

A sentença de primeiro grau julgou improcedente o pedido, por entender inexistente a comprovação do dano moral alegadamente suportado pela demandante. No entanto, o Tribunal de Justiça do Estado de São Paulo reformou a decisão de primeiro grau, concedendo provimento à apelação interposta pela autora, por entender que o vazamento de dados caracterizou falha na prestação de serviços, uma vez que a concessionária possuiria o dever de garantir a privacidade dos dados afetados. Inconformada, a parte demandada interpôs recurso especial ao STJ.

O acórdão ficou conhecido no mundo jurídico por abordar questões relevantes sobre a aplicação da LGPD, especificamente no que se refere à distinção entre dados pessoais comuns e sensíveis, associando esta diferenciação à definição da necessidade de comprovação do dano moral para fins de indenização.

4.1.1 Distinção entre dados pessoais comuns e sensíveis no aresp 2.130.619/SP

Concedendo ao apelo da concessionária, o STJ destacou que os dados pessoais afetados no vazamento objeto da lide não se enquadrariam como dados pessoais sensíveis, nos moldes do conceito previsto no art. 5º, II, da LGPD, enumerados como as informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos (LGPD, 2018).

Partindo deste princípio, o Tribunal delimitou dois regimes jurídicos diferenciados para fins de enquadramento da responsabilidade civil: um regime

relativo aos dados pessoais sensíveis e outro aplicado aos dados pessoais não-sensíveis. Verifica-se assim que é determinante para a formação da ratio decidendi a categorização dualista dos dados pessoais.

Primeiramente em seu voto, o Ministro relator observou que os dados vazados no caso em análise - como nome, endereço, RG, CPF, telefone e dados de consumo de energia – não poderiam ser classificados como sensíveis, por se tratarem de dados de cunho pessoal, porém não afetos à índole íntima do indivíduo, servindo somente como meio de identificação da pessoa natural (STJ, 2023):

> O art. 5º, II, da LGPD, dispõe de forma expressa quais dados podem ser considerados sensíveis e, devido a essa condição, exigir tratamento diferenciado, previsto em artigos específicos. Os **dados de natureza comum, pessoais mas não íntimos, passíveis apenas de identificação da pessoa natural não podem ser classificados como sensíveis** (STJ, 2023, grifo nosso).

Com efeito, haveria um contraste jurídico entre os dados de "índole íntima", que seriam os dados classificados taxativamente como sensíveis pela LGPD e os dados comuns, meros identificadores da pessoa natural.

Segundo este entendimento, por consequência, o vazamento de dados pessoais não-sensíveis não teria o condão de causar dano à esfera íntima do titular ao qual os dados se referem, uma vez que os dados afetados na situação em questão se resumiriam a informações pessoais facilmente acessíveis, reveladas corriqueiramente pelo titular em qualquer site. Dessa forma, para o Tribunal, não seria necessário proteger a confidencialidade desse tipo de informação:

> Desse modo, conforme consignado na sentença reformada, revela-se que os dados objeto da lide são aqueles que se fornece em qualquer cadastro, inclusive nos sites consultados no dia a dia, não sendo, portanto, acobertados por sigilo, e o conhecimento por terceiro em nada violaria o direito de personalidade da recorrida.
> Na mesma esteira, merece êxito o apelo especial no ponto em que defende não ser possível indenizar por dano moral o vazamento de dados informados corriqueiramente em diversas situações do dia-a-dia (STJ, 2023).

Desta análise, pode-se agrupar os fundamentos da decisão do Tribunal em três premissas principais:

a) Os dados pessoais não-sensíveis seriam dados meramente identificadores, desvinculados da “índole íntima” do titular;
b) O direito ao sigilo dos dados, disposto na LGPD, não se aplicaria aos dados pessoais não-sensíveis;
c) O tratamento irregular dos dados pessoais não-sensíveis não causaria dano aos direitos de personalidade dos titulares. Aqui se fala na própria inexistência de dano moral.

Disso pode-se chegar a algumas hipóteses. Em primeiro lugar, a tese de que (a) os dados pessoais não-sensíveis seriam dados meramente identificadores, desatrelados à esfera íntima da pessoa, deve ser enfrentada com ressalvas. Acerca disso, cumpre mencionar que o art. 17 da LGPD dispõe que “toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei” (Brasil, 2018). Isso quer dizer que, para além da capacidade de identificar uma pessoa natural, o dado pessoal é uma representação direta desse indivíduo.

Note-se o exemplo do CPF. A cada pessoa, desde o seu nascimento, é atribuído um número de CPF. Este número é um identificador único, não podendo existir a situação hipotética em que duas pessoas são identificadas pela mesma sequência numérica. Esta informação passa a manter, portanto, um vínculo indissociável com seu titular, revelando aspectos dessa pessoa. Utilizando um número de CPF, para além de garantir a identificação de um indivíduo, é possível ter acesso a uma série de informações privadas de seu titular, como dados de padrão e preferências de consumo, dados financeiros e até a filiação.

Neste sentido, como observa Danilo Doneda, as informações vinculadas a uma pessoa são representações diretas de sua personalidade:

> a informação mantém um vínculo indissolúvel com a pessoa, e sua valoração específica deve partir basicamente dela ser uma representação direta da pessoa. Por força do regime privilegiado de vinculação entre a informação pessoal e a pessoa à qual ela se refere como representação direta de sua personalidade – , tal informação deve ser entendida, portanto, como uma extensão da sua personalidade (Doneda, 2019, p. 145).

Destaque-se que, neste ponto, Doneda (2019) está se referindo a dados

pessoais, de modo geral e indistinto, de maneira que esta característica não se restringiria apenas aos dados sensíveis.

A segunda tese, segundo a qual (b) os dados pessoais não-sensíveis, por serem considerados "que se fornece em qualquer cadastro", não se submeteriam à regra do sigilo de dados, logo não estariam protegidos pelo regime jurídico da LGPD. À princípio, importa salientar que, nos moldes do art. 3º, a lei de proteção de dados pessoais se aplica a qualquer operação de tratamento de dados pessoais, independentemente de serem objetos do tratamento dados sensíveis ou não-sensíveis, ressalvadas as hipóteses de exclusão de aplicabilidade expressas pela própria lei, no artigo 4º.

De igual modo, ao dispor que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (Art. 5º, LXXIX, CRFB/88) a Constituição Federal não limita um tipo de dado pessoal que merece tutela, em detrimento de outro, mas veicula um conceito amplo de dados pessoais, entendidos como qualquer informação capaz de identificar uma pessoa, direta ou indiretamente.

Consequentemente, a ideia de que os dados pessoais comuns não seriam protegidos pelo sigilo é premissa contrária ao regime legal disposto na LGPD6, que prevê o sigilo dos dados como a regra geral a ser seguida pelos agentes de tratamento, tanto no contexto de manuseio de dados sensíveis, como de dados não-sensíveis, ressalvadas as hipóteses autorizativas legalmente previstas nos artigos 7º e 11º da lei. Em que pese o artigo 11º defina algumas especificidades para o tratamento dos dados sensíveis, não seria por isso verdadeiro afirmar que os dados pessoais comuns não se submeteriam à regra de sigilo, como inicialmente aventado no acórdão em análise.

Sobre isso, a Seção I da LGPD - Da Segurança e Sigilo dos Dados (Capítulo VII, Da Segurança e Boas Práticas, 2018) – especialmente em seu artigo 46, determina que proteger a confidencialidade dos dados de acessos não autorizados e demais formas de tratamento irregular é norma mandamental da legislação de dados pessoais, se aplicando impreterivelmente a qualquer categoria de informação pessoal, visto que a lei se aplica a "qualquer operação de tratamento" de dados pessoais (art. 3º, LGPD, 2018). Por consequência lógica, a quebra indevida do sigilo dos dados pessoais não-

6 Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados (Brasil, 2018).

sensíveis é fato que viola os princípios dispostos no art. 2º, especialmente o respeito à privacidade e à intimidade da pessoa natural (art. 2º, incisos I e IV da LGPD, 2018) respectivamente:

> LGPD
> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018, grifo nosso).

Nesse ponto é importante retomar a ideia de proteção da privacidade, que envolve também, neste contexto, o direito à privacidade de dados, a partir da qual um sujeito exerce o direito de tomar decisões sobre como seus dados são tratados. Este conceito se pauta no que Rodotá chama de eixo “pessoa-informação-circulação-controle” (Rodotá, 1995 apud Doneda, 2020, p. 39). Daí a concepção amplamente consolidada na teoria da proteção de dados pessoais, segundo a qual o titular dos dados deve ter o controle sobre a circulação das suas informações.

No caso em tela, o compartilhamento dos dados com pessoais alheias à relação jurídica, impede a titular de exercer seu direito à privacidade dos dados, visto que ela passa a não conseguir acessar o rastro da informação, que poderia estar transitando em um número infinito e desconhecido de ambientes.

O direito do titular de decidir sobre quais dados são íntimos e sensíveis para si, além de exigir que as informações sejam tratadas de forma legítima, também faz parte desse conceito. Neste sentido, pode-se dizer que a proteção do sigilo dos dados pessoais, seja qual for a sua categoria, está intimamente ligada à proteção da privacidade e intimidade7.

---

7 Revelante mencionar que para Danilo Doneda, contemporaneamente a proteção da privacidade passa a ocorrer a partir da proteção dos dados pessoais. Ademais, para o autor, “a proteção da privacidade identifica-se e acompanha a consolidação da própria teoria dos direitos da personalidade e, em seus mais recentes desenvolvimentos, afasta a leitura segundo a qual sua utilização em nome de um individualismo exacerbado alimentou o medo de que eles se tornassem o “direito dos egoísmos privados”. Algo paradoxalmente, a proteção da privacidade na sociedade da informação, a partir da proteção de dados

Em terceiro lugar, os fundamentos da decisão da Segunda Turma indicam que (c) o tratamento irregular de dados pessoais não-sensíveis não possuiria o potencial de causar dano moral à esfera jurídica do titular dos dados, uma vez que o vazamento dos dados não constituiria lesão a direitos de personalidade.

A esse respeito, é relevante buscar entender os limites jurídicos desta premissa. Importante analisar, primeiramente, que aqui se nega não somente a possibilidade de ocorrência do dano moral presumido, mas a própria existência do dano. Em regra, conforme preleciona grande parte da doutrina e jurisprudência, a responsabilidade civil surge “mediante a existência do dano” (Stolze; Pamplona Filho, 2023, p. 40).

Dano, como dito em capítulo anterior, é o prejuízo injustamente suportado pela vítima em virtude do ato ilícito praticado pelo ofensor. Aqui o elemento fundador do dano é o ato ilícito e não o bem jurídico tutelado. É evidente que em algumas situações, a depender do valor social do bem jurídico, a lei prevê diferenças de valoração do dano. No direito Penal, por exemplo, o dano ao patrimônio material tem valor diferente de um dano à vida, por exemplo. Entretanto, em nenhuma das situações, estando presente o ato ilícito, nega-se a existência do dano.

No caso em análise há demonstrado ato ilícito perpetrado pela concessionária de energia, que violou o dever de adotar as medidas de segurança esperadas pelo titular, como previsto pela LGPD no artigo 46. Com a consequente exposição indevida dos dados pessoais, consolida-se o dano.

Acerca disso, o Parágrafo único do artigo 44 é inequívoco quando dispõe que responderá pelos danos decorrentes da violação da segurança dos dados “o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano” (Brasil, 2018).

Quanto ao potencial do tratamento irregular de causar lesão aos direitos de personalidade, neste aspecto é oportuno retomar a tese de Pierre Catala, que assevera neste contexto: “quando o objeto dos dados é um sujeito de direitos, a informação é um atributo de sua personalidade” (Catala, 1983 apud Doneda, 2020, p.142).

O CPF, exemplo utilizado acima, não é classificado pela LGPD como dado pessoal sensível. Sob esta ótica, a sua exposição irregular não poderia

---

pessoais, avança sobre terrenos outrora improponíveis e nos induz a pensá-la como um elemento que, mais do que garantir o isolamento ou a tranquilidade, serve a proporcionar ao indivíduo os meios necessários à construção e consolidação de uma esfera privada própria,” (Doneda, 2020, p. 39).

permitir o acesso a outras informações pessoais, inclusive àquelas consideradas sensíveis? Em que pese sua característica de “mero identificador”, a partir do CPF é possível ter acesso a uma vasta gama de dados pessoais referentes a determinada pessoa, tanto em bancos de dados públicos, como privados.

O mesmo poderia se questionar com relação à imagem. Esta informação, isoladamente considerada, não é um dado sensível à luz do artigo 5º da Lei. Seria possível então afirmar que o compartilhamento indevido de uma foto não poderia gerar constrangimento ou lesões à honra de seu titular? O potencial lesivo de uma foto, apesar de não ser um dado sensível, é incansavelmente tratado pela jurisprudência pátria como fato ensejador de dano moral. Além do que, a imagem é ainda um direito de personalidade expressamente previsto na sistemática do Código Civil de 2002.

O formalismo jurídico que engessa os conceitos de dados pessoais sensíveis, de um lado, e não sensíveis de outro, não deve servir como um meio de obstar o acesso do titular aos direitos, principalmente ao direito à reparação de danos previsto pela sistemática da proteção de dados pessoais.

Nesta perspectiva, a criação de dois regimes de responsabilidade civil diferenciados em relação à categoria dos dados pessoais se apresenta como uma estratégia jurídica de difícil aplicação, quando se realiza uma interpretação sistemática da proteção de dados pessoais.

4.1.2 O dano moral presumido: a necessidade de comprovação do dano no aresp 2.130.619/SP

Há um tipo de dano moral convencionado pela doutrina e jurisprudência como dano moral presumido. Conforme orientam Stolze (2023) e Pamplona Filho (2023), como regra, a responsabilidade civil nasce com a existência do dano, considerando-se a extensão do prejuízo suportado pela vítima como a base de cálculo do valor indenizatório devido. Todavia, convencionou-se a possibilidade de configuração do dano moral presumido em alguns casos, que é a situação em que se exclui a necessidade de comprovação do dano suportado (Stolze; Pamplona Filho, 2023, p. 40).8

8 De acordo com Stolze e Pamplona Filho: “A jurisprudência tem sido pródiga em reconhecer situações em que o dano se comprova in re ipsa. A título meramente exemplificativo, vale lembrar hipóteses como a inscrição indevida em cadastro de inadimplentes, atraso de voo, equívocos administrativos e emissão de diplomas sem reconhecimento. caso do dano in re ipsa, não é necessária a apresentação de provas que demonstrem a ofensa moral da pessoa. O próprio fato já configura o dano. Uma das hipóteses é o dano

Entretanto, no caso em discussão no AREsp 2.130.619/SP, a corte superior entendeu que o vazamento de dados pessoais não-sensíveis, isoladamente, não ensejaria a configuração de dano moral presumido:

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

Para a configuração do dano moral, conforme o entendimento da terceira turma, seria imprescindível a demonstração do efetivo abalo à esfera íntima do titular dos dados pessoais. Caso contrário, se trataria somente de "inconveniente exposição de dados pessoais comuns desacompanhados de comprovação do dano" (STJ, 2023). Nesta ótica, portanto, a presunção de dano moral só seria cabível em casos que envolvam dados pessoais sensíveis, em razão do seu potencial lesivo.

A decisão do STJ no AREsp 2.130.619/SP representou à época importante precedente na interpretação da LGPD, ao delimitar os contornos entre dados comuns e sensíveis e afastar a possibilidade de indenização automática por dano moral em situações de mero vazamento de dados comuns. Firmou-se, desde então, interpretação no sentido de que o titular dos dados teria que comprovar concretamente o prejuízo experimentado, para que então houvesse a responsabilização civil dos agentes de tratamento.

Mais recentemente, verifica-se uma tendência de mudança desse entendimento por parte do Superior Tribunal de Justiça, conforme será apresentado a seguir.

2.2 A CONFIGURAÇÃO DO DANO MORAL POR TRATAMENTO IRREGULAR DE DADOS PESSOAIS NÃO-SENSÍVEIS: ANÁLISE DO RESP Nº 2133261/SP, DE RELATORIA DA MINISTRA NANCY ANDRIGUI

provocado pela inserção de nome de forma indevida em cadastro de inadimplentes". Serviço de Proteção ao Crédito (SPC), Cadastro de Inadimplência (Cadin) e Serasa, por exemplo, são bancos de dados que armazenam informações sobre dívidas vencidas e não pagas, além de registros como protesto de título, ações judiciais e cheques sem fundos. Os cadastros dificultam a concessão do crédito, já que, por não terem realizado o pagamento de dívidas, as pessoas recebem tratamento mais cuidadoso das instituições financeiras. Uma pessoa que tem seu nome sujo, ou seja, inserido nesses cadastros, terá restrições financeiras. Os nomes podem ficar inscritos nos cadastros por um período máximo de cinco anos, desde que a pessoa não deixe de pagar outras dívidas no período. No STJ, é consolidado o entendimento de que 'a própria inclusão ou manutenção equivocada configura o dano moral in re ipsa, ou seja, dano vinculado à própria existência do fato ilícito, cujos resultados são presumidos' (Ag 1.379.761)" (Stolze; Pamplona Filho, 2023, p. 40).

Essa trajetória histórica pode ser segmentada em duas etapas: a que antecede e a que sucede a Convenção de 1949 (Convenção e Protocolo Final para a Repressão do Tráfico de Pessoas e do Lenocínio, Lake Success), o que implica a anulação e a substituição explícita das normas anteriores (Brasil, 2008).

Em contraponto ao acórdão analisado anteriormente, a decisão proferida pela Terceira Turma do Superior Tribunal de Justiça, no julgamento do Recurso Especial nº 2133261/SP (STJ, 2024) tratou da disponibilização indevida de dados pessoais não-sensíveis de consumidora a terceiros consulentes9, por parte de instituição gestora de banco de dados especializada na formação de histórico de crédito (SCPC).

No caso em tela, a titular dos dados pessoais ajuizou ação de obrigação de fazer cumulada com indenização por danos morais, alegando a comercialização e exposição de seus dados cadastrais - como CPF, nome, nome da mãe, situação do CPF, região de origem do CPF, data de nascimento, mais de um endereço residencial, três contatos telefônicos e sexo - e financeiros, sem seu consentimento ou comunicação prévia, tratando-se assim de tratamento irregular de dados pessoais, à luz da LGPD.

A parte autora, em seus pedidos, requereu que a gestora do banco de dados se abstivesse de divulgar, permitir o acesso, gratuito ou pago, ou compartilhar dados acerca de sua renda mensal, endereço e telefones pessoais com empresas interessadas. Pediu ainda a condenação da parte ré ao pagamento de uma indenização pelos danos morais.

A decisão de primeiro grau julgou improcedente o pedido, entendimento mantido pelo Tribunal de Justiça de São Paulo, sob o fundamento de que os dados em questão não seriam dados sensíveis e, portanto, sua divulgação seria lícita. A controvérsia foi, então, submetida à apreciação do STJ.

No acórdão, o vazamento de dados sigilosos das operações bancárias da consumidora foi julgado como fato incontroverso pela Terceira Turma do STJ, assim como a responsabilidade da gestora de banco de dados pela fraude que a consumidora sofreu em virtude do tratamento irregular.

De acordo com o Tribunal (STJ, 2024), o credit scoring (pontuação de crédito) poderia ser utilizado sem consentimento, visto haver previsão legal

9 A Lei do Cadastro Positivo define o terceiro consulente como a “pessoa natural ou jurídica que acesse informações em bancos de dados para qualquer finalidade permitida por esta Lei” (art. 2º, V, Lei nº 12.414, 2011).

autorizando o tratamento dos dados na Lei do Cadastro Positivo (Lei nº 12.414/2011), que regulamenta a consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Neste sentido, o tratamento seria realizado com a finalidade de proteção ao crédito, conforme seu art. 7º, X, da LGPD (Brasil, 2018).

Todavia, a Lei do Cadastro Positivo não autoriza a divulgação indevida de dados pessoais a terceiros, que somente poderiam ter tido acesso ao score de crédito e, mediante autorização, ao histórico de crédito10, e não aos dados cadastrais da consumidora. Isso porque, a própria Lei do Cadastro Positivo restringe as informações que podem ou não ser divulgadas, exigindo adicionalmente a autorização prévia do titular. Dessa forma, o STJ entendeu que não haveria base legal para o tratamento dos dados pessoais, que acabou sendo classificado como ilícito.

Além da disponibilização indevida dos dados, o Tribunal destacou a obrigatoriedade de comunicação e autorização prévia do titular dos dados, conforme o art. 4º, IV da Lei nº 12.414/2011 (STJ, 2024). Essa comunicação é condição essencial para que o consumidor exerça seus direitos à transparência, à autodeterminação informativa, ao cancelamento e à retificação dos dados, assegurados também pela LGPD (art. 18).

> Merece menção, ainda, o princípio da transparência, que garante aos titulares, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (art. 6º, VI). Nesse sentido, "o consumidor tem o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas" (REsp 1.758.799/MG, Terceira Turma, DJe 19/11/2019). Desse modo, todo o microssistema de proteção de dados pessoais, impõe ao agente de tratamento o dever de informar ao titular acerca do tratamento de seus dados pessoais. A eventual não exigência de consentimento não significa que o consumidor não deva ser cientificado de que seus dados estão sendo utilizados e por quem, inclusive para exercer o indispensável controle, nos

10 O histórico de crédito é definido pela Lei nº 12.414/2011: "conjunto de dados financeiros e de pagamentos, relativos às operações de crédito e obrigações de pagamento adimplidas ou em andamento por pessoa natural ou jurídica" (Brasil, 2011).

limites da lei (STJ, 2024, grifo nosso).

Sobre isso, importa destacar que as premissas da decisão não setorizam os dados pessoais que merecem proteção, de um lado, e os dados dos quais se dispensaria a proteção adequada, em virtude do seu nível de sensibilidade. Ao contrário, neste cenário o Tribunal se preocupa em salientar que mesmo que o tratamento irregular afete dados pessoais não-sensíveis, ainda assim estará presente o dever de cuidado previsto na LGPD:

> Em síntese, embora o gestor de banco de dados para proteção do crédito possa realizar o tratamento de dados pessoais e abrir cadastro sem prévio consentimento do cadastrado, a Lei nº 12.414/2011 (I) restringe o compartilhamento das informações cadastrais a outros bancos de dados – que são geridos por pessoas devidamente autorizadas pelo BACEN; e (II) em relação aos consulentes, apenas autoriza a disponibilização (a) da pontuação de crédito; e (b) do histórico de crédito, desde que autorizado previamente pelo cadastrado, em observância ao modelo de autorização do Decreto nº 9.936/2019. Desse modo, se um terceiro consulente tem interesse em obter as informações cadastrais do cadastrado, ainda que sejam dados pessoais não sensíveis, deve ele obter o prévio e expresso consentimento do titular, com base na autonomia da vontade, pois não há autorização legal para que o gestor de banco de dados disponibilize tais dados (STJ, 2024, grifo nosso).

Juntamente aos princípios e direitos mencionados, a Terceira turma menciona o princípio da finalidade, de acordo com o qual o tratamento dos dados pessoais deve ser realizado para propósitos “legítimos, específicos, explícitos e informados ao titular” (art. 6º, I, LGPD, 2018), da mesma forma que se deve observar o dever de transparência acerca da realização do tratamento.

Desse modo, conforme o art. 16 da Lei nº 12.414/2011 e os arts. 42 e 43 da LGPD, a Terceira Turma determinou que os agentes de tratamento envolvidos responderiam objetivamente responsabilidade pelos danos morais causados à autora, salvo sob comprovação de excludente de ilicitude, o que não ocorreu na hipótese dos autos. (STJ, 2024)

Com base em tais fundamentos, a disponibilização indevida dos dados pessoais não-sensíveis pela gestora de banco de dados caracterizou o dano moral in re ipsa em favor da titular dos dados.

4.2.1. A desnecessidade de comprovação do dano moral no REsp nº 2133261/SP

O voto destacou que a disponibilização indevida de dados pessoais a terceiros, ainda em se tratando de dados pessoais não-sensíveis, configura dano moral in re ipsa, tendo em vista a sensação de insegurança e vulnerabilidade geradas ao titular ao ser exposto a potenciais situações de fraude, importunações e demais atos ilícitos de terceiros:

> A disponibilização indevida de dados pessoais pelos bancos de dados para terceiros caracteriza dano moral presumido (in re ipsa) ao cadastrado titular dos dados, diante, sobretudo, da forte sensação de insegurança por ele experimentada. O gestor de banco de dados que disponibiliza para terceiros consulentes o acesso aos dados do cadastrado que somente poderiam ser compartilhados entre bancos de dados – como as informações cadastrais – deve responder objetivamente pelos danos morais causados ao cadastrado, em observância aos arts. 16 da Lei nº 12.414/2011 e 42 e 43, II, da LGPD (STJ, 2024, grifo nosso).

A esse respeito, entendeu-se que a citada "sensação de insegurança" não deve ser vista como "mero dissabor", uma vez que se considera a "irreparabilidade" do dano moral suportado. Isso porque não seria mais possível restabelecer o status quo anterior à violação dos dados pessoais, sendo "quase impossível que o titular tenha o real controle sobre o tratamento de seus dados após serem disponibilizados de forma indevida a terceiros" (STJ, 2024). Este fato prejudica, por consequência, o exercício de direitos do titular relativo aos dados pessoais.

Assim, o STJ reforçou o entendimento de que o dano moral é presumido em virtude da exposição indevida de dados pessoais não-sensíveis, o que representaria o potencial para causar lesões aos direitos de personalidade do titular:

> A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do titular – dentre os quais se inclui o dever de informar – faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade (STJ, 2024).

Para o Tribunal, o tratamento de dados pessoais pelas entidades de proteção ao crédito, por sua natureza específica, é uma atividade que apresenta riscos aos direitos da personalidade do consumidor. Nesta ótica, as entidades possuem o dever legal de agir em conformidade com a legislação de proteção de dados, caso contrário podem gerar violações aos direitos de personalidade, como a privacidade, e se verem obrigadas, por consequência, ao dever de indenizar:

> STJ – AREsp nº 2.133.261/SP, Ministro relator: Nancy Andrighi, 3ª Turma, Data de julgamento: 08/10/2024:
> [...] conforme aponta a doutrina, "o tratamento de informações – positivas ou negativas – pelas entidades de proteção ao crédito é atividade potencialmente ofensiva a direitos da personalidade do consumidor (privacidade e honra). Embora relevantes para o mercado e para o consumidor, as entidades [...] devem observar rigorosamente os limites e requisitos estabelecidos pela lei, sob pena de ofensa a direitos da personalidade e, consequentemente, surgimento do dever de indenizar os danos morais e materiais causados aos consumidores (BESSA, 2014, p. 53).
> Nesse sentido, como já reconhecido por esta Turma, a disponibilização indevida (em ofensa aos limites legais) de dados pessoais pelos bancos de dados para terceiros caracteriza dano moral presumido (in re ipsa)" (STJ, 2024).

A própria expressão comumente veiculada acerca do indivíduo que está com o "nome sujo na praça" revela o potencial discriminatório e inequivocamente lesivo da exposição indevida dessas informações. Tal entendimento se consolida na esteira de entendimento consolidado anteriormente pelo STJ (Ag 1.379.761, 2011) acerca do dano moral in re ipsa devido em casos de inclusão ou manutenção indevida de pessoas nestes cadastros, entendendo-se que esta prática ilícita pode gerar restrições ao pleno exercício de direitos pelo titular, como a restrições de crédito. Aqui o dano se configura com a "própria existência do fato ilícito, cujos resultados são presumidos" (Stolze; Pamplona filho, 2023, p. 40).

É digno de menção, neste ponto, que de igual maneira se posiciona o STJ em outro julgado recente envolvendo o tratamento de dados pessoais não-sensíveis e a possibilidade de configuração do dano moral presumido, o REsp nº 2147374 - SP (2022/0220922-8), de relatoria do Ministro Ricardo Villas Bôas Cueva. No referido julgamento, o debate acerca do dano moral indenizável,

passa a se relacionar com a ideia de responsabilidade civil proativa do agente de tratamento (STJ, 2024):

> [a] nova lei, porém, introduz, secundando o regulamento europeu, uma mudança profunda em termos de responsabilização. Trata-se da sua união ao conceito de 'prestação de contas'. Esse novo sistema de responsabilidade, que vem sendo chamado de 'responsabilidade ativa' ou 'responsabilidade proativa' encontra-se indicada no inciso X do art. 6º, que determina que às empresas que não é suficiente cumprir os artigos da lei; será necessário também 'demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas. Portanto, 'não descumprir a lei, não é mais suficiente. Exige-se, em síntese, atitudes conscientes, diligentes e proativas por parte das empresas em relação à utilização dos dados pessoais. Assim, a partir de agosto de 2020, quando entra em vigor a LGPD, qualquer empresa que processe dados pessoais, terá não apenas que cumprir a lei, mas também terá que provar que está em conformidade com a Lei. Caberá às empresas, em vez de à Administração Pública, a responsabilidade de identificar os próprios riscos e escolher e aplicar as medidas apropriadas para mitigá-los. (Maria Celina Bodin de Moraes e João Quinelato de Queiroz, "Autodeterminação informativa e responsabilização proativa", Cadernos Adenauer XX (2019) nº 3, p. 113). [...] (STJ – SP, 2024).

A ideia de compliance de dados11 assume extrema importância nesse novo sistema de responsabilidade civil, sendo imprescindível que sejam adotadas eficazes medidas de governança e mitigação de riscos. Assim, a frustração da expectativa legítima de proteção dos dados pessoais, quanto à obrigação legal dos Controladores e Operadores em adotar as medidas de segurança esperadas pelo titular, faz nascer o dever de indenizar o titular pelos danos morais suportados.

Espera-se, portanto, uma atitude preventiva dos agentes de tratamento, o que é reforçado tanto pela técnica legislativa adotada na LGPD, quanto nos posicionamentos da Autoridade Nacional de Proteção de Dados no Âmbito de suas atribuições regulatórias. Além de observar a lei, todo aquele que em suas atividades produtivas trate dados pessoais possui o dever de demonstrar uma conduta de boa-fé e comprometida em assegurar a conformidade com os

11 O ministro relator define compliance de dados como o “esforço de conformidade” e de aplicação da LGPD nas atividades das empresas que lidam com o tratamento de dados pessoais.(STJ, 2024).

mandamentos do sistema regulatório.

O “esforço de conformidade” deve estar, assim, presente nos processos das organizações. A falta de atendimento aos requisitos de segurança e compliance de dados é responsável pela “corrosão” da privacidade. Por isso não é suficiente a opção administrativa por proteger esse ou aquele dado.

Para o ministro relator, esta ideia se relaciona com a adoção de uma nova abordagem no âmbito da teoria da proteção de dados pessoais. Uma abordagem que se aproxima das possibilidades, usos e finalidades do tratamento, ao passo que se afasta gradativamente do conteúdo dos dados pessoais, propriamente dito, ou no fato de “quão sensíveis ou íntimos esses dados são” (STJ, 2024).

Ao não se limitar a uma perspectiva dualista e engessada dos dados pessoais, os julgados do STJ consolidam uma interpretação sistêmica da LGPD, reforçando a necessidade de respeito à autodeterminação informativa, ao dever de segurança, à mitigação de riscos e aos limites legais do tratamento de dados pessoais não-sensíveis, estabelecendo novos parâmetros para as decisões judiciais pertinentes à temática da proteção de dados.

CONCLUSÃO

As recentes decisões judiciais, envolvendo o dano moral em virtude de situações de tratamento irregular de dados pessoais não-sensíveis, revelam uma mudança de paradigmas interpretativos acerca do tema. Inicialmente, o entendimento dominante da jurisprudência do STJ vinculava a responsabilidade civil dos agentes de tratamento diretamente ao tipo de dado pessoal afetado. Isso porque, em tese, o tratamento ilícito de dados pessoais comuns não seria um fato jurídico capaz de lesionar direitos de personalidade, fato gerador por excelência do dano moral. Contudo, esse ponto de vista, que atrela o dano moral diretamente à comprovação do efetivo prejuízo percebido pela vítima, pode acabar gerando um distanciamento entre o arcabouço normativo da proteção de dados pessoais e o acesso efetivo do titular aos seus direitos.

Neste impasse, é oportuno relembrar o princípio da efetividade da tutela jurisdicional, referido no art. 5º, XXXV da Constituição Federal, que prevê: “a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito”(Brasil, 1988). Tal premissa é igualmente reproduzida, em momento posterior, no art. 3º do Código de Processo Civil de 2002, a partir do qual

entende-se que “não se excluirá da apreciação jurisdicional ameaça ou lesão a direito”(Brasil, 2002).

O reforço normativo no que tange aos efeitos da jurisdição é sintoma de um ordenamento jurídico preocupado em assegurar que o Estado, por meio da função jurisdicional, possui o dever de efetivar direitos. Não é suficiente que o indivíduo tenha acesso ao sistema de justiça, mas é preciso ainda que a prestação jurisdicional seja capaz de concretizar o direito material positivado. Portanto, a proteção, prevista na Lei Geral de Proteção de Dados, encontra na tutela judicial um meio de garantir, efetivamente, os direitos do titular, sob o risco de se tornar mera retórica legislativa.

Num segundo momento da apreciação judicial do tema, a Corte Superior colocou em pauta um posicionamento mais alinhado à ideia de responsabilidade civil proativa, assentada no dever jurídico de prevenção do tratamento ilícito e da própria noção de prestação de contas pelos agentes de tratamento, com relação a aplicação das medidas de governança de dados. O dever de adoção de iniciativas de segurança informacional pelos Controladores e Operadores, neste contexto, aparece como um pré-requisito lógico da proteção da privacidade. Com o próprio tratamento irregular, previsto no artigo 44 da LGPD (Brasil, 2018), nasce a responsabilidade civil, não sendo necessária a comprovação do prejuízo pelo titular. É partindo destas premissas que o STJ passa por um redirecionamento de rotas, se afastando do posicionamento adotado num primeiro momento da judicialização do assunto.

Isto posto, pode-se dizer que os julgados analisados apontam um novo caminho para uma tutela jurisdicional efetiva da proteção de dados pessoais. Este novo entendimento destaca, sobretudo, a importância de estender um olhar protetivo às violações de dados pessoais não-sensíveis. No atual cenário, é relevante aludir ao voto da eminente Ministra Carmen Lúcia, na ADI 6387 MC-Ref/DF:

> somos uma sociedade de dados em que [...] realmente não há dados insignificantes. O que pode ser significante ou insignificante é o uso que do dado é feito, que, com a conectividade possível, faz com que todos nós tenhamos de estar atentos a isto que hoje é uma sociedade que depende de dados para passar não apenas informações, mas dados que acabam levando a uma modificação enorme na convivência, quer por seu vazamento, uso indevido, pela malversação desses dados, quer quando (Brasil, 2020).

Em que pese a relevância da opção legislativa em prever categorias apartadas de informações relativas a uma pessoa – os dados pessoais sensíveis e os dados pessoais comuns ou não-sensíveis – a setorização dos dados pessoais "apresenta o risco de enfraquecer a própria tutela da personalidade do indivíduo, considerada unitariamente" (Doneda, 2019, p. 142).

Sob esta perspectiva dualista dos dados, destacam-se, à primeira vista, os dados pessoais sensíveis, aqueles cuja utilização ocasionaria, supostamente, maior potencial lesivo e discriminatório aos indivíduos, em detrimento de outros tipos de informações, menos sensíveis e que, portanto, não exigirão os mesmos padrões de proteção.

Esta premissa, entretanto, poderia conduzir à noção equivocada de que o tratamento de dados pessoais não-sensíveis não apresentaria risco algum aos titulares. Todavia, como observa Danilo Doneda (2019, p. 144), "qualquer dado pessoal pode, em última medida, ser utilizado para o fim de se discriminar". Um dado de localização, por exemplo, poderia indicar o local onde um indivíduo reside, qual a sua situação econômica, sua idade e até informações acerca de sua raça ou etnia.

Nesta perspectiva, os dados pessoas não-sensíveis, a depender da forma de tratamento, também são capazes de expor características consideradas sensíveis sobre seu titular, podendo conduzir, igualmente, a usos lesivos e discriminatórios:

> mesmo dados não qualificados como sensíveis, quando submetidos a um determinado tratamento, podem revelar aspectos considerados sensíveis sobre a personalidade de alguém, podendo levar a práticas discriminatórias. Afirma-se, em síntese, que um dado, em si, não é perigoso ou discriminatório – mas o uso que dele se faz pode sê-lo (Doneda, 2019, p. 144).

A dependência desses contextos setoriais dos dados, pautados no conteúdo das informações, e não nos seus potenciais usos lesivos, produz um esvaziamento da proteção do sujeito titular dos dados pessoais. Configura-se, então, uma verdadeira discrepância entre os meios de tutela, legais e judiciais, e o efetivo exercício do direito fundamental à proteção de dados.

Objetivando atingir uma proteção efetiva do titular dos dados pessoais, é preciso buscar nossos horizontes interpretativos, abandonando-se uma perspectiva conteudista, estática e até patrimonialista dos dados pessoais. É

necessário, portanto, como ensina Danilo Doneda (2019), adotar uma perspectiva pautada na tutela da própria pessoa em si e na afirmação de seus direitos de personalidade.

REFERÊNCIAS

ACADEMIA BRASILEIRA DE LETRAS JURÍDICAS. **Dicionário Jurídico.** (Org) M. Othon Sidou 11. ed., rev. e atual. Rio de Janeiro: Forense, 2016.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Incidentes de segurança com dados pessoais. *In:* SEMANA DA PROTEÇÃO DE DADOS, 2022. *[*S. l.], 2022. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/acoes-e-programas/programas-projetos-acoes-obras-e-atividades/semana-da-protecao-de-dados-2022/incidentes-de-seguranca-com-dados-pessoais. Acesso em: 07 mai. 2025.

BIONI, Bruno. **Proteção de dados**: contexto, narrativas e elementos fundantes. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 mar. 2024.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 27 out. 2023

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Diário Oficial da União, Brasília, 15 ago. 2018.

BRASIL. Superior Tribunal de Justiça (2. Turma). **AREsp nº 2.130.619/SP**. Relator: Francisco Falcão. São Paulo, 07 de março de 2023. Disponível em: https: //www.jusbrasil.com.br/jurisprudência/stj/1780119718.

BRASIL. Superior Tribunal de Justiça (3. Turma). **Resp n° 2133261/SP**. Isalete Helena Silva versus Boa Vista Serviços S.A. Relatora: Nancy Andrighi. São Paulo, 08 de outubro de 2024.

BRASIL. Supremo Tribunal Federal (Plenário). **ADI 6387 MC-Ref/DF**. Medida Cautelar em Ação Direta de Inconstitucionalidade. Medida provisória nº 954/2020. Compartilhamento de dados dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas prestadoras, com o instituto brasileiro de geografia e estatística. Deferimento. Relator: Min. Rosa Weber, 7 de maio de 2020.

BRASIL. Superior Tribunal de Justiça (3. Turma). **REsp nº 2147374 - SP**

(2022/0220922-8). Apelante: Eletropaulo Metropolitana Eletricidade de Sao Paulo S.A. Apelada: Thayna Nayara da Silva Queiroz. Relator: Ricardo Villas Bôas Cueva. São Paulo, 3 de dezembro de 2024.

BRASIL. Superior Tribunal de Justiça. **Ag nº 1.379.761 - SP (2011/0004318-8)** Agravante: Banco Santander Brasil S⁄A. Agravado: Cecilia de Oliveira Crespi e outro(s). Relator: Min. Luis Felipe Salomão. São Paulo, 2 de maio de 2011.

CONSELHO NACIONAL DE JUSTIÇA. **Justiça em números 2024**. Brasília: CNJ, 2024. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2025/04/justica-em-numeros-2024.pdf. Acesso em 26 jun. 2024.

CONSELHO DA UNIAO EUROPEIA. **General Data Protection Regulation.** Bruxelas, 14. Abr. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=FR. Acesso em: 1 abr. 2024.

DINIZ, Maria Helena. **Curso de direito civil brasileiro**. Parte geral. 17. ed. São Paulo: Saraiva, 2002.

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.

DONEDA, Danilo. Os direitos de personalidade no Código Civil. **Revista da Faculdade de Direito de Campos**, Campos dos Goytacazes, ano 6, n. 6, p. 71. jun. 2005.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**. Joaçaba, v. 12, n. 2, p. 91-108, jul/dez, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em 26 jun. 2025. REVER REFERÊNCIA

GAGLIANO, P.S; FILHO, R.P. **Novo Curso de Direito Civil**: Responsabilidade Civil. v. 3. 21. ed. São Paulo: SaraivaJur, 2023. REVER REFERÊNCIA

GOMES, Luiz Roldão de Freitas. Os direitos da personalidade e o novo código civil: questões suscitadas. **Revista da EMERJ**. Rio de Janeiro, v.5, n.19, p.13-22, 2002. Disponível em: https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista19/revista19.pdf. Acesso em 26 jun. 2025.

ROSENVALD, Nelson; BRAGA NETTO, Felipe. **Responsabilidade civil:** teoria geral. 1. ed. Indaiatuba (SP): Editora Foco, 2024.

SARLET, I.W. Proteção de dados pessoais como direito fundamental autônomo na Constituição brasileira de 1988. *In*: BARZOTTO, Luciane Cardoso; COSTA, Ricardo H. Martins (orgs.). **Estudos sobre a Lei Geral de Proteção de Dados:** doutrina e aplicabilidade no âmbito laboral. Porto Alegre: Escola Judicial do Tribunal Regional do Trabalho (4ª região), 2022.

PEREIRA, Caio Mário da Silva. **Responsabilidade Civil**. 13.ed. Rio de Janeiro: Forense, 2022.

MENDES, L. S.; FUJIMOTO, M. (Orgs.). **Painel LGPD nos Tribunais**. Brasília: Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, 2024.

VENTURA, Magda Maria. O estudo de caso como modalidade de pesquisa. **Revista da Sociedade de Cardiologia do Estado do Rio de Janeiro**, Rio de Janeiro, v. 20, n. 5, p. 383-386, set./out. 2007. Disponível em: http://sociedades.cardiol.br/socerj/revista/2007_05/a2007_v20_n05_art10.pdf. Acesso em: 14 jun. 2025.

WARREN, Samuel D.; BRADEIS, Louis D. The Right to Privacy. **Harvard Law Review,** v. 4, n.5, p. 193-220, dec. 1890. Disponível em: https://doi.org/10.2307/1321160. Acesso em 26 jun. 2025.