XXXI CONGRESSO NACIONAL DO CONPEDI BRASÍLIA - DF

DIREITO, GLOBALIZAÇÃO E RESPONSABILIDADE NAS RELAÇÕES DE CONSUMO

CAIO AUGUSTO SOUZA LARA

CELSO HIROSHI IOCOHAMA

GEYSON JOSÉ GONÇALVES DA SILVA

D597

DIREITO, GLOBALIZAÇÃO E RESPONSABILIDADE NAS RELAÇÕES DE CONSUMO [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Caio Augusto Souza Lara, Celso Hiroshi Iocohama, Geyson José Gonçalves da Silva – Florianópolis: CONPEDI, 2024.

Inclui bibliografia
ISBN: 978-65-5274-060-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: UM OLHAR A PARTIR DA INOVAÇÃO E DAS NOVAS TECNOLOGIAS

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito e Globalização. 3. Responsabilidade nas relações de consumo. XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3: 2024 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXXI CONGRESSO NACIONAL DO CONPEDI BRASÍLIA - DF

DIREITO, GLOBALIZAÇÃO E RESPONSABILIDADE NAS RELAÇÕES DE CONSUMO

Apresentação

DIREITO, GLOBALIZAÇÃO E RESPONSABILIDADE NAS RELAÇÕES DE CONSUMO I

Os artigos contidos nesta publicação foram apresentados no Grupo de Trabalho Constituição, Teoria Constitucional e Democracia I durante o XXXI Congresso Nacional do Conselho Nacional de Pesquisa e Pós-graduação em Direito - CONPEDI, realizado dos dias 27 a 29 de novembro de 2024, sob o tema geral "Um olhar a partir da inovação e das novas tecnologias". O evento foi promovido por esta sociedade científica do Direito com o apoio de IPJ – Portucalense Institute for Legal Research e da ENFAM – Escola Nacional de Formação e Aperfeiçoamento de Magistrados. Foram patrocinadores a Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES, Itaipu Binacional, Universidade de Rio Verde, Athena e Universidade Santo Amaro.

A apresentação dos trabalhos abriu caminho para uma importante discussão, em que os pesquisadores do Direito puderam interagir em torno de questões teóricas e práticas, levando-se em consideração a temática central grupo. Essa temática traz consigo os desafios que as diversas linhas de pesquisa jurídica enfrentam no tocante ao estudo dos referenciais teóricos do Direito Constitucional e dos reflexos do constitucionalismo na atuação dos Poderes da República no país.

Os temas apresentados exploram questões contemporâneas relacionadas aos desafios do consumo, proteção de dados, sustentabilidade e justiça social, em um contexto marcado por crises econômicas e avanços tecnológicos. Destacam-se análises sobre o impacto da pandemia na elevação dos preços da cesta básica, o superendividamento e a insuficiência da tutela estatal no mínimo existencial, além da obsolescência programada e o aumento do lixo eletrônico. Questões como a hipervulnerabilidade de idosos em contratações digitais, a proteção de dados nos contratos eletrônicos e a responsabilidade civil por vazamento de informações também evidenciam a urgência de uma regulamentação robusta. Além disso, são discutidos os desafios socioambientais e econômicos da globalização, o desrespeito das Big Techs à privacidade, e a importância da boa-fé objetiva e da educação financeira como instrumentos para promover o consumo sustentável e equitativo, garantindo maior proteção aos consumidores em um cenário de transformações rápidas e complexas.

Na coletânea que agora vem a público, encontram-se os resultados de pesquisas desenvolvidas em diversos Programas de Pós-graduação em Direito, nos níveis de Mestrado e Doutorado, com artigos rigorosamente selecionados, por meio de dupla avaliação cega por pares (double blind peer review). Dessa forma, todos os artigos ora publicados guardam sintonia direta com este Grupo de Trabalho.

Agradecemos a todos os pesquisadores pela sua inestimável colaboração e desejamos uma ótima e proveitosa leitura!

Caio Augusto Souza Lara

Celso Hiroshi Iocohama

Geyson José Gonçalves da Silva

RESPONSABILIDADE CIVIL E VAZAMENTO DE DADOS: UMA ANÁLISE LEGAL DAS IMPLICAÇÕES JURÍDICAS

CIVIL LIABILITY AND DATA BREACH: A LEGAL ANALYSIS OF THE LEGAL IMPLICATIONS

Iolanda Resplande Nogueira
Janaina Gomes Lopes

Resumo

No contexto da era digital, a proteção de dados pessoais tornou-se essencial, especialmente após a promulgação da Lei Geral de Proteção de Dados (LGPD) no Brasil. Este artigo trata da responsabilidade civil por vazamento de dados e a abordagem na legislação brasileira com foco em três decisões do Superior Tribunal de Justiça (STJ) que ilustram diferentes interpretações da responsabilidade civil, além de examinar as tendências jurisprudenciais com base em decisões do Tribunal de Justiça de São Paulo (TJSP). A pesquisa adota uma abordagem bibliográfica qualitativa, explorando doutrinas jurídicas, artigos acadêmicos e decisões judiciais. O trabalho está dividido em oito seções: introdução, distinção entre dados sensíveis e não sensíveis, implicações legais da responsabilidade civil, estudo de caso das decisões do STJ, análise das tendências jurisprudenciais no Tribunal de Justiça de São Paulo (TJSP), levantamento dos casos concretos, conclusões dos estudos de caso e considerações finais. O objetivo geral é analisar a responsabilidade civil decorrente do vazamento de dados no Brasil, com ênfase nas decisões do STJ e nas tendências das decisões do TJSP e na aplicação prática da LGPD. Além disso, busca-se entender a necessidade de uma jurisprudência mais uniforme para proporcionar maior segurança jurídica nesse campo em constante evolução.

Palavras-chave: Responsabilidade civil, Vazamento de dados, Lgpd, Dados sensíveis, Proteção de dados pessoais

Abstract/Resumen/Résumé

In the context of the digital age, the protection of personal data has become essential, especially after the enactment of the General Data Protection Law (LGPD) in Brazil. This article addresses civil liability for data breaches and the approach in Brazilian legislation, focusing on three decisions of the Superior Court of Justice (STJ) that illustrate different interpretations of civil liability, as well as examining jurisprudential trends based on decisions of the São Paulo Court of Justice (TJSP). The research adopts a qualitative bibliographic approach, exploring legal doctrines, academic articles, and court decisions. The work is divided into eight sections: introduction, distinction between sensitive and non-sensitive data, legal implications of civil liability, case study of STJ decisions, analysis of jurisprudential trends in the São Paulo Court of Justice (TJSP), survey of concrete cases,

conclusions of the case studies, and final considerations. The main objective is to analyze civil liability arising from data breaches in Brazil, with an emphasis on STJ decisions and in the trends of the decisions of the São Paulo State Court of Justice (TJSP) and in the practical application of the General Data Protection Law (LGPD) the practical application of the LGPD. Additionally, it seeks to understand the need for more uniform jurisprudence to provide greater legal certainty in this constantly evolving field.

Keywords/Palabras-claves/Mots-clés: Civil liability, Data breach, Lgpd, Sensitive data, Personal data protection

INTRODUÇÃO

No atual panorama global, marcado pelo avanço tecnológico e pela crescente integração da sociedade à era digital, o volume de informações pessoais produzidas e processadas atingiu proporções sem precedentes. Este fenômeno, impulsionado pelo desenvolvimento sofisticado dos setores industriais e pela disseminação de procedimentos burocráticos nos âmbitos público e privado, coloca-nos diante de um cenário onde somos testemunhas da maior produção de dados pessoais na história da humanidade. Como salientado previamente por Mendes em 2014, antes mesmo da existência da Lei Geral de Proteção de Dados Brasileira (LGPD) - Lei 13.709/18.

A multiplicidade de bancos de dados abrangendo informações sobre diversos aspectos da vida humana, desde nascimentos até empregos, reflete a extensão desse fenômeno global. Neste contexto, a era digital surgiu como um catalisador, ampliando exponencialmente a coleta e processamento desses dados por diferentes entidades, sejam elas corporativas, governamentais ou institucionais. Contudo, essa explosão de informações pessoais suscita questões cruciais sobre a proteção dos direitos individuais, particularmente no que diz respeito à privacidade e neste contexto a responsabilidade civil emerge como uma peça-chave na proteção desses direitos, constituindo-se como um instrumento essencial para conter abusos e assegurar a devida reparação por danos decorrentes do tratamento inadequado dos dados pessoais sensíveis.

Ao pensarmos na internet, imediatamente nos vem à mente a quantidade de informações que são transmitidas e acessadas a todo momento. Em cada clique, temos acesso a inúmeras possibilidades. Com os avanços na disseminação da conexão à internet, de acordo com dados estatísticos divulgados pelo governo, provenientes da pesquisa TIC Domicílios 2022, realizada pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), constatou-se que 80% (oitenta por cento) da população brasileira possui acesso à internet, o que gera mais tráfego de informação e mais dados por entrada de usuário. Esse número de pessoas conectadas representa um desafio significativo para a gestão e segurança dos dados pessoais de todos esses indivíduos.

Diante desse cenário, não haveria outra alternativa senão buscar proteger os dados pessoais coletados pelo uso da internet. Deste modo, tornou-se necessária a elaboração de legislação mais específica para abordar questões sobre a proteção à privacidade, integridade das informações e a responsabilidade no uso da internet, para garantir o

tratamento ético e responsável, protegendo a privacidade e segurança das pessoas.

Partindo dessa perspectiva, é possível entender a necessidade do surgimento das legislações específicas no tratamento de dados. O propósito central deste artigo, portanto, é examinar a responsabilidade civil no contexto do tratamento de dados no Brasil, com ênfase em três decisões proferidas pelo Superior Tribunal de Justiça (STJ) e na identificação de tendências jurisprudenciais nas decisões do Tribunal de Justiça do Estado de São Paulo (TJSP).

Durante o desenvolvimento do artigo, utilizaremos como método a pesquisa bibliográfica qualitativa para explorar a discussão jurídica do tratamento de dados no país. Para alcançar esse objetivo, o estudo se propõe a: Investigar as divergências doutrinárias no entendimento da responsabilidade civil no tratamento de dados e examinar como essas divergências têm contribuído para a incerteza jurídica e as dificuldades na aplicação consistente da LGPD. Em uma tentativa de auxiliar na compreensão da legislação e promover um debate construtivo sobre o tema, visamos fomentar o desenvolvimento da doutrina e jurisprudência na proteção de dados.

1. A DISTINÇÃO ENTRE DADOS SENSÍVEIS E NÃO SENSÍVEIS: IMPORTÂNCIA E RELEVÂNCIA NA ERA DA PROTEÇÃO DE DADOS.

A Lei Geral de Proteção de Dados define no seu artigo 5, inciso I e II, o que entende como dado pessoal e dado pessoal sensível. O dado pessoal é descrito como a informação relacionada à pessoa natural identificada ou identificável; já o dado pessoal sensível é o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Dados pessoais constituem nome, endereço, e-mail, número de telefone, entre outros. Os dados pessoais são essenciais para a identificação de um indivíduo, mas não revelam informações sensíveis sobre ele. Já os dados sensíveis são informações mais delicadas e íntimas sobre uma pessoa; como dito anteriormente eles incluem detalhes como origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicatos, dados de saúde, vida sexual, dados genéticos e biométricos. Esses dados são considerados sensíveis porque se mal utilizados ou divulgados, podem causar danos significativos à

privacidade e à integridade da pessoa.

No entanto, apesar da distinção criada pela legislação, parte da doutrina entende que não apresenta relevância a distinção de dados pessoais sensíveis e não sensíveis, conforme dito por Danilo Doneda, cujo entendimento é que um dado em si não é intrinsecamente perigoso ou discriminatório, mas sim o seu uso (DONEDA, 2003, p. 162). Isso significa que até mesmo dados que não são classificados como sensíveis pela LGPD podem tornar-se sensíveis quando submetidos a determinados tipos de tratamento, revelando, por exemplo, aspectos da personalidade de uma pessoa que podem levar a práticas discriminatórias.

Um dado trivial pode também se transformar em um dado sensível; particularmente, quando se têm disponíveis tecnologias (por exemplo, Big Data) que permitem correlacionar uma série de dados para prever comportamentos e acontecimentos" (BIONI, 2018,p. 84).

Dados coletados de "curtidas" que, por si só, não representam conteúdo sensível, no entanto, podem se tornar sensíveis quando tratados de forma a identificar dados personalíssimos, e potencialmente discriminatórios. (BIONI, 2018, p. 85)

A reflexão sobre a natureza dos dados e os possíveis desdobramentos de seu tratamento ressalta a necessidade de estratégias eficazes de proteção e controle, especialmente em um contexto de avanço tecnológico e uso cada vez mais amplo de ferramentas de análise de dados. A compreensão de que até mesmo dados inicialmente considerados triviais podem se tornar sensíveis mediante determinados tratamentos, ressalta a complexidade desse cenário e a urgência em se estabelecer medidas robustas de segurança e regulamentação.

Konder argumenta, por exemplo, que a sensibilidade dos dados está intrinsecamente ligada ao contexto específico em que são utilizados, enfatizando a importância de analisá-los com base na concretude, ou seja, na realidade específica em que se encontram, em oposição a uma avaliação abstrata e individualizada. Ele ressalta que o valor dos dados não pode ser determinado isoladamente, mas sim em relação ao ambiente em que estão inseridos e às finalidades para as quais são empregados.

Para o autor, a definição de um dado como sensível não pode ser feita de forma abstrata, sendo necessário avaliar o potencial de seu tratamento como instrumento de estigmatização ou discriminação, levando em conta a privacidade, identidade pessoal e dignidade humana. Portanto, a natureza jurídica dos dados deve ser examinada com base

no caso concreto, pois um dado que inicialmente não é sensível pode tornar-se sensível dependendo do contexto, enquanto um dado sensível pode não representar riscos para o titular, dependendo de como é tratado. Essa visão contextual é essencial para a aplicação justa e equilibrada da LGPD, considerando a dinâmica e a complexidade das relações digitais atuais

Para Mulholland, em seu artigo Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais(2017), não deve haver distinção nos regimes de responsabilidade civil com base na classificação dos dados como sensíveis ou não. Em outras palavras, a Lei Geral de Proteção de Dados Pessoais estabelece um único regime de responsabilidade civil, independentemente da natureza dos dados protegidos.

Diante da complexidade inerente à distinção entre dados sensíveis e não sensíveis na era da proteção de dados, surge a necessidade premente de uma análise aprofundada das implicações legais associadas ao instituto da Responsabilidade Civil na LGPD. Essa análise se torna crucial para entender como a legislação aborda as responsabilidades das organizações

que lidam com dados pessoais, independentemente da classificação desses dados. Assim, explorar as implicações legais dessa responsabilidade à luz da LGPD permite uma compreensão mais abrangente das obrigações legais e dos desafios enfrentados pelas empresas na proteção dos direitos dos titulares de dados.

2. ANÁLISE DAS IMPLICAÇÕES LEGAIS DO INSTITUTO DA RESPONSABILIDADE CIVIL NO VAZAMENTO DE DADOS

A Lei Geral de Proteção de Dados do Brasil estabelece um conjunto de normas e princípios para o tratamento de dados pessoais por organizações públicas e privadas, com o objetivo de garantir a privacidade e a segurança dessas informações. Dentro dessa estrutura legal, a responsabilidade civil desempenha um papel crucial na responsabilização das partes envolvidas em casos de violação da lei.

De início é essencial compreender que a LGPD atribui responsabilidades específicas aos agentes que lidam com dados pessoais, os chamados controladores e operadores. Os controladores são as entidades responsáveis por tomar decisões sobre o

tratamento dos dados, enquanto os operadores realizam o tratamento em nome dos controladores, seguindo as limitações estabelecidas pelo art. 5º e seguintes da lei. Ambos têm obrigações claras em relação à proteção e ao uso adequado dos dados, e a responsabilidade civil surge quando essas obrigações não são cumpridas.

De acordo com Bioni (2020), a LGPD estabelece duas situações que podem levar à responsabilidade civil dos agentes de tratamento de dados: a violação da legislação de proteção de dados pessoais e a violação da segurança dos dados. Ambas estão relacionadas ao conceito de tratamento irregular, detalhado no artigo 44 da lei.

Segundo o autor, a LGPD institui um regime de responsabilidade civil subjetiva em relação à proteção de dados pessoais. Isso significa que, para responsabilizar um agente de tratamento de dados por danos causados aos titulares dos dados, é necessário comprovar a existência de culpa, ou seja, a conduta inadequada ou negligente do agente que resultou nos danos. Além disso, o art. 43 da lei ressalta que se a alegação da vítima da irregularidade do tratamento de dado for verossímil, ou exista hipossuficiência para a produção de provas ou, ainda, seja a produção de prova onerosa, o juiz poderá decretar a inversão do ônus da prova.

No entanto, para outros autores como José Henrique de Oliveira Couto (2023), é possível verificar a existência implícita da responsabilidade objetiva na LGPD ao analisarmos os princípios embasadores dessa legislação, tais como a boa-fé objetiva, finalidade, segurança, entre outros estabelecidos no art. 6º da legislação. Embora a LGPD não mencione explicitamente a responsabilidade objetiva, essa abordagem pode ser adotada com base nos princípios e normas da legislação vigente, a fim de assegurar a proteção dos dados pessoais e a responsabilização adequada em casos de violação da privacidade e segurança dessas informações.

Além disso, Caitlin Mulholland (2020) destaca três princípios fundamentais da responsabilidade civil que definem a responsabilidade como objetiva: o princípio da segurança, da prevenção e da responsabilização e prestação de contas, conforme delineados nos incisos VII, VIII e X do art. 6º da LGPD. Esses princípios são as definições sólidas que fundamentam a conclusão de que a LGPD, é uma legislação que protege os titulares de dados e lhes confere o direito à indenização com base na teoria do risco, ou seja, objetiva.

Nesse contexto, uma interpretação sistemática, guiada pelos princípios listados, deixa claro que o regime pretendido é o da responsabilização, independentemente da aferição de culpa. Essa conclusão não se baseia exclusivamente na análise dos princípios e

da interpretação sistemática, mas de acordo com essa corrente doutrinária, esses elementos são suficientes para estabelecer as diretrizes esperadas em relação ao tratamento de dados e à responsabilização correspondente em casos de danos.

Diante dessa dualidade de interpretações doutrinárias, é possível compreender por que as decisões judiciais sobre o assunto ainda não estão consolidadas e variam, com algumas concessões de indenização com base apenas na exposição dos dados e outras condicionando o pagamento de danos morais à comprovação de danos sofridos. De qualquer modo, quando ocorre uma violação da LGPD, seja por vazamento de dados, acesso não autorizado ou qualquer outra forma de tratamento inadequado dos dados pessoais, os titulares desses dados têm o direito de buscar reparação pelos danos sofridos, incluindo danos materiais, morais, patrimoniais, entre outros, de acordo com a redação do art. 42 da Lei Geral de Proteção de Dados.

A análise das implicações legais da responsabilidade civil na LGPD deve considerar como esses critérios são aplicados na prática e como as decisões judiciais têm interpretado essas questões. Em resumo, a análise das implicações legais do instituto da Responsabilidade Civil na LGPD é essencial para compreender como a lei busca garantir a proteção dos dados pessoais e responsabilizar as organizações em caso de violação. Isso envolve examinar as obrigações das partes envolvidas, os tipos de danos envolvidos e os critérios para a responsabilização, fornecendo assim um quadro abrangente das questões legais relacionadas à proteção de dados no Brasil.

3. ESTUDO DE CASOS

3.1. DESCRIÇÃO E ANÁLISE DO JULGAMENTO DO STJ NO ARESP 2130619

O Superior Tribunal de Justiça (STJ), por meio da Segunda Turma, determinou no ARESP 2130619 que o vazamento de dados pessoais não constitui automaticamente dano moral indenizável. O caso envolveu a concessionária Eletropaulo, que foi condenada pelo Tribunal de Justiça de São Paulo (TJSP) a pagar indenização por danos morais a uma cliente devido ao vazamento de seus dados. A consumidora alegou que informações como nome, data de nascimento, endereço e número do documento de identificação foram acessadas por terceiros e compartilhadas, gerando riscos de fraude e importunações.

No entanto, o STJ, ao analisar o recurso da Eletropaulo, concluiu que os dados vazados não se enquadram como sensíveis, conforme definido pela Lei Geral de Proteção

de Dados Pessoais (LGPD). O relator do caso, Ministro Francisco Falcão, ressaltou que o dano moral não é presumido no caso de vazamento de dados comuns, sendo necessário comprovar o efetivo prejuízo decorrente do acesso não autorizado às informações. Essa decisão reflete a tese defendida por Bioni, mencionada no tópico 2, ao afirmar que o vazamento de dados pessoais não sensíveis, por si só, não gera dano in re ipsa, ou seja, não se presume o dano moral, tornando indispensável a demonstração de prejuízo concreto e específico.

Dessa forma, o STJ acolheu o recurso da Eletropaulo, revertendo a decisão do TJSP e restabelecendo a sentença que julgou improcedente o pedido de indenização por danos morais. Esse posicionamento está em linha com a interpretação de que, para que a responsabilidade civil seja configurada, é necessário não apenas o evento do vazamento, mas também a prova da existência de um dano real e a culpa do agente responsável pelo tratamento dos dados.

No caso em tela, portanto, a interpretação dada aos dispositivos da LGPD, foi que a responsabilidade descrita é a responsabilidade subjetiva, no qual há o entendimento de que deve ser comprovada a culpa: negligência,imprudência ou imperícia do agente de tratamento de dados, nesse caso, a concessionária de energia de São Paulo.

Assim, o vazamento dos dados foi tratado apenas como uma inconveniente exposição, não havendo dano a ser reparado. Dessa maneira, ficou estabelecido neste caso em comento que o vazamento de dados pessoais não gera automaticamente dano moral.

3.2. DESCRIÇÃO E ANÁLISE DO JULGAMENTO DO STJ NO ARESP 2192605

Em oposição ao caso apontado no ítem 3.1, o Superior Tribunal de Justiça (STJ), por meio da Quarta Turma, no julgamento do Agravo em Recurso Especial nº 2192605, proferiu decisão estabelecendo que o vazamento de dados pessoais configura dano moral indenizável. O caso envolveu a agência de turismo online *Hurb Technologies S.A.* (antigo Hotel Urbano), que foi condenada pelo Tribunal de Justiça do Rio de Janeiro (TJRJ) a pagar indenização por danos morais a uma cliente devido à exposição não autorizada de seus dados.

O consumidor alegou a ocorrência de falha no serviço, pois a empresa foi alvo de um ataque hacker que resultou na divulgação de informações não anonimizadas de seus clientes, como nome, sobrenome e e-mail, o que resultou em diversas tentativas de fraude e

importunações direcionadas à cliente. A empresa foi condenada a pagar R$10.000,00 (dez mil reais) de indenização por danos morais, valor que foi mantido pelo STJ, que considerou o montante adequado para refletir o dano sofrido e para servir como medida preventiva.

O STJ confirmou a decisão de primeira instância, ressaltando que o vazamento de dados pessoais constitui falha no serviço e que a proteção dessas informações é um dever previsto na Lei 13.709/18 (LGPD). A decisão baseou-se na interpretação de que a empresa, ao ser responsável pelos dados, assume o risco de eventuais falhas que resultem em vazamentos, independentemente da culpa direta.

O acesso não autorizado aos dados, somado à exposição não consentida, caracterizou dano moral. Portanto, a jurisprudência do STJ, por meio do julgamento do AREsp 2192605, estabeleceu que o vazamento de dados pessoais constitui um risco inerente à atividade empresarial, equivalente à responsabilidade objetiva. Esse posicionamento converge com a tese de José Henrique de Oliveira Couto, discutida no tópico 2, ao reforçar que as empresas são responsáveis pela segurança dos dados pessoais de seus clientes, inclusive em casos de ataques externos.

3.3. DESCRIÇÃO E ANÁLISE DO JULGAMENTO NO STJ NO ARESP 2.106.817

O Superior Tribunal de Justiça (STJ), por meio da Terceira Turma, proferiu decisão estabelecendo que o tratamento indevido de dados pessoais bancários configura dano moral indenizável. No caso em questão, o Banco Votorantim S.A. foi condenado, em primeira instância, a indenizar seu cliente em razão de uma fraude conhecida como "golpe do boleto", que ocorreu em decorrência de um vazamento de dados. A fraude visava a quitação de um débito referente a um contrato de financiamento de veículo, em que o golpista, utilizando um site que aparentava ser legítimo, simulou a interface da instituição financeira para enganar o consumidor. O suposto representante do banco, após solicitar apenas o CPF do cliente, forneceu os demais dados, como o número do contrato, o valor financiado e o saldo devedor, o que fez o cliente acreditar que se tratava da própria instituição e realizar o pagamento do boleto.

O Tribunal de Justiça do Estado de São Paulo reformou a sentença, argumentando que, na ausência de prova de que a fraude ocorreu no ambiente da instituição financeira ou por culpa desta, o ônus da prova recaía sobre o autor da ação.

No entanto, o STJ restabeleceu a sentença de primeira instância, entendendo que o fato de o fraudador ter acesso aos dados do autor em razão do contrato celebrado com o

banco configurado nexo causal necessário para a responsabilização da instituição financeira.

A questão central reside no nexo causal entre a atuação dos estelionatários e o vazamento de dados pessoais pelo banco. Os dados bancários são, em regra, tratados exclusivamente pelas instituições financeiras, e a possibilidade de terceiros acessem informações sigilosas que causem prejuízo ao consumidor fere não apenas o Código de Defesa do Consumidor (CDC), mas também o artigo 44 da Lei Geral de Proteção de Dados (LGPD). Se criminosos obtiveram acesso a dados do consumidor e o dano resultou do tratamento inadequado desses dados, há responsabilidade objetiva por parte do banco. Esse entendimento é compatível com a Súmula 479/STJ, que estabelece a responsabilidade objetiva das instituições financeiras pelos danos causados por fortuito interno, incluindo fraudes praticadas por terceiros.

Essa decisão difere dos outros recursos repetitivos apresentados, uma vez que se trata de um caso específico envolvendo uma instituição financeira e um dano material decorrente do vazamento de dados, não se limitando ao vazamento em si.

É relevante este destaque, visto que, grande parte dos julgados pelo STJ entre janeiro e agosto de 2024 envolvendo dano moral e vazamento de dados pessoais, estão relacionados a instituições financeiras e seguem o mesmo entendimento.

4. ANÁLISE DAS TENDÊNCIAS JURISPRUDENCIAIS NO TRIBUNAL DE JUSTIÇA DE SÃO PAULO (TJSP)

Seguindo o propósito de se constatar o quão é premente a edição de normativos específicos no tratamento de dados sob a ótica da responsabilidade civil, faremos, neste tópico, um estudo das tendências jurisprudenciais no Tribunal de Justiça de São Paulo (TJSP), a partir de três decisões significativas sustentadas pelo Superior Tribunal de Justiça (STJ) e que demonstram a relevância de se observar as tendências jurisprudenciais apontadas, as suas implicações e interpretações que delas se refletem e desenvolvem.

Para bem ilustrar, são apresentadas, em resumo, as decisões do Egrégio Superior Tribunal de Justiça tratadas no tópico 3:

Caso 1 - ARESP 2130619 – o vazamento de dados pessoais não sensíveis, por si só, não gera dano *in re ipsa*. Não se presume o dano moral, tornando indispensável a demonstração de prejuízo concreto e específico. Para que a responsabilidade civil seja configurada é necessária a prova do dano real e da culpa do agente responsável pelo

tratamento dos dados.

Caso 2 - ARESP nº 2192605 – o vazamento de dados pessoais constitui falha do detentor dos dados, que ao ser responsável por eles, assume o risco de eventuais falhas que resultem em vazamentos, independentemente da culpa direta. A proteção dessas informações é um dever previsto na LGPD, configurando dano moral indenizável.

Caso 3 – ARESP 2.106.817 - o tratamento indevido de dados pessoais bancários configura dano moral indenizável. O fato de o fraudador ter acesso aos dados do autor em razão do contrato celebrado com bancos configura nexo causal suficiente para a responsabilidade objetiva da instituição financeira.

As ações judiciais que tratam do vazamento de dados pessoais têm se pautado por análises mais detalhadas e específicas de cada caso concreto, buscando determinar a responsabilidade do infrator com base em diversos fatores.

As decisões têm considerado aspectos como a natureza dos dados vazados — se são dados sensíveis ou comuns — e os efeitos gerados pelo vazamento. Nos casos que envolvem o vazamento de dados pessoais comuns, tem prevalecido o entendimento estabelecido no AREsp nº 2.130.619/SP, no qual o STJ concluiu que o mero vazamento de dados, por si só, não resulta automaticamente em dano moral indenizável. Considera-se também outros fatores além do próprio vazamento, especialmente quando se trata de dados sensíveis, o que torna a análise mais complexa.

A jurisprudência também tem levado em conta a ocorrência de lesão à honra subjetiva do requerente, a prova da relação entre o responsável pelo tratamento dos dados e terceiros que possam ter acessado os dados indevidamente, e se houve falhas no tratamento ou na proteção dos dados por parte do requerido. Em resumo, a tendência atual é a de uma análise minuciosa de todos os elementos envolvidos no incidente, e não apenas do ato de vazamento em si.

Nos casos cada vez mais frequentes de vazamento de dados relacionados a instituições financeiras, há uma preocupação adicional em distinguir se o evento foi causado por fortuito interno ou externo, se é possível rastrear a origem do vazamento, e se a instituição financeira adotou medidas de proteção adequadas para prevenir tais incidentes.

Dada a crescente dependência da sociedade moderna em relação ao uso diário de dados pessoais para diversas atividades, é crucial que as ações judiciais sejam baseadas em uma análise criteriosa dos fatores envolvidos. Isso evita que a justiça se torne um instrumento exploratório.

4.1. TENDÊNCIAS JURISPRUDENCIAIS – CASOS CONCRETOS

Com o intuito de apresentar uma visão prática do tema abordado no artigo, este tópico analisa alguns casos, conforme apontados na tabela inserida abaixo, selecionados por envolverem situações de vazamento de dados e a consequente avaliação da responsabilidade civil.

Número do Processo – TJ/SP	Pedido Inicial	Sentença
1014883-34.2023.8.26.0161	Boleto falso com dados do consumidor. indenização por danos materiais e morais. Violação aos dados.	Condenação da instituição financeira. Dano moral configurado. Ato de terceiro não elide a responsabilidade da instituição financeira
0015489-74.2023.8.26.0001	Fraude bancária - falso funcionário em posse dos dados do cliente o orientou a realizar pagamento. Vazamento de dados sigilosos, movimentação financeira em desconformidade com o perfil do cliente não detectada. Indenização por danos materiais e morais.	Provimento parcial. Condenação do banco ao ressarcimento da quantia desembolsada. Dano moral não configurado.
1001536-64.2024.8.26.0268	Ação indenizatória contra SERASA - Vazamento de dados à terceiros sem consentimento. Indenização por danos morais.	Pedido improcedente. Não houve verossimilhança nas alegações, pois não foram especificados quais dados teriam sido vazados. Sem dano comprovado. Dano moral não configurado.
483-69.2023.8.26.0472	Ação indenizatória contra banco e instituição de pagamento. Cliente solicitou antecipação de boleto, recebeu via WhatsApp, pagou, mas era falso. Vazamento de dados, indenização por dano material.	Ação improcedente. Autora repassou dados sensíveis e sigilosos a central falsa. não houve indício de vazamento de dados, a autora em contato com uma central falsa repassou dados sensíveis e sigilosos aos criminosos. Sem indícios de vazamento de dados pelo banco; responsabilidade não atribuída ao banco.

10276-53.2024.8.26.0001	Ação indenizatória contra banco. Vazamento de dados pessoais. Boleto falso de parcela de dívida enviado por terceiro.	Pedido improcedente. O contato se originou por meio de canal não pertencente à ré, bem como o beneficiário do pagamento é terceiro. Não há indício de que o suposto vazamento de dados foi causado pela ré.
1055830-93.2021.8.26.0002	Ação de indenização por danos morais em face de uma imobiliária e uma construtora. O autor, após firmar compromisso de compra e venda de imóvel, teve seus dados pessoais compartilhados de forma indevida com empresas estranhas ao negócio.	Autor consentiu compartilhamento para verificação de crédito, dados vazaram para empresas não autorizadas (arquitetura, marcenaria). Violação do art. 46 da LGPD; ré condenada a cessar transmissão de dados; sem dano moral por falta de comprovação de prejuízo relevante. O vazamento de dados, não tem o condão, por si só, de gerar dano moral indenizável.
0032780-84.2023.8.26.0002	Ação indenizatória contra a empresa Shein/ In Glow. Terceiro hackeou a conta da requerida, razão pela qual a autora requer condenação por danos morais.	Pedido improcedente. 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.
1001584-79.2024.8.26.0411	Ação de indenização por danos morais em face de Serasa. Vazamento de dados pessoais que ficaram disponíveis na Dark Web.	Ação improcedente. Ausência de elementos probatórios das alegações do autor. Não foi demonstrado que o suposto vazamento ocasionou dano moral.
1012668-30.2023.8.26.0438	Ação de indenização por danos morais e materiais contra hospital e instituição financeira. Vazamento de dados de paciente internado; golpistas se passaram por médicos. Falha na segurança da instituição financeira na autorização da transferência PIX.	Ação improcedente. Ausência de nexo causal; excludentes de fato de terceiro e fato exclusivo do consumidor. Falha no sigilo de dados do hospital não determinou o dano; descuido do requerente. Banco não responsável, sem vínculo com o autor e sem obrigação de controlar todas as transações.
1000440-28.2023.8.26.0016	Ação de indenização por danos morais em face de empresas de transporte (SPTrans). Exposição de dados após crime cibernético; falha na segurança e na prestação de serviços. Responsabilização da empresa pela falta de segurança dos sistemas.	Ação improcedente. Sem comprovação de dano; vazamento de dados por si só não gera responsabilidade civil. Sem danos morais in re ipsa; não comprovados transtornos graves além da preocupação com o vazamento.

Como demonstrado no quadro de decisões acima, boa parte dos casos envolvendo vazamento de dados e dano moral está relacionada a instituições financeiras. Os tribunais frequentemente responsabilizam as empresas com base na responsabilidade objetiva, no entendimento que o vazamento de dados é um risco inerente à atividade. No entanto, para que

haja condenação, é essencial a comprovação de prejuízo concreto.

Decisões favoráveis aos autores ocorrem quando os bancos não garantem a segurança adequada dos dados, enquanto casos improcedentes costumam se basear na ausência de provas de danos específicos ou na contribuição do próprio cliente para o incidente, como compartilhamento indevido de informações.

Nos demais casos, observa-se uma tendência similar de responsabilização com base na responsabilidade objetiva, mas com nuances específicas dependendo do setor envolvido. Parte dos processos se refere a empresas de tecnologia, plataformas digitais e serviços de proteção ao crédito.

As decisões favoráveis aos consumidores, nesses casos, geralmente se fundamentam na falha das empresas em adotar medidas adequadas de segurança para proteger os dados pessoais, especialmente quando se comprova o uso indevido das informações por terceiros. No entanto, assim como nos casos com instituições financeiras, a comprovação de prejuízo concreto é um fator decisivo para a procedência do pedido de indenização.

Por outro lado, quando os tribunais constatam que as empresas adotaram todas as medidas de segurança razoáveis ou que o vazamento ocorreu por fatores externos imprevisíveis, as ações têm a tendência de serem julgadas improcedentes. Esses casos reforçam a necessidade de demonstrar uma conexão direta entre a falha na segurança e o dano alegado pelo consumidor, evidenciando que a simples ocorrência do vazamento não presume, por si só, o direito à indenização por dano moral.

Esses exemplos concretos permitem relacionar os entendimentos jurisprudenciais às teses abordadas, evidenciando como as decisões dos tribunais dialogam com as questões teóricas sobre a configuração de dano moral e a atribuição de responsabilidade, levando em conta as especificidades de cada caso.

4.2. CONCLUSÕES DERIVADAS DA ANÁLISE DO ESTUDO DE CASO

Em síntese, os julgamentos do Superior Tribunal de Justiça (STJ) nos casos AREsp 2130619, AREsp 2192605 e AREsp 2106817, oferecem abordagens distintas sobre a responsabilidade civil decorrente do vazamento de dados pessoais. Enquanto no primeiro caso o STJ concluiu que o simples vazamento de dados pessoais não sensíveis não gera automaticamente dano moral indenizável, requerendo a comprovação de prejuízo efetivo e a caracterização de culpa do agente de tratamento de dados, no segundo caso, o STJ estabeleceu que o vazamento de dados pessoais configura dano moral indenizável, visto

como um risco inerente ao empreendimento, equivalente à responsabilidade objetiva. Por sua vez, no terceiro julgado, o STJ concluiu que o tratamento indevido de dados bancários, que resulta em fraude, configura dano moral indenizável, e estabelece a responsabilidade do banco pelo vazamento de dados pessoais.

Essas decisões refletem interpretações distintas sobre a responsabilidade civil no contexto do vazamento de dados pessoais, evidenciando a complexidade e as nuances envolvidas nessa matéria. Enquanto a primeira decisão adota uma abordagem mais cautelosa, exigindo a demonstração de prejuízo concreto e culpa do agente, a segunda decisão reconhece o dano moral presumido diante da exposição não autorizada de informações pessoais, atribuindo responsabilidade objetiva ao agente de tratamento de dados.

A terceira decisão, por sua vez, trata de um caso que não envolve apenas o simples vazamento de dados, mas sim um dano evidente. Essa decisão é particularmente relevante, pois aborda uma questão frequentemente levada aos tribunais: o vazamento de dados associado a golpes envolvendo instituições financeiras.

Diante desse panorama, fica evidente a importância dada a uma análise cuidadosa e contextualizada de cada caso concreto, das provas documentais e testemunhais, pois é fundamental levar em consideração as circunstâncias específicas envolvidas.

A jurisprudência do STJ ainda não está consolidada, e cada caso de vazamento de dados pode ser julgado de maneira distinta, como demonstrado anteriormente por esses três casos e pela tabela dos processos oriundos do TJ-SP.

CONSIDERAÇÕES FINAIS

A Lei Geral de Proteção de Dados (LGPD) classifica os dados pessoais como sensíveis ou não, mas diante de uma realidade complexa, caracterizada pela sociedade do risco, do conhecimento, da inovação e da globalização, é fundamental superar essa dicotomia. Nesse contexto, tanto os dados pessoais sensíveis quanto os não sensíveis devem ser avaliados de acordo com o caso específico, considerando o titular dos dados, o contexto envolvido do vazamento de dados, o grau de lesão, o potencial de risco e as medidas tomadas para mitigar ou neutralizar danos decorrentes do tratamento. O caso concreto é quem deve determinar a natureza dos dados pessoais.

O Superior Tribunal de Justiça (STJ), ao analisar os dados pessoais à luz da LGPD,

concluiu que no vazamento de dados pessoais, é preciso comprovar a culpa do agente de tratamento. Em um outro julgado, no entanto, chegou a uma conclusão diferente, como visto em outro momento no artigo. Assim, há divergências dentro do próprio STJ sobre a questão do dano moral relacionado ao vazamento de dados, com algumas turmas entendendo que não há danos morais e outras entendendo o contrário. A saída para essa diferença de entendimento pode estar na análise do caso concreto em cada situação e não apenas na distinção entre dados sensíveis ou não.

A partir da observação da tabela inserida no tópico 4.1, e considerando os pontos expostos ao longo do texto, a conclusão central é que, embora exista uma presunção de responsabilidade das empresas quanto à proteção dos dados, a efetivação dessa responsabilidade e a consequente reparação dependem da comprovação de um nexo entre a falha de segurança e o dano sofrido pelo consumidor. Esse posicionamento busca equilibrar a proteção dos direitos dos titulares de dados com a necessidade de se evitar condenações baseadas apenas na presunção de dano moral in re ipsa.

A busca por uma jurisprudência mais coesa e uma aplicação uniforme da LGPD são fundamentais para assegurar a previsibilidade das decisões e a proteção efetiva dos direitos dos titulares de dados, para assim, conseguirmos garantir uma maior segurança jurídica sobre esse tema.

REFERÊNCIAS

Doutrina

BIONI, Bruno Ricardo. Proteção de Dados Pessoais - A Função e os Limites do Consentimento. Forense, 10/2018.

BRASIL. **Ministério das Comunicações. 80% dos domicílios brasileiros possuem acesso à internet, aponta pesquisa.** Disponível em: <https://www.gov.br/mcom/pt-br/noticias/2023/maio/80-dos-domicilios-brasileiros-possu em- acesso-a-internet-aponta-pesquisa>. Acesso em: 22 dez. 2024.

BRASIL. **Lei Geral de Proteção de Dados**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Acesso em: 25 fev. 2024

COUTO, José Henrique de Oliveira. **Vazamentos de dados e dano moral in re ipsa: comentários ao Agravo em Recurso Especial nº 2.130.619/SP**. Revista IBERC, Belo Horizonte, v. 6, n. 2, p. 171-188, maio/ago. 2023. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/662/506>. Acesso em: 22 dez. 2024.

DONEDA, Danilo César Maganhoto. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados**. São Paulo: Thomson Reuters, 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados**. Rio de Janeiro: Editora Renovar, 2005.

KONDER, Carlos Nelson. **O tratamento de dados sensíveis à luz da Lei 13.709/2018**. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** São Paulo: Thomsom Reuters, Brasil, 2019, p. 460.

MENDES, Laura. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1. ed. Porto Alegre: Livraria do Advogado, 2014.

MULHOLLAND, Caitlin. **A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais**: culpa ou risco? Migalhas, 2020. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-o u-risco>. Acesso em: 25 fev. 2024.

MULHOLLAND, Caitlin. R**esponsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018)**. Disponível em:

<https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-da dos-sensi%CC%81veis.pdf>. Acesso em: 25 fev. 2024.

Jurisprudência

STJ. *Agravo em Recurso Especial 2.130.619* - SP. Julgado em: 7/03/2023. Relator: Francisco Falcão.

STJ. *Agravo em Recurso Especial 2.192.605* - RJ. Julgado em: 10/11/2022. Relator: Antonio Carlos Ferreira.

STJ. *2.106.817*– SP. Julgado em: 16/04/2024. Relator: Ricardo Villas Boas Cuevas.

Processos analisados no Tribunal de Justiça do Estado de São Paulo

TJSP. *Apelação Cível: AC 1000094-64.2022.8.26.0161*, Relator: Daise Fajardo Nogueira Jacot, Data de Julgamento: 28/02/2023

TJSP. *Recurso Inominado Cível: 0015489-74.2023.8.26.0001*, Relator: Olavo Paula Leite Rocha - Colégio Recursal, Data de Julgamento: 14/08/2024

TJSP. Procedimento do Juizado Especial Cível. Processo nº 1001536-64.2024.8.26.0268, Juiz (a) de Direito: Dr (a). Patricia Braguini, Data de Julgamento 30/07/2024

TJSP. *Procedimento do Juizado Especial Cível. Processo nº 0000483-69.2023.8.26.0472*, Juiz (a) de Direito: Dr (a). Otacilio José Barreiros Junior, Data de Julgamento 02/08/2024

TJSP. *Procedimento do Juizado Especial Cível. Processo nº 0010276-53.2024.8.26.0001*, Juiz (a) de Direito Dr (a): Aluísio Moreira Bueno, Data de Julgamento 01/08/2024

TJSP. *Procedimento Comum Cível. Processo nº 1055830-93.2021.8.26.0002.* 2ª Vara Cível, Juiz(a) de Direito: Dr(a). Cindy Covre Rontani Fonseca, Data de Julgamento 16/08/2024

TJSP. *Procedimento do Juizado Especial Cível. Processo nº 0032780-84.2023.8.26.0002,* Juiz(a) de Direito: Jonas Ferreira Angelo de Deus, Data de Julgamento 07/08/2024

TJSP. *Procedimento Comum Cível. Processo nº 1001584-79.2024.8.26.0411*, Juiz (a) de Direito: Dr (a). Luciana Bertoncini, Data de Julgamento 16/08/2024

TJSP. *Procedimento Comum Cível. Processo nº 1012668-30.2023.8.26.0438*, Juiz (a) de Direito: Dr (a). Vinicius Nascimento, Data de Julgamento 18/07/2024

TJSP. *Procedimento do Juizado Especial Cível. Processo Civil nº 1000440-28.2023.8.26.0016*, Juiz (a) de Direito: Dr (a). Ligia Bueno, 13/07/2023.