INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA

ESCOLA DE DIREITO E ADMINISTRAÇÃO PÚBLICA

PROGRAMA DE PÓS-GRADUAÇÃO PROFISSIONAL

STRICTO SENSU EM DIREITO

MESTRADO PROFISSIONAL EM DIREITO

Alexandre Magalhães Pinheiro

A RESPONSABILIDADE CIVIL POR INCIDENTES DE SEGURANÇA NA LGPD: UMA ANÁLISE À LUZ DA JURISPRUDÊNCIA DO SUPERIOR TRIBUNAL DE JUSTIÇA

BRASÍLIA – DF
2025

Alexandre Magalhães Pinheiro

A RESPONSABILIDADE CIVIL POR INCIDENTES DE SEGURANÇA NA LGPD: UMA ANÁLISE À LUZ DA JURISPRUDÊNCIA DO SUPERIOR TRIBUNAL DE JUSTIÇA

Dissertação de Mestrado apresentada no Programa de Pós-Graduação *Stricto Sensu*, no curso de Mestrado Profissional em Direito, do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP/Brasília), para obtenção do título de Mestre.

Orientadora: Laura Schertel Ferreira Mendes

BRASÍLIA – DF
2025

Alexandre Magalhães Pinheiro

A RESPONSABILIDADE CIVIL POR INCIDENTES DE SEGURANÇA NA LGPD: UMA ANÁLISE À LUZ DA JURISPRUDÊNCIA DO SUPERIOR TRIBUNAL DE JUSTIÇA

Dissertação de Mestrado apresentada no Programa de Pós-Graduação *Stricto Sensu*, no curso de Mestrado Profissional em Direito, do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP/Brasília), para obtenção do título de Mestre.

Data da aprovação: 16/06/2025

BANCA EXAMINADORA

_____

Prof.ª Drª Laura Schertel Ferreira Mendes
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP)
Presidente/Orientadora

_____

Prof.ª Drª. Tainá Aguiar Junquilho
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP)
Coorientadora

_____

Prof. Dr. Guilherme Pereira Pinheiro
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP)
Professor Membro

_____

Prof. Dr. Filipe José Medon Affonso
Professor Convidado

_____

Prof.ª Drª Karina Nunes Fritz
Avaliadora externa

BRASÍLIA – DF
2025

Código de catalogação na publicação – CIP

P654r Pinheiro, Alexandre Magalhães

A responsabilidade civil por incidentes de segurança na LGPD: uma análise à luz da jurisprudência do Superior Tribunal da Justiça / Alexandre Magalhães Pinheiro. — Brasília: Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa, 2025.

101 f. : il.

Orientadora: Profa. Dra. Laura Schertel Ferreira Mendes
Coorientadora: Profa. Me. Tainá Aguiar Junquilho

Dissertação (Mestrado Profissional em Direito) — Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa – IDP, 2025.

1. Responsabilidade civil. 2. Proteção de dados. 3. Agentes de tratamento. 4. Incidentes de Segurança. I.Título

CDDir 340

Elaborada por Natália Bianca Mascarenhas Puricelli – CRB 1/3439

Este trabalho é dedicado à minha esposa, Mariana, e aos meus filhos, Henrique e Sofia, fontes inesgotáveis de amor.

AGRADECIMENTOS

Agradeço primeiramente a Deus, meu maior guia.

Meu sincero agradecimento à professora Laura Schertel Mendes, uma das maiores especialistas mundiais no tema proteção de dados, grande referência profissional, que muito me honrou como orientadora, pela disponibilidade e disposição para compartilhar tantos valorosos conhecimentos.

À querida professora Tainá Junquilho, minha coorientadora, pela grande contribuição, ainda em sala de aula, para aperfeiçoar meu interesse no direito digital.

Ao professor Guilherme Pinheiro, que primeiro me apresentou conceitos básicos dos mercados digitais como *big data* e neutralidade de rede, basilares ao escopo da pesquisa.

Ao professor Filipe Medon, ícone no estudo da interseção entre o direito civil e as novas tecnologias, pelo rigor na orientação desde a qualificação, essencial a este trabalho.

À professora Karina Fritz, que tenho o prazer de desfrutar da amizade, pelos ensinamentos aprofundados sobre responsabilidade civil, temática que domina como poucos.

Aos colegas de Mestrado e demais professores do IDP, pela amizade e pelos maravilhosos momentos vivenciados nestes últimos dois anos.

À equipe do escritório Uchôa e Magalhães Advogados, minha segunda casa, pelo apoio.

Por fim, à minha família, especialmente a Mariana, o Henrique e a Sofia, o trio que dá sentido à minha vida, pela torcida e compreensão das necessárias ausências.

LISTA DE ABREVIATURAS E SIGLAS

ABREVIATURAS:

Art. por artigo

Arts. por artigos

Ibid. por *ibidem*

Cf. por confira

Obs. por observação

SIGLAS:

ANPD – Autoridade Nacional de Proteção de Dados

AREsp – Agravo em Recurso Especial

CC – Código Civil (Lei nº 10.406/2002)

CDC – Código de Defesa do Consumidor (Lei nº 8.078/1990)

CEDIS-IDP – Centro de Direito, Internet e Sociedade do Instituto Brasiliense de Direito Público

EC – Emenda Constitucional

GDPR – General Data Protection Regulation

IBM – International Business Machines

LAI – Lei de Acesso à Informação (Lei nº 12.527/2011)

LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018)

MCI – Marco Civil da Internet (Lei nº 12.965/2014)

PL – Projeto de Lei

REsp – Recurso Especial

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

TJ – Tribunal de Justiça

TRF – Tribunal Regional Federal

RESUMO

A Lei Geral de Proteção de Dados (LGPD), nº 13.709/2018, atribuiu responsabilidades aos agentes de tratamento (controladores e operadores) no que se refere aos danos causados aos titulares de dados pessoais, notadamente em incidentes de segurança (vazamentos ou uso indevido de informações). A responsabilidade civil é um dos principais temas da judicialização dessa lei no país, em especial nas ações movidas por consumidores que buscam reparação material e moral. Contudo, embora o art. 45 da lei preveja que violações de direitos do titular no âmbito das relações de consumo "se sujeitam às regras de responsabilidade previstas no CDC", em claro indicativo de adoção do regime de responsabilidade civil objetiva, havia grande divergência doutrinária e jurisprudencial acerca da matéria, muitos optando pelo regime subjetivo, mesmo em matéria consumerista. Além disso, as cláusulas gerais de responsabilidade da LGPD (arts. 42 a 44) não indicaram, de forma expressa, a adoção por um ou outro regime (subjetivo ou objetivo). Era necessário, portanto, aguardar a manifestação dos Tribunais Superiores, sobretudo do Superior Tribunal de Justiça. Desde 2023, o STJ tem se posicionado em julgamentos de grande repercussão, específicos sobre esse assunto. Esta pesquisa acadêmica busca, portanto, investigar as premissas iniciais da jurisprudência brasileira, no âmbito do Tribunal, sobre o regime de responsabilidade civil dos agentes de tratamento, em casos concretos de incidentes de segurança de dados pessoais.

Palavras-chave: responsabilidade civil; proteção de dados; agentes de tratamento; incidentes de segurança; Superior Tribunal de Justiça.

ABSTRACT

The General Data Protection Law – LGPD (No. 13.709/2018) assigned responsibilities to data processing agents (controllers and operators) regarding damages caused to personal data holders, especially in security incidents (leaks or misuse of information). Civil liability is one of the main topics of judicialization of this law in the country, especially in lawsuits filed by consumers seeking material and moral compensation. However, although Article 45 of the law provides that violations of the data subject's rights in consumer relations "are subject to the liability rules set forth in the Consumer Protection Code," clearly indicating the adoption of the objective civil liability regime, there was significant divergence in doctrine and case law on the matter, with many opting for the subjective regime, even in consumer matters. Furthermore, the general liability clauses of the LGPD (Articles 42 to 44) did not expressly indicate the adoption of one or the other regime (subjective or objective). Therefore, it was necessary to await the ruling of the Higher Courts, especially the Superior Court of Justice. Since 2023, the Superior Court of Justice has taken a position in high-profile judgments, specifically on this subject. This academic research therefore seeks to investigate the initial premises of Brazilian jurisprudence within the scope of the Court on the regime of civil liability of data processing agents, in specific cases of personal data security incidents.

Keywords: civil liability; data protection; data processing agents; security incidents; Superior Court of Justice.

SUMÁRIO

INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, entrou em vigor em 18 de setembro de 2020 para trazer à ordem jurídica brasileira a disciplina do tratamento[1] e da segurança dos dados pessoais. Nela, há previsão de direitos do titular de dados e de obrigações e responsabilidades dos agentes de tratamento (controladores e operadores de dados[2]), entre as quais a de ressarcimento de danos causados por estes àqueles.

Embora a legislação preveja a obrigação de proteção por entes públicos e privados que tratem dados pessoais, foram as relações privadas (em especial as de consumo) que receberam maior atenção da comunidade jurídica.

O início de vigência da LGPD coincidiu com o primeiro ano de pandemia da covid-19, período em que as relações entre cidadãos e *big techs* foram intensificadas com o isolamento social, favorecendo a atuação de criminosos virtuais, o que tornou as pessoas mais vulneráveis à perda de privacidade no mundo digital. De lá para cá, foram recorrentes os episódios de grandes vazamentos nacionais de dados, com milhões de brasileiros afetados com a exposição de suas informações.

Milhares de ações judiciais passaram a ser propostas por titulares de dados, em sua maioria na qualidade de consumidores, na busca de compensação de danos materiais e morais, em casos envolvendo incidentes de vazamento ou uso indevido de informações pessoais.

Nesse contexto, um dos conteúdos mais relevantes nos debates judiciais que envolvem proteção de dados é o da responsabilidade civil dos agentes de tratamento em incidentes de vazamento[3], especialmente no que se refere ao regime jurídico, se de natureza objetiva ou subjetiva, na medida em são estabelecidos parâmetros para a reparação (ou não) de danos indenizáveis ao titular de dados.

Isso porque, embora o art. 45 da lei preveja que violações de direitos do titular no âmbito das relações de consumo "se sujeitam às regras de responsabilidade previstas no CDC", em claro indicativo de adoção do regime de responsabilidade civil objetiva, houve grande divergência doutrinária e jurisprudenciais nas ações reparatórias consumeristas, ora

---

[1] LGPD, art. 5º: Para os fins desta Lei, considera-se: [...] X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[2] LGPD, art. 5º: [...] IX – agentes de tratamento: o controlador e o operador.

[3] A disciplina da responsabilidade civil tem sofrido grandes alterações dogmáticas e sido desafiada pelas mudanças sociais dos últimos anos, causadas pela exposição aos riscos da sociedade de informação, acidentes de consumo e danos ambientais (Madalena, 2021, p. 251).

responsabilizando os fornecedores, ora considerando os vazamentos “meros aborrecimentos”, não suscetíveis de reparação.

Foi intensa a discussão sobre o grau de vinculação do regime de responsabilidade civil objetiva, previsto no Código de Defesa do Consumidor, aos agentes de tratamento, à luz da Lei Geral de Proteção de Dados, decorrente, dentre outros aspectos, do disposto no citado art. 45 e das redações (e cargas semânticas) quase idênticas entre os artigos 12, § 3º, 14, § 3º, do CDC, e o art. 43 da LGPD, que disciplinam as excludentes de responsabilidade.

Ademais, as cláusulas gerais de responsabilidade da LGPD (arts. 42 a 44) não indicaram, de forma expressa, a adoção por um ou outro regime (subjetivo ou objetivo), acarretando diversas interpretações da doutrina, seja no sentido de que dependeria da verificação de culpa do agente de tratamento (responsabilidade subjetiva), seja no sentido de que se configuraria independentemente de culpa, bastando o nexo de causalidade e a comprovação do dano (responsabilidade objetiva). Mais recentemente surgiram novas linhas doutrinárias que mesclam os dois regimes ou que optam por um tipo especial.

Essa ausência de clareza do regime a ser adotado motivou, portanto, uma miríade de interpretações nas milhares decisões judiciais acerca da matéria. A judicialização da LGPD no Brasil é tamanha que tem motivado pesquisa, desde 2020, do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) e do Portal JusBrasil, e concluído, nos processos em que a lei é o motivo central, serem assuntos predominantes justamente a responsabilização dos agentes de tratamento e o ressarcimento de danos (Mendes; Fujimoto, 2024).

Deste modo, no processo de efetivação do tema responsabilização, era necessário aguardar a manifestação dos Tribunais Superiores, notadamente do Superior Tribunal de Justiça, responsável pela uniformização da jurisprudência em matéria infraconstitucional.

Em março de 2023, a Segunda Turma daquele Tribunal, no julgamento do AREsp nº 2.130.619 – SP, relatado pelo ministro Francisco Falcão, enfrentou o tema em decisão polêmica, abordando a questão dos dados sensíveis e da possibilidade de dano moral em vazamento de dados. O episódio envolvia a relação entre uma consumidora e a concessionária de energia do estado de São Paulo.

Em outubro de 2023 foi a vez da Terceira Turma do STJ se pronunciar sobre responsabilização de agente de tratamento, no julgamento do REsp nº 2.077.278 – SP, de relatoria da ministra Nancy Andrighi. Do mesmo modo, o caso envolveu vazamento de dados, desta vez bancários, em típica relação de consumo. O foco do julgado foi o nexo de causalidade entre a atuação de estelionatários e a instituição financeira.

Em dezembro do mesmo ano, em um novo julgado da Terceira Turma (REsp nº 2.092.096 – SP), igualmente relatado pela ministra Nancy Andrighi, o mote responsabilidade do agente de tratamento voltou à baila, abordando o acesso indevido de terceiros à plataforma virtual de investidores da Bolsa de Valores B3.

Um ano depois, em dezembro de 2024, a Terceira Turma enfrentou novo caso (REsp nº 2.147.374), desta vez sob a relatoria do ministro Ricardo Villas Bôas Cueva, em que se discutiu se a responsabilidade decorrente de atividade ilícita (ataque *hacker)* gera ao agente de tratamento (no caso, a concessionária de energia paulista) o dever de indenizar a vítima. Ali, pela primeira vez, o Tribunal firmou posição sobre a responsabilidade civil dita proativa, no âmbito da LGPD.

Muito recentemente, em fevereiro de 2025, a Terceira Turma tornou a tratar do tema no REsp nº 2.121.904 – SP, mais uma vez com relatoria da ministra Nancy, em disputa envolvendo contrato de seguro de vida, para deixar sedimentada sua visão sobre o regime de responsabilidade diante de vazamento de dados sensíveis.

Foram identificados, ainda, outros julgados do STJ que, embora não tratem a responsabilização sobre a ótica específica da LGPD, geraram posicionamentos importantes que reforçam o debate e ajudam a compreender a visão do Tribunal.

Estariam em formação, portanto, precedentes sobre a responsabilização de agentes de tratamento de dados em incidentes de segurança? Em que medida tais decisões impactam a eventual divergência doutrinária e jurisprudencial sobre o regime de responsabilidade civil na LGPD? Considerando o regime de responsabilização do CDC, qual a relação dessas decisões com o arcabouço de decisões que o Superior Tribunal já produziu em contextos consumeristas semelhantes? (Tamer, 2023)[4].

Apesar de amparados em decisões isoladas, tais questionamentos justificam essa perquirição acadêmica, que busca investigar as primeiras premissas formadoras da jurisprudência brasileira sobre a matéria e delinear seus efeitos, tendo como pano de fundo o papel do Poder Judiciário na interpretação da lei (em seu quinto ano de vigência) e na efetivação do direito fundamental à proteção de dados[5].

---

[4] "A Corte tem entendido que há dano moral *in re ipsa* se há a inscrição indevida em cadastro negativo de crédito, negativa indevida de cobertura pelo plano de saúde e o uso indevido da marca. Em contrapartida, tem afastado o dano presumido nas situações de mero inadimplemento ou descumprimento contratual, simples desconto indevido de valores em conta corrente bancária, a simples omissão de socorro em acidente de trânsito, simples demora da baixa do gravame de alienação fiduciária, atraso de entrega de imóvel ao promitente-comprador".

[5] A Emenda Constitucional nº 115, promulgada em 10 de fevereiro de 2022, acrescentou à Constituição Federal o direito à proteção de dados no rol dos direitos fundamentais, inserindo o inciso LXXIX no art. 5º: é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Convém frisar que os casos analisados nesta pesquisa se centram em relações de natureza consumerista entre o titular de dados e o controlador (consumidor e empresa fornecedora de bens ou serviços). Tal recorte se justifica por se tratar, como se verá, de uma das figuras mais judicializadas e por merecer atenção especial da doutrina. O avanço tecnológico, a defesa do consumidor e a proteção da privacidade não podem andar separados, de modo que a LGPD e o CDC não apenas se encontram, mas se complementam, sendo de consumo a maioria das relações jurídicas que sofrem o impacto da LGPD (Sousa, 2023, p. 114-115).

As metodologias escolhidas para a pesquisa foram a bibliográfica, documental e jurisprudencial, com a análise de casos concretos julgados pelo Superior Tribunal de Justiça e por alguns tribunais estaduais. Foram investigados livros, dissertações, teses, artigos e periódicos, predominantemente nacionais.

Como critério metodológico, os julgados escolhidos para a pesquisa, no caso do STJ, foram todos os encontrados no portal de jurisprudência do Tribunal, e no caso dos tribunais estaduais, para a medida dos primeiros impactos, foram todos os identificados nos Tribunais de Justiça de São Paulo e do Paraná.

No que tange aos objetivos específicos, pretende-se: i) atualizar as posições doutrinárias sobre o regime de responsabilidade civil (objetiva, subjetiva e especiais) dos agentes de tratamento na LGPD em matéria consumerista; ii) analisar sete acórdãos do STJ, proferidos entre 2023 e 2025 (AREsp nº 2.130.619 – SP; REsp nº 2.077.278 – SP; REsp nº 2.092.096 – SP; REsp nº 2.147.374 – SP; REsp nº 2.121.904 –SP; REsp nº 1.995.458 – SP; e AREsp nº 2.311.731 – RS), seus fundamentos, pontos convergentes e divergentes; iii) explicitar qual o grau vinculante dessas decisões, pela hierarquia do sistema de Justiça, aos tribunais estaduais, notadamente o TJ-SP e o TJ-PR.

Os acórdãos pesquisados, embora partam de bases factuais distintas, nos permitem extrair elementos comuns de aspectos necessários à compreensão da matéria responsabilidade civil na Corte, tais como o tipo de dado envolvido (se comum ou sensível), o dever de segurança pelo controlador de dados, a possibilidade de inversão do ônus da prova e as excludentes de responsabilidade.

A dissertação está estruturada em três capítulos.

O primeiro capítulo é destinado aos contornos gerais dos cinco primeiros anos de vigência da Lei Geral de Proteção de Dados (LGPD), com foco nos incidentes de segurança e vazamentos de dados, sua conceituação e exemplificação, e como estes influenciaram a

judicialização dos titulares de dados, com informações da pesquisa IDP-JusBrasil do ano de 2023, divulgada em 2024.

O segundo capítulo é dedicado ao tema responsabilidade civil dos agentes de tratamento (operadores e controladores de dados), sobretudo em observância ao disposto nos arts. 42 a 45 da LGPD. Mais do que apontar diferenciações entre as responsabilidades objetiva e subjetiva (sobejamente estudadas), busca-se atualizar as posições doutrinárias e trazer as novas linhas (especial, mista e ativa). Será aventada ainda, em breves considerações, a abordagem do assunto pelos tribunais estaduais, antes das decisões do STJ.

O terceiro e último capítulo materializa o ponto central, qual seja a LGPD no âmbito do Superior Tribunal de Justiça, em que serão dissecados os sete julgamentos base (AREsp nº 2.130.619 – SP; REsp nº 2.077.278 – SP; REsp nº 2.092.096 – SP; REsp nº 2.147.374 – SP; REsp nº 2.121.904 – SP; REsp nº 1.995.458 – SP; e AREsp nº 2.311.731 – RS), além de outros julgados da Corte relacionados com a temática. É finalizado com indicativos dos primeiros impactos das referidas decisões na jurisprudência de 2º grau dos tribunais estaduais paulista e paranaense.

Na conclusão, expõem-se as ideias enunciadas ao longo de todo o trabalho proposto. Será apresentada, como anexo à dissertação, tabela-resumo com as decisões do STJ citadas.

A pesquisa não se prestará a analisar apenas dispositivos da lei, tampouco repisar os conceitos jurídicos envolvidos. Por se tratar de mestrado profissional, no qual a produção acadêmica deve partir de pressupostos práticos, o fundamental será definir os parâmetros e os efeitos desses julgamentos.

1 INCIDENTES DE SEGURANÇA À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

1.1 Incidentes de segurança: conceito e exemplos

Há mais de uma década, as mais variadas relações humanas, das cotidianas às complexas, de âmbito pessoal, empresarial ou governamental, de natureza social, econômica ou política, estão inseridas, em maior ou menor grau, num contexto digital, hiperconectado e, direta ou indiretamente, movido a dados.

Se a "digitalização" das relações, por um lado, trouxe evidentes benefícios aos cidadãos, como o encurtamento das distâncias, por outro, acarretou graves problemas sociais, como a proliferação das desinformações, as assimetrias informacionais, a atuação enviesada das empresas de tecnologias (*big techs*), a discriminação algorítmica e, o mais comum, a perda de privacidade.

Nesta economia 4.0, os dados se interconectam para gerar informações (Doneda, 2006, p. 136) e se constituem como *commodities* em constante valorização, merecedores de tutela jurídica que proteja não apenas a intimidade no sentido clássico, mas efetive a proteção dos dados pessoais sob o aspecto da autodeterminação informativa[6] (Cueva; Frazão, 2021, p. 34), da escolha livre, racional e informada de cada cidadão, no exercício de um direito fundamental (Doneda, 2011, p. 96).

Essa tutela passa a ser mais relevante diante do fenômeno dos grandes incidentes de vazamentos de dados, que ganharam holofotes globais após o escândalo da *Cambridge Analytica* de 2018, em que informações pessoais de 50 milhões de usuários do Facebook foram manipuladas para influenciar a campanha presencial norte-americana de 2016 (Cadwalladr; Graham-Harrison, 2018), episódio que, inclusive, contribuiu fortemente para pressionar governos mundo afora a elaborarem suas leis protetivas de dados.

No Brasil, não são poucos os casos de incidentes dessa natureza, a exemplo do ocorrido no Ministério da Saúde, em dezembro de 2020, e do identificado pela empresa PSafe, em janeiro de 2021, em que mais de 200 milhões de brasileiros foram afetados com a exposição de suas informações, como nome e CPF (Cambricoli, 2020; Milhões de..., 2021).

[6] Constituída como extensão das liberdades presentes nas leis de segunda geração, tal expressão foi cunhada em 1983 pelo Tribunal Constitucional Federal alemão ("*informationelle selbstestimmung"*), que a consolidou como um direito segundo o qual um indivíduo controla a obtenção, a titularidade, o tratamento e a transmissão de dados relativos à sua pessoa (Doneda, 2011, p. 95, 97)

O fato é que incidentes de segurança envolvendo dados pessoais têm sido cada vez mais frequentes, com danos aparentemente invisíveis e efeitos deletérios ainda não totalmente dimensionados, o que demonstra que as atividades de risco não possuem mais alcance individual, mas coletivo, social, global (Medon, 2022a, p. 330). Tal circunstância justifica o interesse desta pesquisa em conceituar, exemplificar e analisar esses incidentes sob diferentes óticas.

A Lei Geral de Proteção Dados não conceitua "incidente de segurança"[7], embora seu art. 48 estabeleça o dever do controlador de dados[8] de comunicá-lo à Autoridade Nacional de Proteção de Dados (ANPD), com parâmetros informativos dessa comunicação e da análise de sua gravidade.[9]

Tal conceituação coube à própria ANPD, com competência legal para editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade[10], ao publicar a Resolução CD/ANPD nº 15, de 24 de abril de 2024 (Brasil, 2024):

> Regulamento de Comunicação de Incidente de Segurança:
>
> CAPÍTULO II
> DAS DEFINIÇÕES

---

[7] O Regulamento Geral de Proteção de Dados Europeu (nº 2016/679 – GDPR: *General Data Protection Regulation)*, base para a LGPD, por sua vez, traz definição mais ampla de "violação de dados pessoais" entendida como "violação que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conversados ou sujeitos a qualquer outro tipo de tratamento" (União Europeia, 2016, art. 4.0).

[8] LGPD, art. 5º: Para os fins desta Lei, considera-se: [...] VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

[9] LGPD, art. 48: O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de **incidente de segurança** que possa acarretar risco ou dano relevante aos titulares.
§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
I – a descrição da natureza dos dados pessoais afetados;
II – as informações sobre os titulares envolvidos;
III – a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
IV – os riscos relacionados ao incidente;
V – os motivos da demora, no caso de a comunicação não ter sido imediata; e
VI – as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
§ 2º A autoridade nacional verificará a **gravidade do incidente** e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
I – ampla divulgação do fato em meios de comunicação; e
II – medidas para reverter ou mitigar os efeitos do incidente.
§ 3º **No juízo de gravidade do incidente**, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los (grifo nosso).

[10] LGPD, art. 55-JJ: Compete à ANPD: [...] XIII – **editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade**, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; [...] XX – **deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;** (grifo nosso).

> Art. 3º Para efeitos deste Regulamento, são adotadas as seguintes definições:
> [...]
> XII – **incidente de segurança: qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais;** (grifo nosso).

Como o próprio nome sugere (Regulamento de Comunicação de Incidente de Segurança – RCIS), a citada resolução pormenoriza todos os procedimentos a serem adotados nos casos de violações aos dados pessoais dos titulares, incluindo prazos e informações obrigatórias a serem encaminhadas à ANPD (Brasil, 2024, Capítulo III).

Além do propósito de mitigar ou reverter os prejuízos causados, o RCIS contribui com a prevenção, na medida em que promove boas práticas, impõe responsabilizações, exige prestação de contas às vítimas e obriga a manutenção dos registros dos incidentes por cinco anos (Brasil, 2024, Capítulo IV).

Conceituação semelhante pode ser encontrada na *Cartilha de Segurança pela Internet* (Versão 4.0), elaborada pelo Comitê Gestor de Internet no Brasil (CGI.br), composta de dezenas de informações e recomendações aos usuários da rede destinadas ao aumento da segurança e proteção de possíveis ameaças, que, em seu glossário, define incidente de segurança como "qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança de sistemas de computação ou de redes de computadores" (CGI.br, 2012, p. 116).

Dentre os casos mais comuns de incidentes, destacam-se os *scans* (notificações de varreduras em redes), os *worms* (notificações de processos automatizados de atividades maliciosas em redes), os ataques e as invasões a servidores ou páginas, como os *DoS (Denial of Service),* nos quais o tráfego malicioso em excesso torna inoperante o funcionamento do *website* ou servidor[11].

Quaisquer dessas situações pode, na prática, gerar ações administrativas ou judiciais, individuais ou coletivas, ajuizadas pelos afetados.

O tópico é tão significativo que foi o escolhido pelas professoras Ana Frazão e Caitlin Mulholland para o episódio de estreia do PodCast *Direito Digital*, intitulado "Vazamento de Dados", lançado em abril de 2021, em que citam grandes vazamentos ocorridos no início

[11] A Cartilha de Segurança da Internet (Versão 4.0) oferece uma lista pormenorizada dos riscos virtuais (golpes, ataques, códigos maliciosos e outros), com respectivas explicações e orientações preventivas, entre os quais furto de identidade (*identify theft*), fraude de antecipação de recurso (*advance fee fraud*), *phishing*, golpes de comércio eletrônico (site fraudulento, site de compra coletiva, site de leilão), boato (*hoax*), falsificação de e-mail (*e-mail spoofing*), intercepção da tráfego (*sniffing*), força bruta (*brute force*), desfiguração de página (*defacement*), *bot*, *spyware*, *backdoor*, Cavalo de troia (*Trojan*), *rootkit*, riscos em c*ookies*, janelas de *pop-up*, *links* patrocinados, *banners* de propaganda, e outros (CGI.br, 2012, p. 5-45).

daquele ano, com mais atingidos do que a própria população brasileira (224 x 212 milhões de pessoas)[12], já que também incluíam dados de falecidos.

Nesse episódio, as autoras lembram os inúmeros atos ilícitos que podem ser praticados por terceiros em posse dos dados recebidos destes vazamentos[13], tais como abertura de contas bancárias, prática de fraudes, solicitação de serviços, além da utilização por sistemas de inteligência artificial.

Em termos conceituais, merece destaque a diferenciação feita por Caitlin Mulholland, na qual o termo "vazamento" indica uma "conduta omissiva" da base de dados de onde saíram as informações, enquanto "incidente de segurança" é o termo tecnicamente mais correto, ao indicar uma violação a um sistema de segurança da informação, geralmente praticada por *hackers*, vírus, *phishing* (indução de pessoas a acesso de *sites* indevidos), usualmente gerados pelo uso de senhas comuns em *sites* e aplicativos ou da guarda de dados sem criptografia.

Para Ana Frazão, os vazamentos imputam riscos operacionais, reputacionais e legais aos controladores de dados (empresas/governos/instituições), estes últimos decorrentes do regime de responsabilidade civil imposto pela LGPD, objeto de análise adiante.

Vale lembrar que, se o incidente de vazamento ocorrer no contexto de uma relação de consumo, estará relacionado à noção de defeito na prestação de serviço, diante da transposição de previsão do CDC para a LGPD[14] dos dispositivos que abordam o chamado "tratamento irregular", base para a responsabilização do agente de tratamento de dados, como se verá nos próximos capítulos.

[12] Em fevereiro de 2021, a Secretaria Nacional do Consumidor já investigava 40 episódios de vazamentos no Brasil (Frazão; Mulholland, 2021).
[13] Consequência de uma sociedade de vigilância, movida a dados – grandes ativos, cobiçados por criminosos –, em que todos são constantemente monitorados em processos de coleta que comprometem a privacidade e sujeitam as pessoas à manipulação por agentes econômicos e políticos.
[14] Bioni; Dias, 2020, p. 1.

1.2 Incidentes de segurança na judicialização da LGPD no Brasil: 5 anos de vigência

A LGPD entrou em vigor em agosto de 2020. De lá para cá, exerceu o importante papel de conferir efetividade ao direito constitucional à privacidade e à intimidade, ditando rigoroso controle técnico para a governança da segurança das informações e conferindo um novo patamar de proteção aos dados pessoais (Cueva, 2023, p. 99; Frazão; Carvalho; Milanez, 2022, p. 423).

Nesses quase cinco anos de vigência, foram milhares as ações judiciais de titulares de dados envolvendo incidentes de segurança, reflexo da busca pela efetividade desse direito à privacidade, num mercado rico em dados (*data-rich market*) e fruto da máxima na qual o Brasil é um país reconhecido pela excessiva judicialização.

A relevância da judicialização da LGPD é tão grande que motivou um projeto de iniciativa do Centro de Direito e Internet (Cedis) do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), em parceria com o JusBrasil e o Programa de Apoio das Nações Unidas para o Desenvolvimento (Pnud), desde 2020, dedicado a "estudos avançados sobre proteção de dados e direitos fundamentais no Brasil e ao mapeamento de possíveis tendências e posicionamentos nos Tribunais no desenvolvimento de uma cultura de proteção de dados" (Mendes; Fujimoto, 2024, p. 7).

A compilação dos dados do ano de 2023 foi publicada em junho de 2024 com o título *Relatório LGPD nos Tribunais 2023*[15]. O documento destaca, em sua apresentação, o objetivo de colaborar com o debate brasileiro à matéria de proteção de dados pessoais, a partir dos precedentes judiciais, oferecendo à comunidade jurídica e científica um panorama atualizado e inédito dos casos julgados pelo Poder Judiciário[16], o que perfeitamente se encaixa com o propósito da presente pesquisa.

Seu resultado oferece um excelente instrumento para exame sobre a aplicação da LGPD pelo Judiciário brasileiro, seja pelo alcance quantitativo (todas as regiões do país estão contempladas), seja pela profundidade qualitativa, com a sistematização das decisões, inclusive por níveis de relevância[17]. Nas edições segunda e terceira (última), as temáticas

[15] A edição 2025, com dados do ano de 2024, será apresentada no Fórum de Lisboa, em julho de 2025.
[16] Merece registro a elevação do grau de rigor técnico com que sua 3ª edição foi concebida. Com 130 envolvidos (incluídos alunos, professores e pesquisadores do *Privacy Lab* do Cedis-IDP), foram aprimoradas as ferramentas e recursos tecnológicos de busca, coleta, organização e categorização de um banco de mais de 7.500 documentos (decisões judiciais), as de Primeiro Grau coletadas a partir de 40 tribunais e as de Segundo Grau e Tribunais Superiores a partir de 74 Cortes (Mendes, Fujimoto, 2024, p. 8; 15).
[17] Neste último aspecto, os julgados estão divididos quanto ao nível do debate em torno da LGPD (superficial, incidental ou central) e quanto aos temas abordados (*Id., ibid.*, p. 28).

responsabilidade e ressarcimento de danos em incidentes de segurança são uma das mais recorrentes (Mendes; Fujimoto, 2024, p. 29-31, grifo nosso):

> Tanto na primeira quanto na segunda instância o Art. 5º, II, da LGPD (definição de dado pessoal sensível); o art. 7º, X, da LGPD (base legal proteção de crédito); o art. 7º, VI, da LGPD (base legal exercício regular de direitos); o Art. 7°, *caput*, da LGPD (bases legais); **o Art. 42, *caput*, da LGPD (responsabilidade de agentes de tratamento repararem danos)** e o Art. 1º, *caput*, da LGPD (objeto e objetivos da LGPD) possuem significativo destaque. **A alta ocorrência desses dispositivos sinaliza de forma representativa algumas conclusões deste relatório.**
> **[…]**
> **A importância do art. 42 nos casos analisados ficará evidente ao longo do relatório por se tratar de dispositivo relacionado à responsabilização de agentes de tratamento por danos causados em decorrência do tratamento de dados pessoais que viole a legislação**. A menção a este artigo está aliada à **recorrência das ações de reparação de danos nos casos analisados.**

Clarividente, portanto, a relevância prática deste trabalho considerando que a responsabilidade civil nas ações de reparação de danos dos titulares de dados (corte proposto) é, comprovadamente, um dos assuntos mais judicializados no Brasil[18].

Outro aspecto relevante é a separação das decisões pesquisadas por áreas do Direito, incluindo 1º e 2º graus. Direito do Consumidor é a área mais frequente (correspondente a 43% dos casos, a maioria envolvendo reparação de danos – o que também justifica o recorte escolhido), seguido do Direito do Trabalho (36%), Direito Civil (27%), Processo Civil (13%) e Direito Constitucional (9%) (Mendes; Fujimoto, 2024, p. 43; 45)[19].

Os dados do quesito "Incidentes de Segurança" são apresentados em subtítulo específico, iniciado com definições basilares para sua compreensão (Mendes; Fujimoto, 2024, p. 90, grifo nosso):

> analisar a jurisprudência relativa aos incidentes de segurança à luz da LGPD requer compreender que
> **i) nem todo incidente de segurança envolve dados pessoais e se submete ao disposto na legislação;**
> **ii) nem todo incidente de segurança gera danos indenizáveis;**

[18] Além do viés temático, o estudo IDP-JusBrasil 2023-2024 divide, com significativa pormenorização, os casos por setor econômico envolvido (o bancário é o mais demandado) e critério geográfico, este último acrescido dos percentuais de cada tribunal (o Tribunal de Justiça de São Paulo concentra 25% das demandas nacionais). Há, ainda, a subdivisão quanto à menção aos princípios da lei, sendo o da segurança (previsto no art. 6º, VII) o mais citado nos casos que envolvem incidentes de segurança e ações de reparação de danos. O entendimento firmado é de que a falta de adoção de medidas para proteger dados pessoais em conjunto com a ocorrência de vazamento e a utilização indevida de dados e outros tipos de incidente de segurança indicam a violação ao princípio da segurança, especialmente em virtude da falta de zelo dos agentes na proteção dos dados, provocando, em alguns casos, o reconhecimento de falha na prestação de serviços (Mendes; Fujimoto, 2024, p. 31; 33; 63).

[19] Nota: a soma dos percentuais não é 100%, o que se supõe ser erro de digitação de alguma(s) da(s) linha(s).

> iii) além da previsão de um regime de responsabilização pelos incidentes de segurança, a legislação também reconhece os desafios técnicos que permeiam a temática, assim como a importância do aspecto preventivo, concretizado no princípio da segurança.

Nesse cenário, o estudo aponta a dificuldade dos tribunais de identificarem que a exposição dos dados decorreu de um incidente de segurança e a importância da categoria dos dados pessoais impactados (se comuns ou sensíveis), citando a corrente jurisprudencial segundo a qual informações como nome e número de telefone são públicas, obtidas por simples busca na *internet* e muitas vezes divulgadas pelo próprio titular.

Uma das conclusões do Relatório é a de que a judicialização da LGPD no Brasil tende a aumentar nos próximos anos, em decorrência das restrições de admissibilidade de petições administrativas na ANPD, somado ao contexto dos grandes vazamentos de dados ocorridos nos últimos anos, sem a aferição e responsabilização efetiva (Mendes; Fujimoto, 2024, p. 78).

Também necessário o registro do estudo liderado pela IBM, em sua 19ª edição, compilado no *Relatório do Custo das Violações de Dados de 2024* (IBM, 2024), segundo o qual foi de U$ 4,88 milhões o custo médio global envolvendo violação de dados em 2024, o mais alto da história e 10% maior que 2023. Nele, o Brasil ocupa a 16ª posição global, com custo anual, em 2024, de U$ 1,36 milhão, dado que somente reforça a necessidade de estudo da reparação civil dos danos causados por essas violações.

No Brasil, vários órgãos e agentes são responsáveis pelas investigações dos incidentes de vazamento, tais como a Polícia Federal, o Comitê Gestor da Internet no Brasil (CGI.br), o Ministério Público, a Secretaria Nacional do Consumidor (Senacon) – em casos de dados vazados de consumidor – e a própria ANPD[20]. Contudo, a efetividade da proteção dos titulares de dados lesados está condicionada à efetiva responsabilização judicial dos agentes de tratamento.

---

[20] A própria LGPD dispõe sobre a possibilidade de atuação dos órgãos de defesa do consumidor na defesa dos direitos do titular de dados, como se vê no parágrafo 8º do art. 18 e do art. 55-K:
Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...]
§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
§ 8º O direito a que se refere o § 1º deste artigo também poderá ser **exercido perante os organismos de defesa do consumidor** (grifo nosso).
Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, **sobre as competências correlatas de outras entidades ou órgãos da administração pública** (grifo nosso).

2 RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO NA LGPD

2.1 Agentes de tratamento na LGPD: papéis e responsabilidades

Os incidentes de segurança com vazamentos de dados pessoais, embora possam ser causados diretamente por terceiros (ex.: *hackers* criminosos), estranhos à relação entre o titular dos dados pessoais (vítimas afetadas) e o fornecedor do produto ou serviço para qual o titular forneceu seus dados, devem ser analisados sob a ótica das ações (culposas ou dolosas) ou omissões (ausência de medidas de proteção) destes últimos, na medida em que são eles os responsáveis pela guarda e lida desses dados.

Dessa forma, a aplicabilidade de uma lei protetiva dos dados pessoais, como é a LGPD, passa, necessariamente, pelo papel desempenhado por esses agentes responsáveis, designados pela lei como agentes de tratamento[21] e constituídos de dois tipos: o controlador e o operador de dados. O primeiro é a pessoa natural ou jurídica, de direito público ou privado, que toma decisões relacionadas ao tratamento de dados pessoais. O segundo realiza o tratamento sobre instruções do primeiro[22].

Na prática, pessoas, empresas, governos e instituições que manipulam dados pessoais são controladores de dados, ao passo que quaisquer daqueles que agem em nome destes assumem o papel de operadores (exemplo: o contabilista contratado pela empresa, que manipula dados pessoais de seus colaboradores, para a elaboração dos demonstrativos contábeis).

A ANPD disponibiliza o "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado" (Brasil, 2021) que traz, além de conceituação e exemplos do controlador e do operador, as figuras da controladoria conjunta e singular (a primeira, extraída do art. 42, § 1º, II, da LGPD e prevista no art. 26 da GDPR, envolve dois ou mais controladores com interesse comum, num mesmo tratamento, e a segunda ocorrida quando, embora juntos, não possuam finalidades convergentes[23]) e do suboperador (contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador, equiparado àquele em termos de responsabilidade. Ex.: subcontratação de serviço de armazenamento em nuvem[24]).

---

[21] LGPD, art. 5º, IX.
[22] LGPD, art. 39: O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.
[23] Brasil, 2021. p. 12 e 13.
[24] *Id., ibid.*. p. 19 e 20.

Há, ainda, a função de encarregado de dados, indicado pelo controlador[25] para atuar como canal de comunicação entre o próprio controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD), que, embora não seja considerado agente de tratamento pela literalidade do art. 5º, IX, da LGPD, pode ser responsabilizado[26] [27].

Além da guarda e da correta manipulação dos dados pessoais, são muitas as atribuições dos agentes previstas na lei, tais como a manutenção do registro das operações de tratamento (art. 37), a elaboração de relatório de impacto de proteção de dados pessoais (art. 38), a adoção de medidas de segurança, técnicas e administrativas de proteção (art. 46)[28], o dever de notificação em caso de incidente de segurança (art. 48) e a formulação de regras de boas práticas e governança (art. 50). A atuação deles deve ser pautada na boa-fé[29] e na fidelidade a princípios norteadores[30].

---

[25] LGPD, art. 5º: Para os fins desta Lei, considera-se: [...] VIII – encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

LGPD, art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

[26] Como o art. 42 da LGPD – que trata da responsabilidade civil – cita expressamente apenas controlador e operador, a responsabilidade de eventuais danos causados pelo encarregado de dados seria regida por aplicação subsidiária do Código Civil (Ehrhardt Jr., 2022, p. 398).

[27] O Guia Orientativo para Definições dos Agentes de Tratamento da ANPD, por outro lado, indica que, embora tenha atribuições, a responsabilidade pelo tratamento continua sendo do Controlador e do Operador, nos termos do art. 42 da LGPD (Brasil, 2021. p. 22).

[28] 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.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no *caput* deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no *caput* do art. 6º desta Lei.

§ 2º As medidas de que trata o *caput* deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

[29] Victoria Paganella lembra que embora o tratamento de dados possa ser objeto principal de um contrato, na maioria dos casos ele não é o objeto principal da relação, mas acompanha a prestação dos mais variados serviços (bancários, de saúde etc.) e fornecimento de produtos, o que reforça a aplicação dos deveres de proteção decorrentes da boa-fé (Paganella, 2021, p. 225).

[30] LGPD, art. 6º: As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII – segurança: utilização de medidas 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 difusão; VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X – responsabilização e prestação de contas:

Um desses princípios é justamente o da responsabilização e prestação de contas, previsto no inciso X do art. 6º, dirigido aos agentes de tratamento, que dita "a 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".

O fato é: se violam a lei, atuam de forma irregular no exercício dessas atribuições ou causam prejuízos aos titulares de dados, podem sofrer as sanções administrativas previstas no art. 52[31] ou judiciais, por meio da responsabilidade civil – tema tratado aqui – e até criminal, se for o caso.

Na seara administrativa, as violações às diretrizes da LGPD não são suficientemente equacionadas pelos processos administrativos sancionadores, mesmo porque a ANPD, além de suas limitações técnicas, operacionais e financeiras, não se preocupa necessariamente com prejuízos concretos sofridos por indivíduos ou coletividades determinadas, mas, sim, com uma abordagem macro dos direitos à proteção de dados[32]. Assim, sem prejuízo da responsabilidade administrativa, a responsabilidade civil buscada pela via judicial é uma ferramenta eficiente de tutela do direito fundamental à proteção de dados pessoais (Frazão; Carvalho; Milanez, 2022, p. 423)[33].

---

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.

[31] LGPD, art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I – advertência, com indicação de prazo para adoção de medidas corretivas; II – multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III – multa diária, observado o limite total a que se refere o inciso II; IV – publicização da infração após devidamente apurada e confirmada a sua ocorrência; V – bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI – eliminação dos dados pessoais a que se refere a infração; VII – (VETADO); VIII – (VETADO); IX – (VETADO); X – suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI – suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII – proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

[32] Embora a ANPD possa aplicar multas individuais, foi concebida para sancionar violações coletivas de maior repercussão, como se extrai das atribuições previstas no art. 55-J da LGPD: Compete à ANPD: [...] I – elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; IV – fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; V – apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; VI – promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; VII – promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; [...] IX – promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; [...].

[33] Em maio de 2020, antes da vigência da LGPD e da aprovação da PEC nº17/2019, o Supremo Tribunal Federal, em decisão histórica, reconheceu o direito fundamental à proteção de dados, ao referendar medida cautelar nas Ações Diretas de Inconstitucionalidade nºs 6.388, 6.389, 6.390 e 6.393, de relatoria da ministra Rosa Weber, com maioria de 10 votos, suspendendo a aplicação da Medida Provisória nº 954/2018¸ que obrigava as operadoras de telefonia a repassarem ao IBGE dados identificados de seus consumidores de telefonia móvel, celular e endereço.

A Lei Geral de Proteção de Dados dedica capítulo específico para a previsão de normas de responsabilidade desses agentes, intitulado "Da Responsabilidade e do Ressarcimento de Danos", com as seguintes disposições:

> 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.[34]
>
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I – o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
>
> II – os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
>
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
>
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do *caput* deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
>
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.
>
> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I – que não realizaram o tratamento de dados pessoais que lhes é atribuído;

A tônica do julgamento se centrou na importância do tema da proteção de dados à manutenção da democracia em face dos desenvolvimentos tecnológicos. A decisão deu início ao delineamento desse novo direito fundamental, que terá contornos definidos de forma mais precisa, tanto pela jurisprudência, como pela doutrina (Mendes, 2020). Em setembro de 2022, no julgamento da ADI nº 6.649/DF, relatada pelo ministro Gilmar Mendes, que versou sobre a constitucionalidade do Decreto nº 10.046/2019, instituidor do Cadastro Base do Cidadão, o STF reafirmou a importância do direito fundamental à proteção de dados, ao declarar ser plenamente possível o compartilhamento dos dados entre as entidades de administração pública federal, desde que respeitados os parâmetros da LGPD (STF, 2021).

[34] Este dispositivo muito se assemelha com o art. 82 da GDPR: Art. 82. 1 – Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indenização do responsável pelo tratamento ou do subcontratante pelos danos sofridos. 2 – Qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o presente regulamento. O subcontratante é responsável pelos danos causados pelo tratamento apenas se não tiver cumprido as obrigações decorrentes do presente regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento (União Europeia, 2016). Victoria Paganella enfatiza que os dispositivos relacionados à responsabilidade civil na LGPD sofreram forte influência da GDPR (Paganella, 2021, p. 226).

> II – que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III – que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.
>
> 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.
>
> 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.
>
> Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

Antes de se adentrar no tema regime de responsabilização, é pertinente pontuar quatro pontos importantes: o primeiro relacionado à expressão "outrem" no *caput* do art. 42, que indica que as vítimas não são apenas os titulares de dados, mas qualquer pessoa que sofra um dano, inclusive pessoas jurídicas, a exemplo de um ato ilegal causado por um concorrente (Bodin de Moraes, 2019, p. 2).

O segundo se refere à solidariedade existente entre as figuras do controlador e operador, insculpida no inciso I do § 1º do art. 42, no sentido de que este terá responsabilidade solidária quando descumprir obrigações legais ou não tiver seguido as instruções lícitas daquele, bem como a do inciso II, quando houver mais de um controlador, todos igualmente envolvidos no evento danoso, observada a proporcionalidade na contribuição de cada um e a possibilidade do direito de regresso[35] (§ 4º do art. 42).

O terceiro diz respeito ao tipo de dano, dispondo a lei que a reparação pode envolver qualquer tipo (o patrimonial ou moral, o individual ou coletivo[36]), mas sendo omissa quanto à possibilidade da presunção de dano (dano *in re ipsa*), sobretudo nos incidentes de segurança,

[35] Aquele que, não tendo cometido o dano, for responsabilizado por conduta alheia com ressarcimento da vítima, tem direito de regresso contra os demais responsáveis, na medida da sua participação no evento danoso (Ehrhardt Jr., 2022, p. 400).
[36] Merece ênfase o voto detalhado do REsp nº 1.737.412/SE, julgado à unanimidade em 5/2/2019, relatado pela ministra Nancy Andrighi, sobre dano moral coletivo e suas funções punitiva, repressiva e preventiva na relação consumerista. O caso envolvia o tempo de espera na fila e assentos preferenciais de clientes de bancos.

em que, não raras vezes, são muitos os titulares afetados e é difícil sua comprovação[37]. Essa análise, além de estar relacionada ao regime de responsabilidade civil a que os agentes de tratamento estariam submetidos, foi enfrentada pelo STJ, como no AREsp 2.130.619 – SP, que fez clara distinção dos efeitos dessa presunção, se envolver dados comuns ou dados sensíveis, e no REsp nº 2.147.374 – SP, para o qual o vazamento de qualquer tipo de dados é passível de responsabilização.

Por fim, merece registro o fato de que a LGPD, embora preveja e tutele de forma especial os dados sensíveis (art. 5º, II), em matéria de responsabilização, como a própria leitura dos artigos 42 a 45 deixa clara, não os distingue dos dados comuns, de modo que o tratamento indevido de ambos gera o dever de indenizar. Tal constatação é relevante na medida em que, como se verá a seguir, muitas decisões, inclusive do STJ, sugerem que apenas incidentes envolvendo dados sensíveis são passíveis de responsabilização.

[37] A dificuldade de aferição do dano individual pode ser fortalecida com os mecanismos de ação coletiva, previstos no § 3º do art. 42, especialmente pela tradição brasileira de proteger direitos difusos e coletivos por meio da Ação Civil Pública e do Mandado de Segurança Coletivo (Frazão; Carvalho; Milanez, 2022, p. 441).

2.2 Regimes da responsabilidade civil dos agentes de tratamento da LGPD

No ordenamento jurídico brasileiro, a responsabilidade civil tem amparo nos arts. 186, 927 e correlatos do Código Civil, que tratam do dever de indenizar daquele que comete ato ilícito e causa danos a outrem[38]. É conceituada como a "aplicação de medidas que obriguem alguém a reparar dano moral ou patrimonial causado a terceiro em razão de ato do próprio impugnado, de pessoas por quem ele responde, de fato de coisa sob sua guarda ou, ainda, por simples imposição legal" (Diniz, 2019, p. 50).

Em suma, constitui-se em instrumento de reparação dos danos sofridos pelo sujeito, do modo mais completo, na busca, dentro do possível, da avaliação dos prejuízos, da quantificação da indenização e do retorno do *status quo ante* do lesado, fazendo cessar a ofensa e corrigindo o evento danoso (Sanseverino, 2011, p. 39; 48).

Nesse conceito, estão presentes seus quatro elementos caracterizadores: ação comissiva ou omissiva, dano, nexo de causalidade entre a ação e o dano e a culpa. Destes se extraem os eixos para a definição dos dois principais regimes de responsabilidade: a **objetiva**, prevista no parágrafo único do art. 927[39], segundo a qual o causador do dano fica obrigado a repará-lo independentemente de culpa, bastando o nexo de causalidade (teoria do risco), seja por expressa previsão legal, seja pela valoração de que a ação danosa expõe pessoas a riscos ou prejuízos; e a **subjetiva** (culposa), prevista no art. 186, segundo a qual a reparação do dano dependerá da comprovação de culpa[40] do agente.

A responsabilidade objetiva está prevista em legislações específicas como o CDC (arts. 12 a 14), a Lei Anticorrupção e em casos pontuais do CC, como o do art. 931, que trata da responsabilidade de empresas pelos danos causados por produtos postos em circulação.

No âmbito da proteção de dados, a LGPD, inobstante tenha previsto uma cláusula geral de imputação de responsabilidade civil (art. 42), não especificou o regime, o que permitiu a

---

[38] CC, Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

[39] Deste dispositivo pode-se deduzir que o Código Civil recebeu a corrente principiológica da Constituição de 1988 que, pautada na dignidade da pessoa humana, valorizou o ressarcimento da vítima decorrente de um ato ilícito, reforçando o direito de justiça e paz social (Madalena, 2021, p. 257).

[40] Caracterizada pela imperícia (falta de habilidade na ação do agente), negligência (ausência de diligência e prevenção) ou imprudência (com precipitação). Além disso, a culpa recebe da doutrina diversas classificações, tais como culpa *in eligendo* (escolha errada do agente), *in vigilando* (ausência de cuidados e fiscalização do responsável), *in cometendo* (agente não pratica ação positiva ao direito e à boa-fé que se presume), *in custodiendo* (relativo à guarda) e culpa grave (sem atenção e cuidado) (Madalena, 2021, p. 255).

discussão sobre qual seria o aplicado nos casos de violação da lei pelos agentes de tratamento (controladores e operadores de dados) em relação aos titulares afetados.

Essa ausência de clareza do regime a ser adotado permitiu interpretações as mais diversas, que devem ser compreendidas pelas óticas legislativa, doutrinária e jurisprudencial.

Na perspectiva legislativa, o primeiro indicativo interpretativo advém da própria leitura dos supracitados arts. 42 e 45. O art. 42, considerado cláusula geral de responsabilidade, ao deixar clara a possibilidade de reparação de danos patrimonial ou moral, individual ou coletivo, pelos envolvidos nas operações de tratamento que "violem a legislação de proteção de dados" poderia indicar o regime da responsabilidade subjetiva[41] [42]. Já o art. 45, ao dispor que a violação dos direitos do titular no âmbito das relações de consumo está sujeita à regra de responsabilidade do CDC, indicaria uma opção pelo regime de responsabilidade objetiva para casos consumeristas[43] [44] [45] [46] [47].

Um segundo indicativo seria a análise da tramitação legislativa da LGPD no Congresso Nacional. Tanto a primeira versão do anteprojeto, quanto a primeira proposta apresentada no Senado, continham disposições de responsabilidade objetiva ("tratamento de dados como atividade de risco" e "responsabilização independentemente de culpa"). Na segunda versão do anteprojeto, após audiência pública realizada na Câmara dos Deputados, as expressões "independentemente de culpa" e "atividade de risco" foram retiradas do texto final, o que

---

[41] Maria Celina Bodin de Moraes entende que uma suposta adoção do regime subjetivo pelo legislador seria reforçada por três mecanismos: imprescindibilidade da violação da lei por parte do causador, excludente de responsabilidade prevista no inciso II do art. 43 (que autoriza a prova de inexistência de falta – *rectius*, violação à legislação – pelo tratador de dados) e ausência de qualquer menção legislativa à responsabilidade sem culpa (Bodin de Moraes, 2019, p. 3).

[42] No modelo baseado na culpa, a responsabilização pelos danos decorrentes da violação da legislação deve ser vista pelo prisma do "deixar de fazer algo que era esperado" seja no sentido de imprudência (ação precipitada e sem cautela), negligência (deixar de fazer aquilo que sabidamente deveria ter feito, dado causa ao resultado danoso) e imperícia (não saber praticar o ato) (Zanatta, 2022, p. 409).

[43] Embora a responsabilidade objetiva seja a regra no CDC, a responsabilidade subjetiva é trazida em casos excepcionais expressamente previstos, como o dos profissionais liberais, nos termos do art. 14, parágrafo 4º ("§4° - A responsabilidade pessoal dos profissionais liberais será apurada mediante a verificação de culpa.") (Lages, 2020, p. 86).

[44] Ana Frazão, Angelo Prata e Giovanna Milanez sustentam que o próprio art. 45 pode ser visto como um elemento em favor da natureza subjetiva, já que não faria sentido excetuar as relações de consumo se o regime geral da LGPD fosse o objetivo (Frazão; Carvalho; Milanez, 2022, p. 433).

[45] Para Guilherme Martins, embora o art. 45 faça remissão ao CDC como fonte adequada à tutela das relações de consumo que envolvem dados, ele não tem o condão de afastar ou mitigar a cogência da LGPD quanto à tutela de acidentes de consumo que envolvem dados (Martins, 2021, p. 87).

[46] O instituto da responsabilidade civil nas relações de consumo, visto sob a ótica regulatória estatal, não deve se limitar à edição de marcos regulatórios, mas ser constantemente revisitado e compreendido, para estar em compasso com a tutela do usuário do mercado digital (ciberconsumidor), mercado este permeado por nebulosidade, discriminação algorítmica e monopólio de poucas grandes empresas (Martins, 2021, p. 82-84).

[47] Há quem defenda que o regime de responsabilização objetiva não pode ser banalizado e deve ser afastado, nos incidentes de tratamento sempre que os dados envolvidos forem secundários e não centrais, ou, dito de outra forma, sempre que o titular de dados não seja o destinatário final do produto ou serviço envolvido, pela ótica do art. 2º do CDC (Maldonado; Opice Blum, 2022, p. 346).

poderia indicar a opção do legislador pela adoção, na regra geral, do regime subjetivo (Bioni; Dias, 2020, p. 5; 8).

Já o disposto no art. 45, exige a extração de elementos comparativos entre o CDC (mais generalista) e a LGPD (mais específica). A conexão entre as duas legislações é reforçada pelo disposto no art. 64 da LGPD, no qual "os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria [...]", o que configura "diálogo das fontes", lembrado por Claudia Lima Marques (Marques; Martins; Magalhães, 2023, p. 139).

O primeiro dos elementos comparativos é o envolvimento ou não de risco na atividade de tratamento de dados[48] [49] [50] e a segurança esperada pelo titular de dados. O art. 14 do CDC[51] prevê a responsabilidade objetiva do fornecedor, quando as informações sobre a fruição do produto ou serviço forem insuficientes ou inadequadas e causem risco ao consumidor, levando-se em consideração a segurança que este espera. Já o art. 44 da LGPD prevê o chamado "tratamento irregular", caracterizado quando o agente de tratamento viola a legislação, não

[48] Para a LGPD, a teoria do risco integral (independentemente de nexo de causalidade) não se aplica em virtude da previsão das excludentes do art. 43.

[49] Em versões anteriores do PL da LGPD, chegou-se a incluir disposição como sendo a atividade de tratamento de dados como de risco, mas isso foi retirado na tramitação do processo legislativo.

[50] Rafael Zanatta propõe a análise dos riscos a partir de três critérios: avaliação sobre a natureza dos dados envolvidos, sobre a expectativa de segurança esperada e sobre o risco criado pela atividade econômica. Cita dois exemplos: o caso da invasão ao sistema de segurança do STJ em 2021 e um hipotético de um incidente numa modesta clínica médica com informações sobre portadores de HIV. No primeiro, embora seja órgão de cúpula do Judiciário, não envolveu exposição de danos sensíveis, sendo, portanto, de baixo impacto e pouca probabilidade de processos discriminatórios, abusivos ou lesivos; no segundo, o impacto e a expectativa de segurança no mercado de exames laboratoriais sobre doenças estigmatizadas são muito maiores (Zanatta, 2022, p. 420-421).

[51] CDC, 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 (grifo nosso).

adota os melhores esforços para evitar o incidente ou não oferece a segurança que o titular médio espera[52] [53], considerado o modo, os resultados e as técnicas utilizadas[54] [55] [56].

No campo dos incidentes de segurança, quanto à segurança esperada, os exemplos são facilmente identificados: um usuário de *software* desatualizado não pode esperar estar imune a ataques virtuais (Maldonado; Opice Blum, 2022, p. 352), ou um cliente de um pequeno comércio de bairro não deve exigir o mesmo nível de segurança contra vazamentos de uma operação bancária com sigilo (p. 358).

Tal como no CDC, a LGPD exige a comprovação do dano sofrido pelo titular de dados decorrente de "violação à legislação de proteção de dados"[57], conforme previsão do *caput* do art. 42, de modo que os agentes não responderão por toda e qualquer situação que causarem danos, mas somente quando suas condutas não se adequarem ao *standard* estabelecido pelo legislador (Tepedino; Terra; Guedes, 2021, p. 288)[58] [59] [60].

---

[52] Não se trata de qualquer expectativa de segurança, mas das expectativas juridicamente legítimas, a exemplo da criptografia assimétrica de "ponta a ponta" nos aplicativos de mensagens, o que não se exigiria num passado não muito distante, em que esta tecnologia não estava disseminada (Bioni; Dias, 2020, p. 13). Outro caso é o do consumidor que adentra uma loja física e parte da premissa de que seu nome e CPF, solicitados para finalização da compra, sejam protegidos pela empresa, assim como o consumidor que realiza uma compra virtual, informando número de cartão de crédito, endereço e outros dados (Schmitt, 2023, p. 70).

[53] A violação da expectativa de segurança equivale, desse modo, à responsabilidade civil pelo fato do produto ou serviço previstos no CDC.

[54] Já o parágrafo único do art. 44 prevê a responsabilidade civil por ato de terceiro, em que o dano não é causado por ato, e sim por omissão do agente de tratamento, que permitiu uma terceira pessoa se aproveitar da brecha de segurança no tratamento dos dados pessoais. Essa omissão, contudo, deve estar relacionada à adoção das medidas de segurança e padrões técnicos previstos no art. 46 e seu parágrafo único e disciplinados pela ANPD. A esse tipo de tratamento se dá o nome de "indevido" (Nunes, 2023a, p. 30-31).

[55] A irregularidade de tratamento é elemento determinante para a imputação de responsabilidade (Bioni; Dias, 2020, p. 15). Os autores asseveram que a análise não envolve apenas o porte ou o tamanho do agente, mas a atividade de tratamento em si, como por exemplo uma "empresa nascente de tecnologia, com apenas cinco colaboradores, que fornece uma solução de inteligência artificial para automatizar diagnósticos e prognósticos na área de oncologia. Para tanto, é necessário manipular um grande volume de dados sensíveis de pacientes de uma série de hospitais e laboratórios. Tal atividade de tratamento de dados é mais arriscada do que aquela praticada por uma grande rede de supermercados, com mais de quinhentos colaboradores, que não tem sequer um programa de fidelidade dos seus consumidores" (Bioni; Dias, 2020, p. 16).

[56] Na comparação com o CDC, há quem critique a redação do art. 44. Para Rafael Zanatta, o CDC, ao estabelecer o conceito de serviço defeituoso e posteriormente as excludentes de responsabilidade, apresenta um desenho normativo mais consistente que a LGPD, que primeiro define as excludentes no art. 43 para depois elaborar um conceito genérico de tratamento irregular no art. 44 (Zanatta, 2022, p. 414).

[57] Exemplos de violação à legislação são a não eliminação dos dados após o término do tratamento previsto nos arts. 15 e 16 da LGPD e a inobservância dos direitos dos titulares dispostos no art. 18 (Paganella, 2021, p. 212).

[58] A aferição de prejuízos pecuniários (materiais), embora possa ser verificada mais objetivamente, geralmente enfrenta dificuldades de quantificação, especialmente em se tratando de danos concretos sofridos por titulares específicos, sendo de percepção mais facilitada as consequências sofridas por toda uma coletividade (Mulholland, 2018, p. 10).

[59] A técnica legislativa de não responsabilizar todo e qualquer dano decorrente de tratamento, mas apenas os de tratamento irregular assemelha-se à adotada pelo CDC, no sentido de que não são todos os danos causados por produtos ou serviços que ensejam a responsabilização, mas somente os causados por produtos ou serviços defeituosos. Isso porque o CDC não estabelece um sistema de segurança absoluta, mas requer uma segurança dentro dos padrões de expectativa legítima dos consumidores (Benjamin; Marques; Bessa, 2016, p. 180).

[60] A vinculação da responsabilidade civil à violação de um dever específico não significa uma "carta em branco" da lógica "o que não é proibido é permitido" (Nunes, 2023a, p. 34).

Ademais, nos incidentes de segurança, a regra é o pleito indenizatório por dano moral, em decorrência da violação à intimidade do titular. Ocorre que não são quaisquer dados expostos que têm o condão de violar a intimidade do afetado. Isso porque a maior parte dos incidentes expõem apenas nome, número de documento e outros de menor severidade, fato que, por si só, como entendeu o STJ no julgamento do AREsp nº 2.130.619 – SP – que será analisado no próximo capítulo –, não teria o condão de gerar dano moral indenizável (Maldonado; Opice Blum, 2022, p. 356).

Outra questão oportuna na comparação entre o CDC e a LGPD é a do ônus probatório na aferição da responsabilidade. Tal qual o CDC, que em seu art. 6º, VIII, prevê a inversão do ônus probante, a LGPD admite essa possibilidade, pela inteligência do § 2º do art. 43, ainda que não se trate de relação de consumo[61].

A classificação do regime de responsabilidade civil na LGPD também permeia o debate na alçada doutrinária.

Laura Schertel Mendes lembra a intensa vulnerabilidade a que são submetidos os consumidores no âmbito de coleta e tratamento de dados pessoais, seja como "consumidores de vidro" (nos termos de Susane Lace), expostos no mercado de consumo, frágeis diante das estratégias empresariais que influenciam decisões, numa economia de especialização flexível e de tecnologias disruptivas, seja como objeto da "indústria de bancos de dados" (expressão de Daniel Solove) (Mendes, 2021, p. 93; 117).

É esse o sentido para, no campo da responsabilização, a autora defender a aplicação da responsabilidade **objetiva**, na medida em que o abuso das empresas em relação à utilização dos dados pessoais dos consumidores ou suas omissões em instituir sistemas de proteção de privacidade caracterizarem, por si só, danos morais e ensejarem o dever de indenizar (Mendes, 2021, p. 140). Essa omissão na instituição das medidas de proteção (dever de segurança[62]) fundamenta a chamada responsabilidade *ex-ante*, apresentada por Laura Schertel Mendes e citada pela ministra Nancy no julgamento do REsp nº 1.995.458 – SP, que se verá a seguir.

---

[61]A inversão do ônus da prova se justifica ao titular de dados diante da hipossuficiência geralmente a que é submetido numa cultura permeada pela *big data*; e, aos agentes de tratamento, para reforçar a importância dos registros e controles rigorosos das operações envolvendo dados pessoais, de modo a permitir-lhes uma defesa efetiva no processo de responsabilização no que se refere ao nexo de causalidade. Na prática, o nexo de causalidade vem sendo considerado pela doutrina mais como um juízo de imputação jurídica, valorativa, do que uma efetiva demonstração naturalística do caminho percorrido pelos dados no incidente, em que o papel desempenhado pelo agente de tratamento é fundamental (Frazão; Carvalho; Milanez, 2022, p. 442).

[62] Para Ana Frazão, Angelo Prata e Giovanna Milanez, o dever de segurança deve ser proporcional à complexidade do tratamento de dados (porte, risco, finalidade), de modo que os meios de comprovação de sua observância dependem do caso concreto e das expectativas legítimas de segurança, decorrentes da observação das tecnologias difundidas no mercado e acessíveis ao agente de tratamento (Frazão; Carvalho; Milanez, 2022, p. 439).

Danilo Doneda se alia a Laura Schertel Mendes para enfatizar que a obrigação de reparar o dano é ínsita à própria atividade de tratamento de dados, que apresenta risco intrínseco aos titulares (Mendes; Doneda, 2018a, p. 477). A mesma linha é a de Caitlin Mulholland, para quem os danos resultantes da atividade habitualmente desempenhada pelo agente de tratamento, se concretizados, são quantitativamente elevados, pois atingem um número indeterminado de pessoas, e qualitativamente graves, já que violam direitos de natureza personalíssima, fundamentais (Mulholland, 2018, p. 15)[63].

A principal crítica à aplicação da responsabilidade civil puramente objetiva é a de que ela afeta o ambiente de negócios, desestimula a inovação, novas tecnologias e permite uma "indústria de multas da LGPD" [64] [65]. Todavia, a história já demonstrou o contrário: assegurou-se o pleno desenvolvimento tecnológico e industrial, e os custos dos modelos de responsabilização objetivos, em especial nas relações de consumo, foram incorporados pelo mercado sem prejuízo do ressarcimento das vítimas de danos injustos, implementando-se o modelo solidarista de responsabilidade, fundado no cuidado com o lesado, mesmo porque não se pode considerar que interesses ligados à proteção de dados pessoais dos titulares sejam de *status* inferior aos interesses empresariais (Bodin de Moraes, 2018, p. 4).

Já Gustavo Tepedino, Aline Terra e Gisela Sampaio Guedes (2021, p. 286) pregam que a responsabilidade do agente de tratamento (em geral, incluídos os casos de consumo) é de natureza **subjetiva**, já que o legislador criou uma série de deveres de cuidado, não havendo sentido responsabilizá-los, independentemente de culpa, se tiverem cumprido perfeitamente esses deveres[66]. Nessa linha, Bruno Bioni e Daniel Dias (2020) lembram que o estímulo legislativo à capacidade dos agentes de tratamento de se auto-organizarem, com boas práticas,

---

[63] Felipe Medon lembra de que o progresso tecnológico e a nova configuração de absorção de riscos provocaram reflexos na responsabilidade civil, que alterou seu foco da verificação da culpa (identificação do culpado) para a reparação da vítima (verificação do dano), no chamado "Direito de Danos" (Medon, 2022a, p. 332).

[64] Argumenta-se que LGPD tem como pilar o fomento à livre iniciativa e à segurança jurídica, sendo incongruente a excessiva responsabilização dos agentes de tratamento (Maldonado; Opice Blum, 2022, p. 357)

[65] Discute-se, também, o possível efeito gerado, pela LGPD, de empoderamento do titular de dados, assim como ocorreu com o consumidor quando da edição do CDC, na década de 1990. Neste ponto, de fato, a maioria das legislações de proteção de dados, ao estabeleceram direitos subjetivos aos titulares (informação, acesso, retificação etc.) como forma de tornar efetivo o exercício de princípios e possibilitar o controle acerca dos dados, terminou por "empoderá-los". Contudo, esses direitos não são suficientes para garantir proteção de dados efetiva e adequada numa sociedade da informação (Mendes, 2021, p. 46). Esse empoderamento aliado à institucionalização de mecanismos de controle e supervisão sobre o uso dos dados, permite ao cidadão ser protagonista das decisões, em linha com o conceito de autodeterminação informativa, princípio da LGPD (Mendes; Doneda, 2018).

[66] Embora a ilicitude seja constatada pelo cumprimento ou não de tais deveres, há quem defenda a necessidade de diferenciação entre deveres de resultado e deveres de meio (normas de conduta), de modo que, somente para os primeiros, a não consecução do resultado almejado implica presunção de culpa em relação ao inadimplemento (Bioni; Dias, 2020, p. 20). Nessa esteira, Victoria Paganella cita o dever dos agentes de tratamento de manter registros das operações (art. 37, LGPD) e o dever do operador de dados de seguir instruções do controlador (art. 39, LGPD) como exemplos de obrigações de resultado, ao tempo em que o dever do agente de "adotar medidas de segurança" seria obrigação de meio (Paganella, 2021, p. 225).

relatórios de impacto à proteção de dados pessoais e *accountability*, reforçam, ainda que indiretamente, a opção pelo regime subjetivo.

Críticos da teoria subjetiva alertam para as dificuldades probatórias dos danos por parte das vítimas[67], fato agravado pelas vulnerabilidades a que são submetidos os cidadãos num ambiente virtual marcado pela *big data* e por tecnologias disruptivas e enviesadas. Essa corrente questiona a relativização do direito constitucional à proteção de dados[68].

Há o posicionamento de Rafael Dresch, que entende ser **objetiva especial**, centrada na garantia de segurança no sentido de que a LGPD não teria adotado o risco como critério de imputação da responsabilidade civil, mas, sim, o ilícito geral decorrente de um tratamento irregular[69].

Anderson Schreiber, por sua vez, classifica a responsabilidade do agente de tratamento como **mista**, fruto da dualidade entre os dois regimes, subjetivo e objetivo. Para ele, o tratamento irregular de dados por fornecimento de segurança inferior à esperada pelo titular seria uma previsão de responsabilidade objetiva, em virtude da aproximação com o CDC, enquanto o tratamento irregular por inobservância da legislação ou a não adoção de medidas específicas do art. 46, seria regra da responsabilidade subjetiva (Schreiber, 2021, p. 336)[70].

Maria Celina Bodin de Moraes, não convencida da existência de um terceiro tipo de responsabilização, opta por enquadrá-la como **ativa (ou proativa),** focada na demonstração da efetividade das medidas de segurança adotadas pelo agente de tratamento para evitar os incidentes de segurança. Isso porque, para ela, o legislador pretendeu não apenas determinar o ressarcimento dos danos eventualmente causados, mas, principalmente, prevenir e evitar a ocorrência destes danos. Não descumprir a lei não seria suficiente, exigindo-se uma postura proativa de prevenção (Bodin de Moraes, 2019, p. 2)[71].

---

[67] Esse calvário não se resolveria com a possibilidade de inversão do ônus probatório em seu favor (previsto no art. 42 § 2º da LGPD) já que a regra continuaria sendo a exigência da prova do descumprimento por parte do tratador dos dados e a exceção, mediante decisão fundamentada e após a instauração judicial da demanda, a sua inversão (Bodin de Moraes, 2018, p. 3).

[68] Rafael Zanatta lembra que as atuais assimetrias informacionais, massificação social e declínio do individualismo devem justificar uma "coletivização da responsabilidade civil", tudo para que não se negligencie direitos e valores fundamentais eleitos pela Constituição Federal, especialmente em se tratando de alto risco (Zanatta, 2022, p 418).

[69] Defende uma coerência sistemática entre o CDC, segundo o qual o dever geral de segurança está fundado no defeito, e o art. 44 da LGPD, sustentado na quebra da legítima expectativa quanto à segurança dos processos de tratamento de dados (Dresch, 2020, p. 11).

[70] O regime dual de responsabilidade civil também pode ser classificado com foco na conduta do agente (tratamento irregular, por sua vez dividido em ilícito – art. 42, *caput* – e indevido – art. 44, parágrafo único c/c art. 46, *caput* e § 1º da LGPD) ou na tutela do titular, que torna útil a enumeração dos diferentes requisitos exigidos para determinação do dever de indenizar (Nunes, 2023a, p. 29).

[71] Fruto dos riscos da sociedade contemporânea, a função preventiva da responsabilidade civil passa a ser tão importante quanto a função compensatória (Rosenvald, 2017, p. 28). Felipe Medon reforça a importância da precaução, na medida em que a responsabilidade não tem conseguido cumprir a função reparatória, seja pela gravidade e irreversibilidade dos danos, seja pela dificuldade de identificação dos causadores ou ausência de meios

Existem, ainda, os defensores da **coexistência de mais de um regime**, ao fundamento de que os riscos inerentes aos tratamentos podem ser muito distintos. É o caso de Ana Frazão, Ângelo Prata e Giovanna Milanez, que sugerem a aplicação da responsabilidade subjetiva para os casos de menor risco e da objetiva para os casos que ultrapassem riscos ordinários[72].

Impreterível, ainda, é o destaque às situações em que, mesmo diante da ocorrência de um incidente de vazamento, os agentes de tratamento não são responsabilizados. São as excludentes de responsabilidade da LGPD, estatuídas no art. 43, segundo o qual esses agentes de tratamento não serão responsabilizados quando provarem: I – que não realizaram o tratamento de dados pessoais que lhes é atribuído; II – que, embora tenham realizado o tratamento que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III – que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro[73].

A primeira hipótese carrega obviedade, a exemplo do titular que busca a reparação do controlador errado[74] [75], e se vincula ao dever de registro das operações de tratamento[76]. A segunda traz o afastamento da ilicitude, como é o caso de uma decisão automatizada de um banco, baseada em critérios transparentes e sem viés, que nega um empréstimo a alguém (Dresch; Melo, 2022, p. 401). Para alguns doutrinadores, essa previsão confirmaria a tese de

---

financeiros destes para custear a compensação, o que impõe mecanismos de coletivização e socialização de riscos, a exemplo dos seguros obrigatórios (Medon, 2022a, p. 339-341).

[72] Na mesma linha, os autores apontam a necessidade de um regime de responsabilidade mais rigoroso aos agentes que têm no tratamento de dados seu negócio principal, do que àqueles que usam dados apenas como subsídios. Ou seja: o regime de responsabilidade objetiva pode parecer adequado para *big techs* ou grandes agentes, mas excessivamente oneroso para pequenos agentes econômicos que tratam dados de forma acessória às suas atividades (Frazão; Carvalho; Milanez, 2022, p. 436).

[73] As disposições legais dos arts. 12 e 14, § 3º, do CDC, e 43 da LGPD são quase idênticas:

CDC. Art. 12. [...] § 3° O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar:
I – que não colocou o produto no mercado;
II – que, embora haja colocado o produto no mercado, o defeito inexiste;
III – a culpa exclusiva do consumidor ou de terceiro.
Art. 14. [...] § 3° O fornecedor de serviços só não será responsabilizado quando provar:
I – que, tendo prestado o serviço, o defeito inexiste;
II – a culpa exclusiva do consumidor ou de terceiro.
LGPD. Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
I – que não realizaram o tratamento de dados pessoais que lhes é atribuído;
II – que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
III – que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro (grifo nosso).

[74] Desse dispositivo se extrai a presunção legal de autoria do tratamento por parte do agente a quem o tratamento é atribuído (Bioni; Dias, 2020, p. 19).

[75] Ana Luisa Tarter Nunes registra que essa excludente não pode ser utilizada como argumento pelo agente de tratamento que realiza tratamento indevido, ou seja, sem a adoção das medidas de segurança previstas no art. 46 (*caput* e § 1º) da LGPD. Cita, como exemplo, um ataque *hacker*, que é causado por terceiro, caso em que o agente, se não provar que adotou as referidas medidas, responderá pela conduta omissiva, isentando-se a vítima de identificar o terceiro (*hacker*) (Nunes, 2023a, p. 32).

[76] Pelo agente de tratamento, nos termos do art. 37 da lei (Dresch; Melo, 2022, p. 401).

que o regime geral adotado pela lei seria o da responsabilidade subjetiva (Bioni; Dias, 2020, p. 7), inclusive presumida (pelo uso da redação em sentido negativo: "os agentes de tratamento só não serão responsabilizados"), e afastada, numa interpretação conjunta com o disposto no art. 44, se o agente demonstrar que adotou as providências de segurança adequadas, possíveis e viáveis, no contexto do tratamento de dados.

A terceira afasta o nexo causal, nos casos de culpa exclusiva da vítima[77] ou de terceiro, excludentes clássicas da responsabilidade civil. Exemplo interessante é se o ataque *hacker* é considerado culpa de terceiro. O art. 46 da LGPD exige "adoção das medidas de segurança". Todavia, nenhum sistema é a prova de vulnerabilidade, até porque as tecnologias de invasão evoluem muito rapidamente. Logo, em se comprovando que o ataque foi muito sofisticado e que o controlador adotou medidas eficientes, poderia se admitir a excludente (Maldonado; Opice Blum, 2022, p. 358; Dresch; Melo, 2022, p. 402). O assunto foi abordado pelo STJ no julgamento do REsp nº 2.147.374 – SP, como se verá no próximo capítulo.

A invocação em juízo da LGPD, por ser uma lei abrangente, deve se dar ao lado de outros dispositivos normativos, como os citados Código de Defesa do Consumidor e Marco Civil da Internet[78], e de outros que, em breve, poderão entrar em vigor, como é o caso da Lei de Inteligência Artificial[79] (PL nº 2.338/2023), em tramitação no Congresso[80]. Essas normas

[77] Nos embates envolvendo incidentes de vazamento, geralmente os fornecedores evocam esse artigo para imputar culpa exclusiva do consumidor, que teria negligenciado no cuidado com seus dados (Schmitt, 2023, p. 71). A excludente se aplica aos casos em que a causa para a ocorrência do evento danoso somente pode ser imputável à vítima, a exemplo do titular de dados que disponibiliza seus dados a *site* reconhecidamente não confiável (Dresch, Melo, 2022, p. 402).

[78] MCI – Lei nº 12.965/2014. Antes da vigência da LGPD, constituía-se como o principal arcabouço legislativo de proteção dos dados pessoais, restringindo-se, contudo, como o próprio nome sugere, à relação dos usuários com provedores de conexão e aplicação na internet. O diploma prevê, expressamente, direitos ao usuário relacionados à privacidade e proteção de dados pessoais (arts. 3º, II e III; 7º, 8º e 11) e responsabilidade dos agentes (art. 3º, VI), eximindo, todavia, o provedor de conexão quanto aos danos decorrentes de conteúdo gerado por terceiros (art. 18), exceto nos casos em que, após ordem judicial específica, não tome providências para tornar indisponível o conteúdo apontado como infringente (art. 19). Foi utilizado como fundamento de algumas decisões do STJ, como os Recursos Especiais nºs 1.914.596-RJ e 2.092.096 – SP, analisados nesta pesquisa.

[79] Sobre a responsabilidade civil no campo da inteligência artificial (IA), cirúrgicos são os estudos de Felipe Medon segundo os quais, diante da limitação das legislações em se atribuir personalidade jurídica às máquinas, o caminho deva ser o da responsabilidade baseada no risco (objetiva), já que a subjetiva seria de difícil conjugação com a plena reparação das vítimas, seja pelas dificuldades de identificação do resultado danoso nas técnicas de *machine learning*, seja pela possibilidade de inúmeros sujeitos terem contribuído para a programação (incerteza das contribuições individuais). Ressalta, ainda, que a classificação dos danos causados por robôs como meros defeitos imputáveis aos fabricantes (concepção consumerista), deve ser repensada diante da crescente autonomia das IAs, amplificando os dilemas da responsabilidade civil. Para ele, tais dilemas podem ser enfrentados com a solidariedade, a coletivização e o gerenciamento de riscos, tudo para que a simples aplicação de um regime objetivo não iniba o desenvolvimento tecnológico (Medon, 2020b, p. 346-351).

[80] De autoria do Senador Rodrigo Pacheco, dispõe sobre "o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana" e foi aprovada no plenário do Senado Federal e remetido à Câmara dos Deputados em março de 2025, onde aguarda designação de Relator para Comissão Especial. Traz em seu texto a proteção de dados como princípio ("Art. 2º – O desenvolvimento, a implementação e o uso de sistema de IA no Brasil têm como fundamentos: [...] IX – privacidade, proteção de dados pessoais e autodeterminação informativa) e cita, em diversos dispositivos (art. 5º, II, art. 13, § 2º, art. 22, I, art. 30, IV, art.

não existem isoladamente, mas coexistem num mesmo ambiente normativo, o que exige interpretação sistemática (Cueva, 2023, p. 97).

44, art. 49, IX) direitos elencados na LGPD. Indica, ainda, capítulo específico para a responsabilidade civil de agentes no uso da IA (arts. 35 a 39). Tramitação e inteiro teor disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262. Acesso em: maio 2025.

2.3 Responsabilidade civil dos agentes de tratamento: breves considerações sobre a jurisprudência dos tribunais estaduais

A presente pesquisa complementa a realizada em 2022, no IDP, intitulada *Responsabilidade Civil dos Agentes de Tratamento à Luz da Lei Geral de Proteção de Dados – Análise Jurisprudencial dos Tribunais Estaduais* (Landim Neto, 2022), resultado do Mestrado Profissional de José Emiliano Paes Landim Neto.

Aquele trabalho analisou julgados de casos consumeristas compreendidos entre 2019 e 2022, dos tribunais de Justiça de Alagoas, Acre, Amapá, Bahia, Distrito Federal, Minas Gerais, Paraíba, Rio de Janeiro, Rio Grande do Sul e São Paulo, que, ora decidiram pela responsabilidade objetiva (dano não configurado), ora pela subjetiva.

Concluiu que "as decisões judiciais não possuem consenso acerca da responsabilidade civil dos agentes de tratamento" e "o Judiciário ainda não chegou a uma uniformidade, nem está atendido tecnicamente para fins de verificar todas as violações alegadas pelo titular à luz da LGPD".

Não houve, contudo, naquela dissertação, qualquer menção às decisões do STJ, mesmo porque estas somente ocorreram no ano de 2023. Consequentemente, não analisou em que medida as decisões dos tribunais estaduais foram afetadas após os pronunciamentos superiores.

A ausência de uniformidade jurisprudencial em âmbito estadual também foi citada no estudo IDP-JusBrasil 2023-2024, ao elencar os questionamentos frequentes nas demandas que envolvem o tema responsabilidade civil: "1) a eventual configuração de dano moral pelo mero vazamento de dados (dano moral *in re ipsa*); 2) se o mero vazamento configura violação dos direitos da personalidade; e 3) o dano moral por negligência no atendimento às reclamações dos titulares" (Mendes; Fujimoto, 2024, p. 47, grifo nosso):

> percebeu-se que as dificuldades dos titulares em comprovar a existência e a extensão do vazamento de dados pessoais têm trazido maior espectro de complexidade para os julgadores. Muitas das ações que discutem fraude e vazamento de dados à luz da LGPD também endereçam questões de dano moral, e, até este terceiro ano do painel, ainda **não foi possível identificar um consenso jurisprudencial sobre o tema**.

O referido estudo traz um dado interessante. Nele, houve a metrificação dos casos pesquisados pelos artigos da LGPD, utilizados pelos litigantes como fundamento das ações. O que intriga é: embora responsabilização e ressarcimento de danos em incidentes de segurança seja um dos temas mais recorrentes, o art. 42, *caput*, da lei – que trata particularmente sobre a

responsabilidade e o ressarcimento de danos – aparece apenas em 11º lugar no rol dos mais utilizados, correspondendo a apenas 5% dos casos (Mendes; Fujimoto, 2024, p. 27)[81].

Há, dessa forma, nítida discrepância entre os pedidos de responsabilização dos agentes de tratamento e os artigos de lei utilizados para embasar esses pedidos, o que pode denotar um aspecto da judicialização brasileira da LGPD no âmbito de tribunais estaduais: os titulares de dados não estão fundamentando corretamente suas ações reparatórias.

O mesmo ocorre com as excludentes de responsabilidade, comumente evocadas nas demandas judiciais. Sobre ela, o relatório lembra da alegação corriqueira dos agentes de tratamento de que os danos sofridos pelos titulares de dados foram gerados por culpa exclusiva de terceiro, mormente nos casos de golpes e fraudes no setor financeiro e de telecomunicações, cujas decisões não indicam o art. 43, III, da LGPD – que trata justamente dessa excludente –, e, sim, o art. 14, § 3°, I, do CDC. Já no segundo grau, o art. 43, III, é citado com mais frequência, embora seja mais comum a menção concomitante de ambos os artigos (Mendes; Fujimoto, 2024, p. 47).

Nessa instância de Justiça, o estudo não identificou posição clara sobre se o regime previsto na LGPD é de responsabilidade civil objetiva ou subjetiva**,** em que pese tenha sido possível deduzir a utilização recorrente do CDC para responsabilizar objetivamente o agente de tratamento-fornecedor causador de dano ao titular de dados-consumidor[82]. Constatou-se, ainda, que mesmo nos posicionamentos judiciais que optam por um regime, a aplicação dos artigos do CDC se sobrepõe à dos da LGPD (Mendes; Fujimoto, 2024, p. 47-49).

Tais ponderações podem indicar duas faces do retrato atual da judicialização da LGPD no país[83]: i) a não utilização correta dos artigos da Lei Geral de Proteção de Dados para o

---

[81] Os artigos mais utilizados são os seguintes: art. 5º, II (que define dado sensível) que representa 19% dos casos; art. 7º, X (que trata sobre tratamento para proteção ao crédito), 17%; art. 5º, I (que define dado pessoal), 15%; art. 7º, VI (que trata sobre tratamento para o exercício regular de direitos), 10%; e art. 20, *caput* (que aborda o direito do titular de revisar decisões com base em tratamento automatizado de dados), 8%. Mesmo quando se considera apenas as decisões em níveis 4 e 5 (LGPD como debate incidental ou central), ainda assim a menção aos arts. 42 a 45 do Capítulo VI da lei (relacionados à responsabilidade e ressarcimento de danos) ocupa apenas o terceiro lugar (com 14% dos casos), sendo em primeiro (57%) os arts. 1º ao 6º do Capítulo I (Disposições Preliminares) e em segundo (54%) os arts. 7º ao 10 do Capítulo II (Tratamento de Dados) (Mendes; Fujimoto, 2024, p. 95). Nota: a soma dos percentuais não é 100%, o que se supõe ser erro de digitação de alguma(s) da(s) linha(s).

[82] Outra constatação foi a forte tendência da vinculação da ocorrência de danos morais com o tipo de dado envolvido no incidente, se comum ou sensível (Mendes; Fujimoto, 2024, p. 103), foco do julgamento do AREsp nº 2.130.619 – SP, discutido no terceiro capítulo.

[83] Não menos relevante é a tabulação das decisões que o estudo traz quanto à qualificação do dano indenizável, com preponderância do dano moral em relação ao dano patrimonial: "em termos quantitativos, observa-se que, entre as decisões judiciais de **níveis 4 e 5, há mais julgados que cuidaram da qualificação do dano moral do que decisões que versaram sobre danos patrimoniais** advindos do tratamento de dados. Porém, é em **termos qualitativos que esse protagonismo do dano moral se coloca em maior evidência**". Nessa qualificação, ganha destaque a classificação do dado pessoal entre comuns (não sensíveis) e **sensíveis**, na medida em que estes têm exercido, na grande maioria das decisões estudadas, dupla função: "(i) elemento de qualificação do dano

embasamento das demandas judiciais de reparação civil, substituídos pelos equivalentes do Código de Defesa do Consumidor; e ii) a indefinição do regime de responsabilidade civil da LGPD (se objetiva ou subjetiva) pela jurisprudência de 1ª e 2ª instâncias, que, igualmente, ainda utilizam o CDC para basear suas fundamentações[84].

No plano dos incidentes de segurança, alguns temas foram sobejamente julgados pelos tribunais estaduais, até serem enfrentados pela Corte Superior de Justiça. É o caso do chamado "golpe do motoboy" que, antes de ser objeto do REsp nº 1.995.458 – SP (analisado adiante), foi debatido por vários tribunais, como o TJ-RS, como se vê:

> APELAÇÃO CÍVEL. CARTÃO DE CRÉDITO. GOLPE DO MOTOBOY. DESCONSTITUIÇÃO DO DÉBITO. INDENIZAÇÃO POR DANO MORAL. FURTO. FRAUDE. 1 – FALHA NA PRESTAÇÃO DO SERVIÇO CONFIGURADA. 1.1 – A utilização de cartões de crédito e, até mesmo, de débito, exige cautela, tanto por parte do usuário como do seu fornecedor. Este precisa conferir ao cliente todas as garantias possíveis de serem aplicadas, ainda que isso onere a sua prestação, no intuito de que a segurança das relações estabelecidas por meio do uso do plástico sejam válidas e, efetivamente, realizadas por quem possua poder a tanto. Ademais, o banco confere e transmite relação de confiança para com o consumidor – relação fiduciária, fazendo-o crer que será o guardião de sua conta e da relação estabelecida entre instituição/correntista. 1.2 – Obviamente, quando o consumidor recebe telefonema, informando dados pessoais e apresentando verossimilhança de que o cartão foi clonado, acredita que a instituição financeira está, justamente, neutralizando a operação ilícita ou sendo competente na função que prometeu. Principalmente quando pede para cortar o cartão ao meio. 1.3 – Verifica-se, outrossim, **que não foram acionadas as medidas de segurança para abortar transações que destoavam do uso regular pelo titular, tampouco para barrar compras que ultrapassavam o limite de crédito concedido**. 1.4 – Assim, **há falha na prestação do serviço quando o fornecedor não imprime a segurança necessária a fim de impedir que terceiro, utilize informações sigilosas do cliente e efetue compras fraudulentas de forma indiscriminada em nome de titular de cartão de crédito**. 2 – DANOS MORAIS 2.1 – Danos morais configurados no périplo percorrido pela parte autora, junto às rés, na busca de reconhecimento da fraude realizada com o seu cartão de crédito furtado, sem obtenção de êxito. 2.2 – Todas as providências administrativas efetuadas pela parte autora foram consideradas insuficientes pelos demandados, que deixaram de reconhecer amigavelmente a falha na prestação de serviço e restituir à parte ao status quo ante, persistindo na imputação de débito à esfera jurídica do autora, razão pela qual está configurado o dano extrapatrimonial. APELAÇÃO PROVIDA. (TJ-RS – AC: 50553661320198210001 PORTO ALEGRE, Relator: Ana Paula Dalbosco, Data de Julgamento: 28/7/2020, Vigésima Terceira Câmara Cível, Data de Publicação: 31/7/2020) (grifo nosso).

extrapatrimonial e (ii) elemento determinante para considerar o dano moral *in re ipsa* – dispensando prova de "abalo moral" (Mendes; Fujimoto, 2024, p. 97; 99, grifo nosso).

[84] Pode parecer lógica a utilização/menção a artigos do CDC, vez que a própria LGPD faz referência expressa ao diploma consumerista (art. 45). A questão que se impõe é a de que, sendo a LGPD uma lei específica, deveria, em regra, tratando do mesmo tema (responsabilidade civil), se sobressair em relação à lei geral (Código de Defesa do Consumidor), diante da aplicação de casos envolvendo dados pessoais.

A conclusão a que o tribunal gaúcho chegou foi a mesma alcançada pela Terceira Turma do STJ naquele julgamento, no sentido de que há falha na prestação do serviço de instituição financeira que não age com dever de segurança para impedir transações que destoam do perfil do consumidor, como se observará.

Outro exemplo é o do golpe do boleto, praticado por estelionatários contra clientes bancários, em posse de seus dados vazados. Objeto de muitas ações judiciais Brasil afora, um mês antes de ser examinado pelo STJ em 3/10/2023 (REsp nº 2.077.278 – SP), foi analisado pelo Tribunal de Justiça do Paraná, em julgamento assim ementado:

> Apelação cível. Ação de busca e apreensão. Crédito direto ao consumidor com alienação fiduciária em garantia. Sentença de procedência do pedido principal e parcial procedência do pedido contraposto. Recurso da instituição financeira. Tese de violação ao princípio da dialeticidade alegada em contrarrazões afastada. Dano moral configurado. Cometimento de fraude por terceiro, que detinha informações pessoais da consumidora, do contrato, das parcelas em atraso e do escritório de advocacia que ajuizou a ação de busca e apreensão. **Pagamento de boleto falso. Fraude cometida por culpa da instituição financeira pela omissão**. **Responsabilidade do fornecedor pela proteção de dados pessoais do consumidor que atrai o dever de indenizar. Art. 42, da Lei Geral de Proteção de Dados.** Precedentes. Pedido de redução do "*quantum*" indenizatório. Impossibilidade. Peculiaridades do caso que justificam o valor indenizatório fixado na origem. Insurgência quanto aos danos materiais. Pleito de afastamento da condenação à restituição das parcelas pagas em atraso pela consumidora. Impossibilidade. Credor que optou pela execução da garantia por meio do procedimento previsto no decreto-lei 911/69. Retenção dos pagamentos posteriores ao ajuizamento da ação que se mostra incompatível com a via eleita. Restituição devida, sob pena de enriquecimento ilícito. Honorários recursais. Enunciado administrativo nº 7 do superior tribunal de justiça e art. 85, §11, do código de processo civil. Recurso desprovido. (TJ-PR, Ap. Cível 0009331-38.2022.8.16.0026, 2ª Cãmara Cível, Relator: Desembargador Rogério Luis Nielsen Kanayama, Julg: 01/09/2023) (grifo nosso).

De igual modo, a Corte paranaense decidiu na esteira do que o Superior Tribunal de Justiça dali a um mês decidiria, pela responsabilidade objetiva do banco, como será detalhado adiante.

Assunto também recorrente nas 1ª e 2ª instâncias é a responsabilização por dano moral coletivo *in re ipsa*, em incidentes de segurança que geram altíssimas condenações, como é caso das Ações Civis Públicas nºs 5064103-55.2019.8.13.0024 e 5127283-45.2019.8.13.0024[85],

[85] Atualmente em fase de julgamento de apelação. As decisões estão disponíveis em: https://pje.tjmg.jus.br/pje/login.seam;jsessionid=i8G1SzSwDJ0faDRpwpe6UcKX52hnuolyDIDE4w05.pje1g-poapp36.intra.tjmg.gov.br?loginComCertificado=false&cid=815849 e https://pje.tjmg.jus.br/pje/Processo/ConsultaProcesso/Detalhe/listProcessoCompletoAdvogado.seam?id=264784

propostas pelo Instituto Defesa Coletiva, que tramitaram na 29ª Vara Cível de Belo Horizonte-MG e condenaram a Meta a pagar R$ 20 milhões em danos morais coletivos, em caso envolvendo vazamento de informações de usuários do *Facebook, Messenger* e *Whatsapp.*

No mesmo sentido foi a Ação Civil Pública nº 5028572-20.2022.4.03.6100, que tramitou na 1ª Vara Cível Federal de São Paulo e condenou a Caixa, a Dataprev e a própria ANPD a pagarem R$ 40 milhões a título de danos morais coletivos, envolvendo beneficiários do programa Auxílio Brasil (TRF 3, 2023). Como se verá a seguir, o dano moral *in re ipsa* não foi acolhido pelo STJ no julgamento do AREsp nº 2.130.619 – SP, mas o foi em outros julgamentos como o do REsp nº 2.121.904 – SP.

8&ca=c1c0bc4ce16b93212c36dbe028359f898519a4d68b706870ac0f700d6d2a6a1c3bf83fba56b0bb69e7f93a5c9221566a554eb10e1f13c0b4&aba=. Acesso em: abr. 2025.

3 RESPONSABILIDADE CIVIL POR INCIDENTES DE SEGURANÇA NA LGPD À LUZ DO SUPERIOR TRIBUNAL DE JUSTIÇA

Necessária uma digressão histórica da apreciação do tema "proteção de dados" pelo Tribunal. O ministro Ricardo Vilas Bôas Cueva assevera que, na década de 1990, os julgados que interpretavam a incidência do art. 43 do Código de Defesa do Consumidor[86] aos cadastros negativos de crédito permitiram um aperfeiçoamento do conceito de privacidade, de mera exclusão de terceiros para a autodeterminação informativa, tal como reconhecido no ordenamento alemão.

Aqui, merece destaque o REsp nº 22.337-9 – RS[87], julgado em fevereiro de 1995, pela Quarta Turma, relatado pelo ministro Ruy Rosado de Aguiar, que abordou caso envolvendo bancos de dados de proteção ao crédito. Ali, pela primeira vez, o Tribunal enfrentou a questão da vulnerabilidade e dos riscos ao indivíduo, decorrentes da atividade de processamento de dados. Segundo o relator, o processamento ilícito poderia causar "devassa de atos pessoais" ou servir de "instrumento de perseguição política ou opressão econômica", sendo necessário um conceito de privacidade que permitisse ao cidadão o controle de seus dados.

Nesse breve histórico, não menos importantes são os Recursos Especiais de nº 306.570 – SP[88], de 2001, relatado pela ministra Eliana Calmon, segundo a qual "o titular de conta bancária tem direito à privacidade em relação a seus dados pessoais", pelo que negou pedido de requisição de seu endereço ao Banco Central, independentemente de não estar acobertado pelo sigilo bancário, e o de nº 1.168.547/RJ[89], mais recente, de 2010, relatado pelo ministro

---

[86] CDC, art. 43: O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

[87] Ementa: SERVIÇO DE PROTEÇÃO AO CRÉDITO. Cancelamento do registro. Prazo (cinco anos). O registro de dados pessoais no SPC deve ser cancelado após cinco anos. Art. 43, § 1º, do Código de Defesa do Consumidor (Lei 8.078/90). (REsp nº 22.337-9 – RS, relator ministro Ruy Rosado de Aguiar, Quarta Turma, julgado em 13/02/1995, *DJ* 20/3/1995, p. 6119). Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=199200114466&dt_publicacao=20/03/1995. Acesso em: set. 2024.

[88] Ementa: EXECUÇÃO – REQUISIÇÃO DE INFORMAÇÃO DE ENDEREÇO DO RÉU AO BANCO CENTRAL – IMPOSSIBILIDADE 1. Embora na hipótese dos autos não se pretenda, através de requisição ao Banco Central, obter informações acerca de bens do devedor passíveis de execução, mas tão-somente o endereço, o raciocínio jurídico a ser adotado é o mesmo. 2. O contribuinte ou o titular de conta bancária tem direito à privacidade em relação aos seus dados pessoais, além do que não cabe ao Judiciário substituir a parte autora nas diligências que lhe são cabíveis para demandar em juízo. 3. Recurso especial não conhecido. (REsp nº 306.570 – SP, relatora ministra Eliana Calmon, Segunda Turma, julgado em 18/10/2001, *DJ* de 18/2/2002, p. 340.) Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200100235255&dt_publicacao=18/02/2002. Acesso em: set. 2024.

[89] Ementa: DIREITO PROCESSUAL CIVIL. RECURSO ESPECIAL. AÇÃO DE INDENIZAÇÃO POR UTILIZAÇÃO INDEVIDA DE IMAGEM EM SÍTIO ELETRÔNICO. PRESTAÇÃO DE SERVIÇO PARA EMPRESA ESPANHOLA. CONTRATO COM CLÁUSULA DE ELEIÇÃO DE FORO NO EXTERIOR. 1. A

Luis Felipe Salomão, da Quarta Turma, que manteve indenização por danos a uma empresa em razão da divulgação de imagem indevida de uma pessoa em página na *internet*. Em seu voto, o relator destacou um novo conceito de privacidade, pelo qual "toda pessoa tem de dispor com

---

evolução dos sistemas relacionados à informática proporciona a internacionalização das relações humanas, relativiza as distâncias geográficas e enseja múltiplas e instantâneas interações entre indivíduos. 2. Entretanto, a intangibilidade e mobilidade das informações armazenadas e transmitidas na rede mundial de computadores, a fugacidade e instantaneidade com que as conexões são estabelecidas e encerradas, a possibilidade de não exposição física do usuário, o alcance global da rede, constituem-se em algumas peculiaridades inerentes a esta nova tecnologia, abrindo ensejo à prática de possíveis condutas indevidas. 3. O caso em julgamento traz à baila a controvertida situação do impacto da internet sobre o direito e as relações jurídico-sociais, em um ambiente até o momento desprovido de regulamentação estatal. A origem da internet, além de seu posterior desenvolvimento, ocorre em um ambiente com características de auto-regulação, pois os padrões e as regras do sistema não emanam, necessariamente, de órgãos estatais, mas de entidades e usuários que assumem o desafio de expandir a rede globalmente. 4. A questão principal relaciona-se à possibilidade de pessoa física, com domicílio no Brasil, invocar a jurisdição brasileira, em caso envolvendo contrato de prestação de serviço contendo cláusula de foro na Espanha. A autora, percebendo que sua imagem está sendo utilizada indevidamente por intermédio de sítio eletrônico veiculado no exterior, mas acessível pela rede mundial de computadores, ajuíza ação pleiteando ressarcimento por danos material e moral. 5. Os artigos 100, inciso IV, alíneas "b" e "c" c/c art. 12, incisos VII e VIII, ambos do CPC, devem receber interpretação extensiva, pois quando a legislação menciona a perspectiva de citação de pessoa jurídica estabelecida por meio de agência, filial ou sucursal, está se referindo à existência de estabelecimento de pessoa jurídica estrangeira no Brasil, qualquer que seja o nome e a situação jurídica desse estabelecimento. 6. Aplica-se a teoria da aparência para reconhecer a validade de citação via postal com "aviso de recebimento-AR", efetivada no endereço do estabelecimento e recebida por pessoa que, ainda que sem poderes expressos, assina o documento sem fazer qualquer objeção imediata. Precedentes. 7. O exercício da jurisdição, função estatal que busca composição de conflitos de interesse, deve observar certos princípios, decorrentes da própria organização do Estado moderno, que se constituem em elementos essenciais para a concretude do exercício jurisdicional, sendo que dentre eles avultam: inevitabilidade, investidura, indelegabilidade, inércia, unicidade, inafastabilidade e aderência. No tocante ao princípio da aderência, especificamente, este pressupõe que, para que a jurisdição seja exercida, deve haver correlação com um território. Assim, para as lesões a direitos ocorridos no âmbito do território brasileiro, em linha de princípio, a autoridade judiciária nacional detém competência para processar e julgar o litígio. 8. O Art. 88 do CPC, mitigando o princípio da aderência, cuida das hipóteses de jurisdição concorrente (cumulativa), sendo que a jurisdição do Poder Judiciário Brasileiro não exclui a de outro Estado, competente a justiça brasileira apenas por razões de viabilidade e efetividade da prestação jurisdicional, estas corroboradas pelo princípio da inafastabilidade da jurisdição, que imprime ao Estado a obrigação de solucionar as lides que lhe são apresentadas, com vistas à consecução da paz social. 9. A comunicação global via computadores pulverizou as fronteiras territoriais e criou um novo mecanismo de comunicação humana, porém não subverteu a possibilidade e a credibilidade da aplicação da lei baseada nas fronteiras geográficas, motivo pelo qual a inexistência de legislação internacional que regulamente a jurisdição no ciberespaço abre a possibilidade de admissão da jurisdição do domicílio dos usuários da internet para a análise e processamento de demandas envolvendo eventuais condutas indevidas realizadas no espaço virtual. 10. Com o desenvolvimento da tecnologia, passa a existir um novo conceito de privacidade, sendo o consentimento do interessado o ponto de referência de todo o sistema de tutela da privacidade, direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações, nelas incluindo o direito à imagem. 11. [...] 12. [...]. 13. Ademais, a imputação de utilização indevida da imagem da autora é um "posterius" em relação ao contato de prestação de serviço, ou seja, o direito de resguardo à imagem e à intimidade é autônomo em relação ao pacto firmado, não sendo dele decorrente. A ação de indenização movida pela autora não é baseada, portanto, no contrato em si, mas em fotografias e imagens utilizadas pela ré, sem seu consentimento, razão pela qual não há se falar em foro de eleição contratual. 14. Quando a alegada atividade ilícita tiver sido praticada pela internet, independentemente de foro previsto no contrato de prestação de serviço, ainda que no exterior, é competente a autoridade judiciária brasileira caso acionada para dirimir o conflito, pois aqui tem domicílio a autora e é o local onde houve acesso ao sítio eletrônico onde a informação foi veiculada, interpretando-se como ato praticado no Brasil, aplicando-se à hipótese o disposto no artigo 88, III, do CPC. 15. Recurso especial a que se nega provimento. (REsp nº 1.168.547/RJ, relator ministro Luis Felipe Salomão, Quarta Turma, julgado em 11/5/2010, *DJe* de 7/2/2011.) Disponível em: https://scon.stj.jus.br/SCON/GetInteiro TeorDoAcordao?num_registro=200702529083&dt_publicacao=07/02/2011. Acesso em: set. 2024.

exclusividade sobre as próprias informações, incorporando assim a necessidade de consentimento" (Cueva, 2023, p. 82; 85; Mendes, 2021, p. 130-136).

Nos anos 2010, o STJ passou a analisar o cadastro positivo de crédito previsto na Lei nº 12.414/2011, o que deu origem aos recursos repetitivos sobre *credit scoring*¸ centrados na preocupação de proteger dados pessoais e evitar discriminações (Cueva, 2023, p. 85)[90].

A jurisprudência evoluiu para casos envolvendo remoção de dados pessoais com o advento do MCI (Lei nº 12.965/2014) (Cueva, 2023, p. 89-90)[91], sucedida pela discussão sobre direito ao esquecimento (p. 90-91)[92].

Como se vê, o Superior Tribunal de Justiça, há mais de 20 anos, debruça-se sobre temas que envolvem privacidade. O ministro Humberto Martins, que já o presidiu, admite que a entrada em vigor da Lei Geral de Proteção de Dados em 2020, colocou o Brasil no rol de países que reconhecem os cidadãos como titulares de direitos sobre seus dados pessoais (STJ, 2020)[93].

---

[90] Cita os REsp nº 1.457.199 – RS, de 2014, Rel. Min. Paulo de Tarso Sanseverino (que realizou audiência pública sobre o tema), no qual "o desrespeito aos limites legais na utilização do *credit scoring* pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço", e nº 1.348.532 – SP (recurso repetitivo), de 2017, Rel. Min. Salomão, no qual é abusiva e ilegal cláusula do contrato de cartão de crédito que "autoriza o banco a compartilhar dados dos consumidores com outras instituições financeiras". Lembra, por fim, que tal discussão fez gerar a Súmula 550: "A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo (julgado em 14/10/2015, *DJe* 19/10/2015)". Tal Súmula foi originada do tema Repetitivo nº 710, julgado antes da vigência da LGPD.

[91] Dá ênfase aos REsp nº 1.407.271 – SP e 1.342.640 – SP, relatados pela Min. Nancy Andrighi, segundo os quais os provedores de pesquisa/aplicação não respondem pelo conteúdo inserido por terceiros, nem são obrigados a exercer controle prévio do conteúdo de informações postadas por seus usuários. O REsp nº 1.660.168/RJ, de 2018, relatado pela ministra Nancy, vencida, no qual a 3ª Turma, evocando o direito à intimidade, à proteção de dados pessoais e ao esquecimento, concluiu que conteúdos ofensivos podem ser removidos pelo Poder Judiciário dos bancos de dados dos provedores de busca.

[92] Cita o REsp 1.660.168/RJ, de 2018, também relatado pela ministra Nancy, vencida, no qual a 3ª Turma, evocando o direito à intimidade, à proteção de dados pessoais e ao esquecimento, concluiu que conteúdos ofensivos podem ser removidos pelo Poder Judiciário dos bancos de dados dos provedores de busca. Posteriormente, o Supremo Tribunal Federal, em repercussão geral, fixou tese segundo a qual o direito ao esquecimento é incompatível com o ordenamento jurídico brasileiro (RE 1.010.606, Rel. Min. Dias Toffoli, em 2021), o que gerou forte repercussão na jurisprudência do STJ, que o afastou dali em diante (REsp nº 1.771.911 – SP, REsp nº 1.771.127 – SP, REsp nº 1.961.581 – MS, AgInt no REsp nº 1.774.425 – RJ; AREsp nº 1.880.762 – RJ).

[93] Além da responsabilidade civil, alguns temas envolvendo a LGPD foram levados à Corte, dentre os quais se destacam o AgInt nos EDcl no RMS 55819-MG, julgado em agosto de 2022, que versou sobre a obrigação da Administração Pública de guarda das informações de servidores, e o AgInt no RMS 70.212 – PR, julgado em junho de 2023, que examinou a questão da divulgação pública das remunerações dos delegatários de serventias extrajudiciais. Merecem destaque julgamentos do STJ em que se debateu a obrigação dos provedores de internet e de aplicação (típicos agentes de tratamento de dados) no que se à refere ao fornecimento de dados pessoais de autores de atos ilícitos. É o caso do REsp nº 1.914.596 – RJ, relatado pelo ministro Luís Felipe Salomão, julgado em novembro de 2021, que tratou sobre a quebra do sigilo de dados de usuários de internet para a identificação de infratores criminais, no contexto do assassinato da ex-vereadora Marielle Franco, decidindo por (i) reconhecer a obrigação do provedor de conexão/acesso à *internet* de fornecer os dados do usuário quando requerido pelo Poder Judiciário (entendimento antes reconhecido no REsp nº 1.785.092 – SP, Rel. Min. Nancy Andrighi) e; (ii) após a identificação do conteúdo ilícito e do IP do usuário (fornecido pelo provedor), assentar a desnecessidade de novo processo judicial para a obtenção dos seus dados cadastrais, bastando mera expedição de ofício à operadora de conexão. Segundo o ministro Ricardo Cueva, ali a jurisprudência buscou compatibilizar o dever leal de guarda dos registros de conexão e de acesso, previstos nos arts. 10, parágrafo 1º, e 22 do MCI, com a proteção da privacidade

Já o ministro Ricardo Cueva reconhece que foram poucas as ocasiões em que a Corte teve a oportunidade de se manifestar acerca da interpretação de seu conteúdo normativo, mas admite que há forte tendência que esse cenário se modifique rapidamente, citando o AREsp nº 2.130.619 – SP, objeto do tópico a seguir (Cueva, 2023, p. 95). Para ele, o aumento das transações dos titulares de dados com o 5G e o uso de instrumentos de inteligência artificial reforçam a importância da lei (STJ, 2020).

Especificamente sobre responsabilidade civil no âmbito da LGPD, embora sejam poucos os casos, a amostra utilizada na presente pesquisa (sete julgados) pode ser representativa, na medida em que o critério de busca foram todos os encontrados no banco de jurisprudência do Tribunal, julgados após a vigência da lei. Se, de um lado, pode denotar que o STJ ainda não amadureceu o tema (decorrente do curto espaço de tempo), de outro, demonstra o início do cumprimento de sua função uniformizadora da jurisprudência.

A análise de cada julgado considerará os seguintes parâmetros: i) se há ou não relação de consumo; ii) quais os tipos de dados pessoais envolvidos (comuns ou sensíveis); iii) circunstâncias do nexo de causalidade; iv) se houve inversão do ônus da prova do dano; v) quais as circunstâncias de segurança esperada / risco envolvidas; (vi) quais os artigos da LGPD citados; vii) se houve responsabilização; e viii) qual o regime aplicado. A definição desses parâmetros concretos e mensuráveis evitará uma abordagem apenas hermenêutica e abstrata, e ajudará a melhor compreensão da questão.

(Cueva, 2023, p. 98-99). Julgamentos correlatos: REsp nº 1.738.651 – MS – Rel. ministra Nancy Andrighi (dever de guarda de registros de aplicação); REsp nº 1.777.769 – SP – Rel. ministra Nancy Andrighi; REsp nº 1.785.092 – SP – Rel. ministra Nancy Andrighi (dever de guarda dos provedores de acesso); REsp nº 1.829.821 – SP – Rel. ministra Nancy Andrighi (fornecimento de IPs pelos provedores de aplicação) e REsp nº 1.859.665 – SC – Rel Min. Luis Felipe Salomão (impossibilidade de quebra de sigilo de todos os usuários que compartilham conteúdos difamatórios). Mais recentemente, os REsp nºs 2.135.783 – DF e 1.955.981 – GO, julgados respectivamente em junho e setembro de 2024 e relatados pela ministra Nancy Andrighi, abordaram a LGPD. O primeiro consignou o direito do motorista de aplicativo, na qualidade de titular de dados pessoais, de exigir a revisão de decisões automatizadas que definam seu perfil profissional (art. 20 da LGPD); o segundo reiterou a possibilidade das instituições financeiras de fornecerem dados de correntistas ao Ministério Público, requisitados em procedimentos criminais, sem violação de reserva de jurisdição e de sigilo bancário.

3.1 AREsp nº 2.130.619 – SP

A primeira decisão do Superior Tribunal de Justiça em que a responsabilidade civil de agente de tratamento, à luz da LGPD, foi o tema central é o Agravo em Recurso Especial nº 2.130.619 – SP, de relatoria do ministro Francisco Falcão, da Segunda Turma, em que litigaram uma consumidora e a companhia de energia do Estado de São Paulo – Eletropaulo, assim ementado[94]:

> PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZAMENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO.
> I – Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais.
> II – A sentença julgou os pedidos improcedentes, tendo a Corte Estadual reformulada para condenar a concessionária ao pagamento da indenização, ao fundamento de que se trata de dados pessoais de pessoa idosa.
> III – A tese de culpa exclusiva de terceiro não foi, em nenhum momento, abordada pelo Tribunal Estadual, mesmo após a oposição de embargos de declaração apontando a suposta omissão. Nesse contexto, incide, na hipótese, a Súmula n. 211/STJ. In casu, não há falar em prequestionamento ficto, previsão do art. 1.025 do CPC/2015, isso porque, em conformidade com a jurisprudência do STJ, para sua incidência deve a parte ter alegado devidamente em suas razões recursais ofensa ao art. 1022 do CPC/2015, de modo a permitir sanar eventual omissão através de novo julgamento dos embargos de declaração, ou a análise da matéria tida por omissa diretamente por esta Corte. Tal não se verificou no presente feito. Precedente: AgInt no REsp 1737467/SC, Rel. Ministro Napoleão Nunes Maia Filho, Primeira Turma, julgado em 8/6/2020, *DJe* 17/6/2020.
> IV – 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.**
> V – **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.**
> VI – Agravo conhecido e recurso especial parcialmente conhecido e, nessa parte, provido.
> (AREsp nº 2.130.619 – SP, relator ministro Francisco Falcão, Segunda Turma, julgado em 7/3/2023, *DJe* de 10/3/2023) (grifo nosso).

[94] Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202201522622&dt_publicacao=10/03/2023. Acesso em: jul. 2024.

A consumidora requeria indenização, a título de danos morais, em decorrência do vazamento e compartilhamento indevido de seus dados pessoais (nome completo, gênero, data de nascimento, idade, telefones, dados do contrato de fornecimento de energia elétrica, como carga instalada, consumo e instalação).

O caso foi julgado pela Segunda Turma em 7 de março de 2023, à unanimidade, tendo os ministros Mauro Campbell Marques, Humberto Martins, Herman Benjamin e Assusete Magalhães acompanhado o relator, ministro Falcão, para, indeferindo o pleito indenizatório, dar parcial provimento ao recurso da concessionária.

A ação indenizatória havia sido julgada improcedente, mas o TJ-SP acolheu a apelação da autora para condenar a concessionária ao pagamento de R$ 5 mil, em decorrência do vazamento de dados reservados, o que configuraria falha na prestação do serviço.

No Recurso Especial, a Eletropaulo alegou que o acórdão não poderia ter se fundamentado apenas na legislação consumerista, mas na Lei Geral de Proteção de Dados, que rege a matéria. Com isso, pugnou pela aplicação das excludentes de responsabilidade previstas no art. 43, II e III, da LGPD, que preveem a não responsabilização do agente de tratamento quando este não viola a legislação de proteção de dados e quando o dano decorre de culpa exclusiva de terceiro. Aduziu, ainda, que os dados não eram sensíveis, nos termos do art. 5º, II, da LGPD[95], e que a lei não acobertava indenização de dano eventual, futuro ou potencial, pelo disposto no art. 42, *caput,* do mesmo diploma.

Em seu voto, o relator deu razão à concessionária para admitir ofensa ao citado art. 5º, II, no sentido de que os dados do caso não eram sensíveis (de índole íntima), mas comuns (encontrados em qualquer cadastro, inclusive em *sites* consultados no dia a dia), não acobertados por sigilo, nem merecedores de tratamento diferenciado. Concluiu afirmando que o dano moral não é presumido, sendo necessário que o titular de dados comprove eventual dano decorrente da exposição a terceiros (Mendes; Fujimoto, 2024, p. 45), tudo para, ao final, afastar a responsabilidade da Eletropaulo.

Por seu pioneirismo, o acórdão foi objeto de debates na comunidade jurídica em torno de sua fundamentação (diga-se de passagem curta, apenas duas páginas), resumida na prescrição segundo a qual o vazamento de dados, por si só, não gera dano indenizável.

[95] LGPD, art. 5º. Para fins desta Lei, considera-se: [...] II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Infelizmente, o acórdão não adentrou em questões importantes da LGPD mencionadas pelo recorrente, como o cumprimento do dever de segurança do agente (art. 46), as excludentes de responsabilidade (art. 43, II e III) e a impossibilidade de reparação de dano futuro (art. 42, *caput),* sob a justificativa de não terem sido abordadas pelo Tribunal *a quo*, o que impôs a incidência da Súmula 211/STJ[96].

Houve quem entendesse que o julgado foi acertado por corrigir condenações excessivas de controladores de dados[97] e por abordar a questão do dano presumido no âmbito da proteção de dados[98]. Para outros, os fundamentos da decisão estariam baseados em falsas premissas (Marcon, 2023):

> (i) a natureza dos dados não deveria ser um critério para o reconhecimento de dano moral, já que não há distinção entre dados sensíveis e comuns nos fundamentos da lei;
> (ii) o rol do art. 5º, II, não é taxativo, e, portanto, exclusivo do tratamento diferenciado previsto no art. 11 da lei [99];
> (iii) dados "comuns" para uns podem ser "sensíveis" para outros; há dados sensíveis publicizados pelo próprio titular; o vazamento de dados comuns pode representar mais riscos a alguém do que a publicidade de dados sensíveis.

Observou-se, ainda, que essa decisão foi contrária ao que o Tribunal já havia decidido sobre dano moral presumido (*in re ipsa*) decorrente de incidentes envolvendo dados. Isto porque

---

[96] Súmula 211/STJ: Inadmissível recurso especial quanto à questão que, a despeito da oposição de embargos declaratórios, não foi apreciada pelo Tribunal *a quo*. (Corte Especial, julgado em 1/7/1998, *DJ* 03/08/1998, p. 366).

[97] "Tem-se dado tamanha importância para a segurança da intimidade das pessoas naturais, presente em seus dados pessoais, **que se passou a verificar verdadeira inversão dos dispositivos e propósitos da lei.** [...] muitos controladores de dados, geralmente empresas, **são condenados ao pagamento de indenizações vultosas ainda que não tenham praticado qualquer ato que efetivamente acarrete dano ao titular**. Isto justamente pela interpretação inadequada, até mesmo precipitada do regramento em evidência" (Rodrigues, 2023, grifo nosso).

[98] "É extremamente relevante em relação às discussões de reparação em decorrência do descumprimento da legislação de proteção de dados pessoais, em especial a LGPD. A um, porque é uma das primeiras decisões no STJ, na sua função de Corte de Uniformização, em que o tema é debatido e firmado. A dois, porque trata especificamente do dano moral *in re ipsa* no âmbito de proteção de dados pessoais. A três, porque, de forma mais sutil, estabelece uma relação entre dados sensíveis e a presunção do dano *in re ipsa*." (Tamer, 2023).

[99] LGPD, art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I – quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

em 2019, no julgamento do REsp nº 1.758.799 – MG[100], relatado pela ministra Nancy Andrighi, em caso que envolvia compartilhamento indevido de dados pessoais, a Terceira Turma entendeu que o descumprimento do dever de informação ao consumidor (não consentimento), somado à facilitação de acesso dos dados a terceiros, favorece a prática de atos ilícitos ou contratações fraudulentas, o que gera dano moral *in re ipsa,* em clara aplicação do regime de responsabilidade objetiva. Ali, contudo, a LGPD ainda não vigorava, sendo as bases legais o CDC e a Lei do Cadastro Positivo (nº 12.414/2011)[101].

Quanto à possibilidade de reparação apenas ao vazamento de dados sensíveis ou íntimos, esta se constituiu na crítica mais reiterada ao julgamento, tendo em vista ter

---

[100] Ementa: RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL IN RE IPSA. JULGAMENTO: CPC/15. 1. Ação de compensação de dano moral ajuizada em 10/05/2013, da qual foi extraído o presente recurso especial, interposto em 29/04/2016 e atribuído ao gabinete em 31/01/2017. 2. O propósito recursal é dizer sobre: (i) a ocorrência de inovação recursal nas razões da apelação interposta pelo recorrido; (ii) a caracterização do dano moral em decorrência da disponibilização/comercialização de dados pessoais do recorrido em banco de dados mantido pela recorrente. 3. A existência de fundamento não impugnado – quando suficiente para a manutenção das conclusões do acórdão recorrido – impede a apreciação do recurso especial (súm. 283/STF). 4. A hipótese dos autos é distinta daquela tratada no julgamento do REsp 1.419.697 – RS (julgado em 12/11/2014, pela sistemática dos recursos repetitivos, *DJe* de 17/11/2014), em que a Segunda Seção decidiu que, no sistema *credit scoring,* não se pode exigir o prévio e expresso consentimento do consumidor avaliado, pois não constitui um cadastro ou banco de dados, mas um modelo estatístico. 5. A gestão do banco de dados impõe a estrita observância das exigências contidas nas respectivas normas de regência – CDC e Lei 12.414/2011 – dentre as quais se destaca o dever de informação, que tem como uma de suas vertentes o dever de comunicar por escrito ao consumidor a abertura de cadastro, ficha, registro e dados pessoais e de consumo, quando não solicitada por ele. 6. 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. 7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor – 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. 8. Em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, prática essa autorizada pela Lei 12.414/2011 em seus arts. 4º, III, e 9º, deve ser observado o disposto no art. 5º, V, da Lei 12.414/2011, o qual prevê o direito do cadastrado ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais 9. O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais. 10. Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos. 11. Hipótese em que se configura o dano moral *in re ipsa*. 12. Em virtude do exame do mérito, por meio do qual foram rejeitadas as teses sustentadas pela recorrente, fica prejudicada a análise da divergência jurisprudencial. 13. Recurso especial conhecido em parte e, nessa extensão, desprovido. (REsp nº 1.758.799 – MG, relatora ministra Nancy Andrighi, Terceira Turma, julgado em 12/11/2019, *DJe* de 19/11/2019). Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201700065219&dt_publicacao=19/11/2019. Acesso em: jul. 2024.

[101] Embora sem referência expressa à LGPD, o acórdão tratou de diversas questões nela contidas, a exemplo dos direitos do titular de acesso aos dados armazenados e de retificação das informações incorretas, previstos respectivamente nos incisos II e III do art. 18.

desconsiderado o paradigma de que não existem dados insignificantes no contexto da proteção de dados, carecendo todos de igual proteção, independentemente de sua categoria jurídica (Mendes; Fujimoto, 2024, p. 46).

Por fim, no que se refere ao regime de responsabilidade civil, embora não especificamente indicado no acórdão, restou configurado como sendo o de natureza subjetiva, mesmo numa relação de consumo, por não admitir dano presumido, portanto, dependente de demonstração de culpa do agente de tratamento no evento danoso.

3.2 REsp nº 2.077.278 – SP

O segundo julgamento do STJ em que a reparação civil em incidente de vazamento figurou como matéria central foi o Recurso Especial nº 2.077.278 – SP. O caso, relatado pela ministra Nancy Andrighi, abordou a responsabilidade de uma instituição financeira no chamado "golpe do boleto"[102]:

> CONSUMIDOR. RECURSO ESPECIAL. AÇÃO DECLARATÓRIA DE INEXIGIBILIDADE DE DÉBITO POR VAZAMENTO DE DADOS BANCÁRIOS CUMULADA COM INDENIZAÇÃO POR DANOS MORAIS E REPETIÇÃO DE INDÉBITO. GOLPE DO BOLETO. TRATAMENTO DE DADOS PESSOAIS SIGILOSOS DE MANEIRA INADEQUADA. FACILITAÇÃO DA ATIVIDADE CRIMINOSA. FATO DO SERVIÇO. DEVER DE INDENIZAR PELOS PREJUÍZOS. SÚMULA 479/STJ. RECURSO ESPECIAL PROVIDO.
> 1. Ação declaratória de inexigibilidade de débito por vazamento de dados bancários cumulada com indenização por danos morais e repetição de indébito, ajuizada em 13/2/2020, da qual foi extraído o presente recurso especial, interposto em 15/2/2022 e concluso ao gabinete em 19/6/2023.
> 2. O propósito recursal consiste em decidir se a instituição financeira responde por falha na prestação de serviços bancários, consistente no vazamento de dados que facilitou a aplicação de golpe em desfavor do consumidor.
> 3. Se comprovada a hipótese de vazamento de dados da instituição financeira, será dela, em regra, a responsabilidade pela reparação integral de eventuais danos. Do contrário, inexistindo elementos objetivos que comprovem esse nexo causal, não há que se falar em responsabilidade das instituições financeiras pelo vazamento de dados utilizados por estelionatários para a aplicação de golpes de engenharia social (REsp 2.015.732 – SP, julgado em 20/6/2023, *DJe* de 26/6/2023).
> 4. **Para sustentar o nexo causal entre a atuação dos estelionatários e o vazamento de dados pessoais pelo responsável por seu tratamento, é imprescindível perquirir, com exatidão, quais dados estavam em poder dos criminosos, a fim de examinar a origem de eventual vazamento e, consequentemente, a responsabilidade dos agentes respectivos**. Os nexos de causalidade e imputação, portanto, dependem da hipótese concretamente analisada.
> 5. Os dados sobre operações bancárias são, em regra, de tratamento exclusivo pelas instituições financeiras. No ponto, a Lei Complementar 105/2001 estabelece que as instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados (art. 1º), constituindo dever jurídico dessas entidades não revelar informações que venham a obter em razão de sua atividade profissional, salvo em situações excepcionais. Desse modo, seu armazenamento de maneira inadequada, a possibilitar que terceiros tenham conhecimento de informações sigilosas e causem prejuízos ao consumidor, configura defeito na prestação do serviço (art. 14 do CDC e art. 44 da LGPD).

[102] Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202301909798&dt_publicacao= 09/10/2023. Acesso em: jul. 2024.

> 6. No particular, **não há como se afastar a responsabilidade da instituição financeira pela reparação dos danos decorrentes do famigerado "golpe do boleto", uma vez que os criminosos têm conhecimento de informações e dados sigilosos a respeito das atividades bancárias do consumidor**. Isto é, os estelionatários sabem que o consumidor é cliente da instituição e que encaminhou e-mail à entidade com a finalidade de quitar sua dívida, bem como possuem dados relativos ao próprio financiamento obtido (quantidade de parcelas em aberto e saldo devedor do financiamento).
> 7. O tratamento indevido de dados pessoais bancários configura defeito na prestação de serviço, notadamente quando tais informações são utilizadas por estelionatário para facilitar a aplicação de golpe em desfavor do consumidor.
> 8. Entendimento em conformidade com Tema Repetitivo 466/STJ e Súmula 479/STJ: "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias".
> 9. Recurso especial conhecido e provido para reformar o acórdão recorrido e reestabelecer a sentença proferida pelo Juízo de primeiro grau.
> (REsp nº 2.077.278 – SP, relatora ministra Nancy Andrighi, Terceira Turma, julgado em 3/10/2023, *DJe* de 9/10/2023) (grifo nosso).

O caso, mais uma vez, versou sobre relação de consumo, agora entre a instituição financeira BV (agente de tratamento, controladora de dados) e uma correntista (titular de dados), em um financiamento de veículo.[103]

Foi julgado pela Terceira Turma em 3 de outubro de 2023, à unanimidade, tendo os ministros Ricardo Villas Bôas Cueva, Humberto Martins e Moura Ribeiro acompanhado a relatora ministra Nancy, para conhecer e dar provimento ao Recurso Especial.

Na origem, a cliente ajuizou ação declaratória de inexigibilidade de débito cumulada com indenização por danos morais, alegando ter pago boleto falso decorrente do vazamento de seus dados bancários. O juízo de 1º grau julgou procedente a pretensão. Inconformado, o banco apelou, argumentando que a cliente não "agiu com o dever de cautela que se espera do homem médio". O TJ-SP reformou a sentença, aduzindo que não houve falha na prestação de serviços do banco e que o dano decorreu de culpa exclusiva de terceiro, excludente de responsabilidade prevista no art. 14, § 3º, do CDC.

O REsp da consumidora evocou a LGPD e sustentou que cabia à BV Financeira o ônus de provar que manteve a segurança necessária de seu sistema de dados para evitar o vazamento.

A ministra relatora iniciou seu voto citando a Súmula 479/STJ ("As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias"), para lembrar que somente

[103] Súmula 297/STJ: O Código de Defesa do Consumidor é aplicável às instituições financeiras.

haveria responsabilidade do agente se averiguado nexo de causalidade[104] entre os estelionatários e o vazamento, o que se identificaria por meio dos tipos de dados envolvidos.

No caso, ela concluiu que os dados vazados não eram meramente cadastrais (com possibilidade de obtenção por fontes alternativas), mas sigilosos[105] (decorrentes das operações financeiras, que somente a BV teria acesso – nº de contrato, valor de quitação, informação do pedido de quitação por e-mail etc.). Tais informações deveriam ser bem guardadas pelo banco, o que não ocorreu, configurando falha na prestação do serviço (art. 14 do CDC e 43 da LGPD[106]). Citou expressamente o "tratamento irregular" contido no art. 44 da LGPD, o dever de segurança e risco esperado pela cliente e a previsão do art. 45, que impõe o regime de responsabilidade objetiva por fato do serviço, para, ao final, restabelecer a sentença de condenação.

Sobre a aplicação do regime de responsabilidade civil, o julgado faz alusão ao de natureza objetiva previsto no CDC: "a proteção conferida pelo CDC abrange a responsabilidade do fornecedor pela reparação dos danos causados por defeitos relativos à prestação de serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos, independentemente da existência de culpa (art. 14 do CDC)".

Desse modo, embora não tenha consignado explicitamente que o regime aplicável à LGPD também seja o objetivo, a citação de diversos artigos da lei (incluído o 43, o 44 e o 45), o foco no nexo de causalidade e a ênfase no tratamento irregular, denota uma mudança de postura da Corte em relação ao julgado analisado no tópico anterior, para se concluir pelo reconhecimento da aplicação da responsabilidade objetiva ao agente de tratamento[107].

---

[104] Fez referência ao REsp nº 2.015.732 – SP, de sua relatoria, julgado em 20/6/2023, que tratou sobre o "golpe do motoboy" e definiu ser a comprovação do nexo de causalidade condição para a responsabilidade das instituições financeiras pelo vazamento de dados utilizados por estelionatários. Essa referência está presente no voto-vista do ministro Humberto Martins. Obs.: este REsp nº 2.015.732 – SP, embora semelhante ao de nº 1.995.458 – SP – analisado adiante no item 3.4.1 – não foi selecionado para análise mais aprofundada desta pesquisa, pois faz uma brevíssima menção à LGPD, sem, contudo, mencionar quaisquer de seus artigos.

[105] Muito antes da vigência da LGPD, em 2001, a ministra Nancy já havia se pronunciado em favor do sigilo dos dados do consumidor-correntista, como relatora do AGREsp nº 251.121 – SP, assim ementado: EXECUÇÃO FISCAL – REQUISIÇÃO JUDICIAL DE QUEBRA DE SIGILO BANCÁRIO – MOTIVO RELEVANTE INEXISTENTE – IMPOSSIBILIDADE. Informações sobre movimentação bancária só devem ser expostas em casos de grande relevância para a prestação jurisdicional, consoante entendimento assentado na jurisprudência desta Colenda Corte. Agravo improvido. (AGREsp nº 251.121 – SP, Relatora ministra Nancy Andrighi, 2ª Turma, unânime, *DJ* de 26/03/2001, página 00415).

[106] Indicou, ainda, que a instituição financeira não se desincumbiu do seu ônus de provar eventual causa excludente da sua responsabilidade nos termos destes dois artigos (14, §3º, do CDC e 43 da LGPD).

[107] Convém citar o REsp nº 2.052.228 – DF, de relatoria da ministra Nancy, julgado em setembro de 2023, que trata de assunto muito semelhante ao analisado (nº 2.077.278 – SP): correntista buscou reparação civil decorrente de golpe caracterizado por movimentação atípica e fora do padrão de consumo. Todavia, embora tenha sido expressamente indicada a responsabilidade objetiva do banco pela falta do dever de segurança, não houve qualquer menção à LGPD, descabendo, desse modo, maior atenção neste trabalho.

3.3 REsp nº 2.092.096 – SP

No fim de 2023, a Terceira Turma julgou novo caso em que a compensação civil na LGPD esteve no centro do debate, o Recurso Especial nº 2.092.096 – SP, também de relatoria da ministra Nancy Andrighi, cuja ementa é a seguinte[108]:

> CIVIL, CONSUMIDOR E PROCESSUAL CIVIL. AÇÃO INDENIZATÓRIA C/C OBRIGAÇÃO DE FAZER. VIOLAÇÃO DOS ARTS. 489 E 1.022 DO CPC. AUSÊNCIA. CONDIÇÕES DA AÇÃO. TEORIA DA ASSERÇÃO. LEGITIMIDADE PASSIVA. CONFIGURAÇÃO. CERCEAMENTO DE DEFESA. AUSÊNCIA. FORNECIMENTO DE SERVIÇOS PELA B3 AOS INVESTIDORES FORA DO ÂMBITO DAS OPERAÇÕES NO MERCADO DE CAPITAIS. RELAÇÃO JURÍDICA DIRETA E AUTÔNOMA DE CONSUMO. INCIDÊNCIA DO CDC. DISSÍDIO JURISPRUDENCIAL. SIMILITUDE FÁTICA. AUSÊNCIA. PLATAFORMA VIRTUAL QUE ARMAZENA E UTILIZA DADOS PESSOAIS DOS INVESTIDORES. INCIDÊNCIA DA LGPD E DO MARCO CIVIL DA INTERNET. ACESSO NÃO AUTORIZADO POR TERCEIROS. EXCLUSÃO DOS DADOS INSERIDOS INDEVIDAMENTE POR TERCEIROS. POSSIBILIDADE. FORNECIMENTO DE REGISTROS E DADOS CADASTRAIS REFERENTES AO ACESSO NÃO AUTORIZADO. POSSIBILIDADE.
> 1. Ação indenizatória c/c obrigação de fazer, ajuizada em 17/2/2022, da qual foi extraído o presente recurso especial, interposto em 24/5/2023 e concluso ao gabinete em 21/8/2023.
> 2. O propósito recursal é decidir se (I) houve negativa de prestação jurisdicional; (II) a relação jurídica em exame é regida pelo CDC;
> (III) há legitimidade passiva da recorrente na espécie; (IV) houve cerceamento de defesa pelo indeferimento de provas; (V) a B3 tem a obrigação de excluir os dados cadastrais inseridos indevidamente por terceiros que obtiveram acesso não autorizado ao perfil do investidor em sua plataforma virtual; e (VI) a B3, por fornecer tal plataforma, se enquadra no conceito de provedora de aplicação de internet previsto no Marco Civil da Internet.
> 3. Não há ofensa aos arts. 489 e 1.022 do CPC, quando o Tribunal de origem examina, de forma fundamentada, a questão submetida à apreciação judicial na medida necessária para o deslinde da controvérsia, ainda que em sentido contrário à pretensão da parte.
> Precedentes.
> 4. Conforme a jurisprudência desta Corte, as condições da ação são verificadas segundo a teoria da asserção, de tal modo que, para o reconhecimento da legitimidade passiva ad causam, basta que os argumentos aduzidos na inicial possibilitem a inferência, em um exame puramente abstrato, de que o réu pode ser o sujeito responsável pela violação do direito subjetivo do autor. Na hipótese, das afirmações constantes da inicial, depreende-se, em abstrato, a legitimidade passiva da recorrente (B3).
> 5. Não configura cerceamento de defesa a sentença que julga antecipadamente os pedidos, resolvendo a causa sem a produção de outras provas em razão da suficiência probatória, porquanto cabe ao juiz decidir sobre os elementos

[108] Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202302947974&dt_publicacao=15/12/2023. Acesso em: jul. 2024.

necessários à formação de seu entendimento, sendo livre para, motivadamente, determinar as provas necessárias ou indeferir as inúteis ou protelatórias. Precedentes.
6. No âmbito das operações no mercado de capitais, não incide o CDC na relação jurídica entre o investidor titular das ações e a B3, tendo em vista que, no âmbito dessas operações, a Bolsa não oferece serviços diretamente aos investidores, mantendo relação exclusivamente com as distribuidoras e corretoras de valores mobiliários. Precedente.
7. Não obstante, ao disponibilizar uma plataforma virtual para acesso direto, pessoal e exclusivo pelo investidor (Canal Eletrônico do Investidor), de caráter informativo a respeito de seus investimentos, a B3 fornece serviços diretamente para o consumo do investidor, estabelecendo com ele relação jurídica autônoma de consumo, regida pelo CDC.
8. A B3, ao manter um sistema que armazena e utiliza dados dos investidores referentes à sua identificação pessoal, realiza operação de tratamento de dados pessoais e, assim, se submete às normas previstas na Lei Geral de Proteção de Dados (LGPD).
9. Em observância aos arts. 18, III e IV, da LGPD, o titular dos dados pessoais tem o direito de requisitar a correção de dados incompletos, inexatos ou desatualizados; e a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei.
10. O agente de tratamento de dados tem o dever de assegurar os princípios previstos na LGPD, dentre eles o da adequação e da segurança (art. 6º, II e VII), devendo, ainda, adotar medidas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de alteração, destruição, perda, comunicação dos dados (art. 46).
11. Assim, havendo requisição por parte do titular, o agente de tratamento de dados tem a obrigação de excluir os dados cadastrais inseridos indevidamente por terceiros que obtiveram acesso não autorizado à conta do titular em sua plataforma, em observância aos arts. 18, IV, c/c os arts. 46 a 49 e 6º, II e VII, da LGPD.
12. Segundo a jurisprudência desta Corte, o art. 22 do Marco Civil da Internet autoriza, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, a requisição judicial de registros de conexão ou de acesso daquele responsável pela guarda dos referidos dados, desde que preenchidos os requisitos previstos no parágrafo único do referido dispositivo legal.
13. Na espécie, a B3 se enquadra no conceito de provedor de aplicação de internet, em razão da sua função de administrar e fornecer uma plataforma virtual aos investidores, que é acessada por dispositivos conectados à internet, incidindo, no âmbito dessa atividade, as normas previstas no Marco Civil da Internet.
14. Hipótese em que foi afastada a responsabilidade civil da B3 por danos morais alegados pelo recorrido; sendo a B3 condenada apenas a fornecer informações, registros de conexão e dados relacionados ao acesso não autorizado pelos terceiros no perfil do recorrido; e a excluir os dados inseridos pelos fraudadores.
15. Recurso especial conhecido e não provido.
(REsp nº 2.092.096 – SP, relatora ministra Nancy Andrighi, Terceira Turma, julgado em 12/12/2023, *DJe* de 15/12/2023) (grifo nosso).

O recurso também foi julgado à unanimidade, tendo participado do julgamento os ministros Ricardo Villas Bôas Cueva, Humberto Martins, Moura Ribeiro e Marco Aurélio Bellizze, que acompanharam a relatora ministra Nancy, para conhecer e negar provimento ao Recurso Especial.

Tratou-se de ação indenizatória cumulada com obrigação de fazer ajuizada por investidor contra a Bolsa de Valores B3, centrada no acesso de fraudadores à sua conta de investimentos na plataforma virtual de negociação de valores mobiliários (Canal Eletrônico do Investidor – CEI). Os fraudadores teriam visualizado os investimentos, solicitado senhas e alterado dados cadastrais, embora não tenham conseguido realizar movimentações financeiras.

O juízo de 1º grau julgou parcialmente procedente o pleito apenas para condenar a ré a fornecer detalhamento desse acesso de terceiros. Já o tribunal estadual negou provimento à Apelação da B3 e, embora tenha afastado responsabilidade por dano, deu parcial provimento ao apelo do investidor para determinar a exclusão dos dados indevidamente inseridos pelo fraudador.

Distintamente dos dois casos anteriores, houve questionamento da recorrente quanto à caracterização da relação entre as partes como de consumo, pelo fato de a Bolsa não oferecer diretamente serviços ao investidor e manter relação somente com as distribuidoras e corretoras. No julgamento, a Turma estatuiu que, embora as relações jurídicas entre investidores e as entidades de compensação/liquidação (Bolsas) não sejam de consumo (cf. REsp nº 1.646.261/RJ), o caso impunha a incidência do CDC, já que a B3 disponibilizou ao investidor um serviço informativo autônomo, canal virtual próprio, por ela criado e gerido exclusivamente.

Também restou consignado que a Bolsa, ao armazenar e utilizar dados dos investidores na plataforma, realiza típica operação de tratamento de dados (incidência dos arts. 3º e 5º, I e X, da LGPD), devendo observar os princípios de adequação e segurança (arts. 6º, II e VII, e 46 da LGPD), inclusive após o término do tratamento (art. 47 da LGPD)[109], obrigando-se, ainda, a excluir dados cadastrais inverídicos inseridos por terceiros, em respeito ao direito do titular de dados de correção de dados incompletos, inexatos ou desatualizados, e de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei (art. 18, III e IV, e 49 da LGPD[110]).

---

[109] LGPD, art. 47: Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

[110] LGPD, art. 18: O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...] III – correção de dados incompletos, inexatos ou desatualizados; IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei. [...] Art 49: Os sistemas utilizados para o tratamento de dados pessoais

Sobre a responsabilidade por danos oriundos da falha na prestação do serviço, o julgado lembrou que, a despeito da fraude da corretora – que não impediu a abertura indevida em nome do investidor por parte dos terceiros – e do fato de a B3 ter comunicado o incidente a ele investidor[111], restou comprovado não ter a recorrente garantido a autenticidade e a segurança do acesso de cada usuário, impondo-se a ela o dever de exclusão dos dados[112] inseridos pelo fraudador.

Ademais, a Terceira Turma manteve a condenação da Bolsa de Valores na obrigação de fornecer o detalhamento do acesso fraudulento (datas, registros de conexão, atividades realizadas, dados acessados etc.), por considerá-la provedora de aplicação de *internet* (já que administra e fornece a plataforma virtual), cabendo, assim, o disposto no art. 22 do MCI[113]. No que se refere aos danos morais, o Tribunal *a quo* asseverou serem indevidos pois constituídos em dissabores ocasionados por terceiros, não tendo o investidor, em sede de Recurso Especial, insurgindo-se contra isso.

Quanto ao regime de responsabilidade civil na LGPD, conquanto não abertamente mencionado, diante do paralelo ao art. 14 do CDC (falha na prestação do serviço), das inúmeras citações à lei e do grande destaque ao defeito no tratamento de dados fornecido com segurança inferior à esperada pelo titular, também se pode extrair a conclusão de ter a Terceira Turma, mais uma vez, optado pelo regime de natureza objetiva.

---

devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

[111] O acórdão acentua que tais circunstâncias, em tese, poderiam atrair a excludente de culpa exclusiva de terceiro (prevista no art. 43, III, da LGPD), tendo sido, todavia, afastada pelas instâncias de origem e não aventadas pelo recorrente.

[112] Não houve questionamento sobre o tipo de dado envolvido (se comum ou sensível), tendo a discussão se centrado na conceituação geral de dado pessoal prevista no art. 5º, I, da LGPD.

[113] MCI, art. 22: A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

3.4 REsp nº 2.147.374 – SP

Um ano após o julgamento estudado no tópico anterior, em dezembro de 2024, a Terceira Turma enfrentou mais um processo focado na responsabilidade civil de agente de tratamento decorrente de ato ilícito, no caso um ataque cibernético (*hacker*)[114]:

> RECURSO ESPECIAL. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. DIREITO À PRIVACIDADE, À LIBERDADE E À AUTODETERMINAÇÃO INFORMATIVA. AGENTE DE TRATAMENTO. **VAZAMENTO DE DADOS NÃO SENSÍVEIS DO TITULAR. INCIDENTE DE SEGURANÇA. ATAQUE HACKER. RESPONSABILIDADE EXCLUSIVA DE TERCEIRO. NÃO COMPROVADA. RESPONSABILIDADE CIVIL PROATIVA. EXPECTATIVA DE LEGÍTIMA PROTEÇÃO.** COMPLIANCE E REGULAÇÃO DE RISCO DA ATIVIDADE. DIREITOS DO TITULAR. CONCRETIZAÇÃO. APLICABILIDADE.
> 1. A controvérsia jurídica consiste em definir se o vazamento de dados pessoais não sensíveis do titular, decorrente de atividade alegadamente ilícita, é passível de imputar ao agente de tratamento de dados as obrigações previstas no art. 19, II, da LGPD, ou se o fato de tal vazamento ter decorrido de atividade ilícita seria uma excludente de responsabilidade, prevista no art. 43, III, da LGPD.
> 2. Ao inscrever a proteção e o tratamento de dados pessoais no rol dos direitos e garantias fundamentais da Constituição (art. 5º, LXXIX), a Emenda Constitucional nº 115/2022 inaugurou um novo capítulo no ordenamento jurídico brasileiro no que tange aos direitos de personalidade, à liberdade e à autodeterminação informativa.
> 3. **A empresa recorrente**, pelo fato de se enquadrar na categoria dos agentes de tratamento, tinha **a obrigação legal de tomar todas as medidas de segurança esperadas pelo titular para que suas informações fossem protegidas, e seus sistemas utilizados para o tratamento de dados pessoais deveriam estar estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD** e às demais normas regulamentares.
> 4. Compliance de dados é o esforço de conformidade e de aplicação da LGPD nas atividades das empresas que lidam com tratamento de dados.
> Referido instrumento assume importância central ao induzir não apenas à obediência ao direito, mas também à comprovação da efetividade dos programas de conformidade.
> 5. O tratamento de dados pessoais configurou-se como irregular quando deixou de fornecer a segurança que o titular dele poderia esperar ("expectativa de legítima proteção"), consideradas as circunstâncias relevantes, entre as quais as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado (art. 44, III, da LGPD).
> 6. **Ao não provar, perante as instâncias ordinárias, que o vazamento dos dados da recorrida teria se dado exclusivamente em razão do incidente de segurança, é impossível aplicar em favor da recorrente a excludente de responsabilidade do art. 43, III, da LGPD.**

[114] Inteiro teor disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202202209228&dt_publicacao=06/12/2024. Acesso em: mar. 2025.

> 7. Assim, correta a conclusão do TJSP de concretizar os direitos do titular ao condenar a recorrente na obrigação de apresentar informação das entidades públicas e privadas com as quais realizou o uso compartilhado dos dados da recorrida (art. 18, VII, da LGPD) e a fornecer declaração completa que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, bem como a cópia exata de todos os dados referentes ao titular constantes em seus bancos de dados (art. 19, II, da LGPD).
> 8. Recurso especial não provido.
> (REsp nº 2.147.374 – SP, relator ministro Ricardo Villas Bôas Cueva, Terceira Turma, julgado em 3/12/2024, *DJEN* de 6/12/2024) (grifo nosso).

O caso envolveu, tal qual o AREsp nº 2.130.619 – SP, a relação entre a concessionária de energia do Estado de São Paulo (Eletropaulo) e uma consumidora. Esta alegou ter recebido comunicado do Instituto Brasileiro de Proteção de Dados (Iprodape) com notícia sobre de incidente de segurança envolvendo seus dados pessoais (nome, número de RG e CPF e telefone), pelo que requereu indenização por danos morais.

A sentença julgou improcedentes seus pedidos. Todavia, o Tribunal de Justiça, embora tenha afastado o pleito indenizatório (ao fundamento da ausência de prova dos danos sofridos), condenou a ré a apresentar as informações das entidades públicas e privadas com as quais realizou o compartilhamento de dados, a fornecer a lista completa desses dados, sua origem, os critérios e finalidade de tratamento e a inexistência de registro. Irresignada, a concessionária interpôs o Recurso Especial.

Dessa vez, tendo como relator o ministro Ricardo Villas Bôas Cueva, o recurso foi julgado em 3 de dezembro de 2024, à unanimidade, com participação dos ministros Nancy Andrighi, Humberto Martins e Moura Ribeiro, os quais, deferindo o pleito indenizatório, negaram provimento ao recurso da Eletropaulo.

No voto, constou preliminar de competência da Terceira Turma, com referência ao julgamento do AREsp nº 2.130619 – SP da Segunda Turma (objeto do subitem 3.1 deste capítulo), em que se reafirmou a competência da Segunda Seção (de Direito Privado, composta pela Terceira e Quarta Turmas) para o julgamento de recursos que versem sobre a responsabilidade civil entre consumidores e concessionárias de serviço público, na medida em que a natureza jurídica dessa relação não decorre de contrato administrativo (o que atrairia a competência da Primeira Seção, de Direito Público, onde está a Segunda Turma), mas, sim, de caráter privado.

No mérito, o acórdão foi iniciado com a reafirmação do direito à proteção de dados como preceito fundamental, seja pela inclusão no rol do art. 5º da Constituição Federal, seja pelo reconhecimento pelo Supremo Tribunal Federal no julgamento das ADIs nºs 6.388, 6.389, 6.390 e 6.393, de relatoria da ministra Rosa Weber, com destaque para as lições de Laura

Schertel Mendes e Danilo Doneda sobre a importância da autodeterminação informativa, de modo que "não existem dados insignificantes nas circunstâncias modernas".

Na esteira de inúmeros dispositivos da LGPD, relacionados a direitos do titular, princípios e responsabilidade (arts. 5º, 17 a 22, 42 a 45, 49 e 50), o julgado enfatizou a necessidade da adoção de medidas de segurança esperadas pelo titular, por parte do agente de tratamento, incluídas as relativas às boas práticas, regras de governança, mecanismos internos de supervisão, prestação de contas (*accontability),* tudo para concretizar o que chama de *compliance* de dados.

Quanto ao incidente de vazamento, consistente num ataque cibernético (*hacker*), acentuou-se a corrosão da privacidade por ele gerada, com apropriação indevida, contínua e indeterminada por terceiros de um grande número de dados, até mesmo sensíveis, e a possibilidade de seu reconhecimento como fortuito interno, gerador de responsabilidade pelo teor da Súmula nº 479/STJ.

No campo da responsabilização, a Terceira Turma reforçou o papel das balizas criadas e consolidadas pelo microssistema introduzido pela LGPD, antes circunscritas às leis civis e ao CDC. A grande novidade é a referência, enfática por sinal, a "um novo sistema de responsabilização", a responsabilidade civil proativa", defendida por Maria Celina Bodin de Moraes e baseada na "demonstração da adoção de medidas eficazes de proteção", para "além da clássica dicotomia entre as vertentes objetiva e subjetiva".

Lembrou-se do tratamento irregular previsto no art. 44, III, da LGPD ("expectativa legítima de proteção") e da obrigatoriedade de prova, por parte do agente de tratamento, perante as instâncias de origem, de que o vazamento se deu exclusivamente em razão do incidente, para que este possa se valer da excludente de responsabilidade prevista no art. 43, III, da lei ("culpa exclusiva de terceiro"), o que, no caso, segundo o STJ, não ocorreu.

Nesse tópico, o acórdão também fez menção à questão do ônus probatório, com o destaque da possibilidade de sua inversão pela inteligência do art. 42, § 2º, da LGPD, e 6º, VIII, do CDC, desde que "a alegação seja admissível, haja hipossuficiência do titular para a produção da prova ou que, sua produção pelo titular, se mostre demais onerosa", razão pela qual aduziu-se que o tribunal estadual acertou ao condenar a concessionária no ônus de apresentação das informações sobre a cópia completa dos dados compartilhados, sua origem, os critérios e finalidades de tratamento, a inexistência de registro e a lista das entidades públicas e privadas com as quais realizou o compartilhamento (respaldo dos arts. 18, VII e 19, II, da LGPD). Não houve condenação em dano moral, porque o acórdão estadual indeferiu esse pleito, contra o qual a consumidora não mais se insurgiu.

Por tais motivos, não é outra a conclusão que se chega se não a de que esse julgamento fortaleceu a adoção do regime de responsabilização objetiva no âmbito da Terceira Turma, dando contornos mais profundos centrados na importância das medidas de segurança a serem adotadas pelo agente de tratamento.

Cumpre considerar que as comparações entre esse julgamento e o do AREsp nº 2.130619 – SP são inevitáveis, uma vez que ambos se centram na mesma relação jurídica (vazamento de dados no contexto de consumo entre usuário e concessionária de energia) para chegar a conclusões distintas. Aqui, sob o viés privado (competência da Segunda Seção, na qual se insere a Terceira Turma), o STJ deixa clara sua visão pela responsabilização objetiva do agente de tratamento em incidente de vazamento, ainda que num contexto de dados comuns (não sensíveis); lá, sob o viés público (competência da Primeira Seção, onde inserida a Segunda Turma), a opção é pelo regime subjetivo em incidentes envolvendo dados comuns (não sensíveis).

3.5 REsp nº 2.121.904 – SP

No início de 2025, a Terceira Turma voltou a julgar caso de responsabilidade do agente de tratamento, no Recurso Especial nº 2.121.904 – SP, igualmente de relatoria da ministra Nancy Andrighi, cuja ementa é a seguinte[115]:

> CIVIL. RECURSO ESPECIAL. **CONTRATO DE SEGURO DE VIDA.** RELAÇÃO DE CONSUMO. CÓDIGO DE DEFESA DO CONSUMIDOR. LEI GERAL DE PROTEÇÃO DE DADOS. **VAZAMENTO DE DADOS SENSÍVEIS. RESPONSABILIDADE OBJETIVA. DANO MORAL PRESUMIDO.** RECURSO CONHECIDO EM PARTE. DESPROVIMENTO.
> 1. Ação de obrigação de fazer c/c indenização por danos morais e materiais, da qual foi extraído o presente recurso especial, interposto em 28/6/2023 e concluso ao gabinete em 22/2/2024.
> 2. O propósito recursal é definir se, em contrato de seguro de vida, o vazamento de dados sensíveis do segurado gera: (a) dano moral presumido e (b) responsabilização objetiva da empresa seguradora.
> 3. Inexistência de negativa de prestação jurisdicional. Acórdão do Tribunal de origem devidamente fundamentado para solucionar integralmente a controvérsia submetida à sua apreciação.
> 4. Não há cerceamento de defesa nas hipóteses em que o julgador resolve a questão controvertida, de forma fundamentada, sem a produção da prova requerida pela parte, em virtude de considerar suficientes os elementos que integram os autos.
> 5. A matéria que não foi objeto de debate no acórdão recorrido, mesmo após a interposição de embargos declaratórios, não pode ser conhecida por meio de recurso especial. Súmula nº 211/STJ.
> 6. Cabe ao fornecedor o ônus de comprovar que cumpriu com seu dever de proteger dados pessoais do consumidor, sobretudo quando se tratam de dados sensíveis, nos termos do CDC (arts. 6º, VIII e 14, *caput* e §3º) e da LGPD (arts. 6º, X, 8º, §2º, 42, §2º e 48, §3º).
> 7. Há especial proteção legal aos chamados dados pessoais sensíveis: aqueles que, quando revelados, podem gerar algum tipo de discriminação, sobretudo os que incidem sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico" (art. 5º, II, da LGPD).
> 8. O tratamento de dados pessoais sensíveis observa requisitos significativamente mais rigorosos, sobretudo com a exigência, em regra, do consentimento específico e destacado do titular (art. 11 da LGPD).
> **9. Em contrato de seguro de vida, deve-se empreender um rigoroso esforço para a proteção dos dados pessoais, já que, para sua celebração, a seguradora, para a avaliação dos riscos, recebe dados sensíveis sobre aspectos pessoais, familiares, financeiros e de saúde do segurado.**
> **10. O vazamento de dados pessoais sensíveis fornecidos para a contratação de seguro de vida, por si só, submete o consumidor a riscos em diversos aspectos de sua vida, como em sua honra, imagem, intimidade, patrimônio, integridade física e segurança pessoal.**

[115] Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202400312927&dt_publicacao=17/02/2025. Acesso em: maio 2025.

> **11. Por isso, em seguro de vida, na hipótese de vazamento de dados sensíveis do segurado, verifica-se a responsabilização objetiva da seguradora e a caracterização de dano moral presumido.**
> 12. Conforme entendimento desta Corte, a revisão da compensação por danos morais só é viável em recurso especial quando o valor fixado for exorbitante ou ínfimo, o que não se constata no recurso sob julgamento.
> 13. Hipótese em que o acórdão recorrido, ao manter a responsabilização da seguradora, reconheceu que: i) houve vazamento de dados pessoais do consumidor; ii) tais dados são classificados como sensíveis, de modo a abranger informações fiscais, bancárias e sobre a saúde do consumidor; iii) há nexo de causalidade entre o vazamento de dados sensíveis do consumidor e falhas na prestação do serviço pela recorrente, que não atendeu a seu dever de garantir a proteção dos dados sensíveis do consumidor.
> 14. Recurso especial parcialmente conhecido e, nessa extensão, desprovido.
> (REsp n. 2.121.904 – SP, relatora ministra Nancy Andrighi, Terceira Turma, julgado em 11/2/2025, *DJEN* de 17/2/2025) (grifo nosso).

O Recurso Especial foi interposto pela Prudential Seguros do Brasil contra acórdão do TJ-SP que negou provimento à sua apelação e deu parcial provimento à apelação do segurado, para condená-la à indenização por dano moral presumido *(in re ipsa)*, decorrente de vazamento de dados sensíveis constantes em apólice de seguro de vida. Na origem, o pleito decorria de informação da própria seguradora, recebida pelo segurado por e-mail, sobre a ocorrência de um incidente de cibersegurança que teria permitido o vazamento de seus dados, incluídos de saúde e de filhos menores.

O recurso foi julgado em 11 de fevereiro de 2025, à unanimidade, pelos ministros Humberto Martins, Ricardo Villas Bôas Cueva, Moura Ribeiro e o desembargador convocado Carlos Cini Marchionatti, que seguiram o voto da relatora para conhecê-lo em parte e negar-lhe provimento, mantendo a condenação imposta pelo Tribunal de Justiça.

A ministra Nancy iniciou seu voto consignando que o contrato individual de seguro de vida é regido pelo CDC, pois caracterizado pela hipossuficiência do consumidor, citando precedente da Corte (AgInt no AREsp nº 2.074.830 – RS, da Quarta Turma).

Abordou a vulnerabilidade a que os consumidores, na qualidade de titulares de dados, estão submetidos, e a importância da resguarda de seus direitos, seja por mandamento constitucional (art. 5º, XXXIII, e 170, V, da CF), seja por proteção legal do CDC (arts. 4º, I, 8º, 14, § 1º e 43) e da LGPD (arts. 2º, 6º, I, II e VI), tudo para repisar o dever de segurança esperado do agente de tratamento, previsto tanto no art. 14, § 1º, do diploma consumerista, como no art. 44 da lei de proteção de dados.

Na sequência, fez distinção entre dados comuns e sensíveis (definidos nos art. 5º, I e II, da LGPD), argumentando serem esses requisitos mais rigorosos de tratamento e consentimento (art. 11 e 14, § 1º, no caso de crianças e adolescentes), e citou o disposto no AREsp nº 2.130.619

– SP – debatido no item 3.1 – no qual o dano moral presumido, embora não exista para vazamentos de dados comuns, aplicar-se-ia aos vazamentos de dados sensíveis.

Mencionou, ainda, o entendimento da Terceira Turma assentado no REsp nº 2.115.461 – SP[116], que impõe dano moral *in re ipsa* em caso de disponibilização a terceiros de banco de dados pessoais sem anuência do titular, ainda que os dados não sejam sensíveis.

Ponderou que a seguradora, embora tenha argumentado "ter adotado protocolos de segurança", não comprovou excludente de responsabilidade prevista no art. 43 da LGPD (culpa exclusiva de terceiro), não conseguindo, portanto, afastar o nexo de causalidade entre o vazamento dos dados sensíveis e a falha na prestação do serviço, o que gera o dever de indenizar.

Por fim, não houve dúvida quanto à opção pelo regime de responsabilidade objetiva, dada pela interpretação conjunta do art. 14 do CDC e dos art. 42 e 45 da LGPD, regime esse expressamente indicado no cabeçalho da ementa. Nesse ponto, o acórdão citou o entendimento assentado no REsp nº 2.077.278 – SP – aqui estudado no item 3.2 –, de que é objetiva a responsabilidade do fornecedor por transferência a terceiros de informações sem o consentimento do consumidor, pugnando pela confirmação dessa tese, ainda mais nas hipóteses de dados sensíveis.

A reiteração desse posicionamento pela responsabilidade objetiva, inclusive com a menção expressa entre os julgamentos citados, demonstra mais claramente a confirmação de tal entendimento naquela Turma.

[116] Relatado pela ministra Nancy Andrighi e julgado em outubro de 2024, conjuntamente com o REsp nº 2.133.261 – SP, tratou do *credit scoring*, objeto do Tema Repetitivo 710 (no qual não se pode exigir o prévio e expresso consentimento do consumidor avaliado, pois não constitui um cadastro ou banco de dados, mas um modelo estatístico). Nesses dois casos, contudo, o STJ fez distinção ao previsto no Repetitivo, pois envolviam compartilhamento de dados (informações cadastrais e de adimplemento) a terceiros consulentes, e não a outros bancos de dados, o que gera, pela responsabilidade objetiva, dano moral presumido. A fundamentação foi toda baseada na Lei nº 12.414/2011 (Lei do Cadastro Positivo), com referências à dispositivos da LGPD.

3.6 Outros julgados

Quanto aos processos em que o tema responsabilização de agentes de tratamento pela ótica da Lei Geral de Proteção de Dados é central, a presente pesquisa, com base no banco de jurisprudências do próprio Tribunal e na análise do estudo IDP-JusBrasil 2023-2024, localizou apenas os casos estudados no tópico anterior. Contudo, são dignos de atenção outros dois julgamentos em que, mesmo não estando a LGPD no centro, o assunto é trazido à discussão.

3.6.1 REsp nº 1.995.458 – SP

É muito apropriada a análise do Recurso Especial nº 1.995.458 – SP, julgado em 9 de agosto de 2022 pela Terceira Turma, relatado pela ministra Nancy Andrighi e assim ementado[117]:

> PROCESSUAL CIVIL. RECURSO ESPECIAL. AÇÃO DECLARATÓRIA DE INEXIBILIDADE DE DÉBITO. CONSUMIDOR. GOLPE DO MOTOBOY. RESPONSABILIDADE CIVIL. USO DE CARTÃO E SENHA. DEVER DE SEGURANÇA. FALHA NA PRESTAÇÃO DE SERVIÇO.
> 1. Ação declaratória de inexigibilidade de débito.
> 2. Recurso especial interposto em 16/08/2021. Concluso ao gabinete em 25/04/2022.
> 3. O propósito recursal consiste em perquirir se existe falha na prestação do serviço bancário quando o correntista é vítima do golpe do motoboy.
> 4. Ainda que produtos e serviços possam oferecer riscos, estes não podem ser excessivos ou potencializados por falhas na atividade econômica desenvolvida pelo fornecedor.
> 5. Se as transações contestadas forem feitas com o cartão original e mediante uso de senha pessoal do correntista, passa a ser do consumidor a incumbência de comprovar que a instituição financeira agiu com negligência, imprudência ou imperícia ao efetivar a entrega de numerário a terceiros. Precedentes.
> 6. A jurisprudência deste STJ consigna que o fato de as compras terem sido realizadas no lapso existente entre o furto e a comunicação ao banco não afasta a responsabilidade da instituição financeira. Precedentes.
> 7. Cabe às administradoras, em parceria com o restante da cadeia de fornecedores do serviço (proprietárias das bandeiras, adquirentes e estabelecimentos comerciais), a verificação da idoneidade das compras realizadas com cartões magnéticos, utilizando-se de meios que dificultem ou impossibilitem fraudes e transações realizadas por estranhos em nome de seus clientes, independentemente de qualquer ato do consumidor, tenha ou não ocorrido roubo ou furto. Precedentes.
> **8. A vulnerabilidade do sistema bancário, que admite operações totalmente atípicas em relação ao padrão de consumo dos consumidores,**

[117] Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202200971883&dt_publicacao=18/08/2022. Acesso em: jul. 2024.

> **viola o dever de segurança que cabe às instituições financeiras e, por conseguinte, incorre em falha da prestação de serviço.**
> 9. Para a ocorrência do evento danoso, isto é, o êxito do estelionato, necessária concorrência de causas: (i) por parte do consumidor, ao fornecer o cartão magnético e a senha pessoal ao estelionatário, bem como (ii) por parte do banco, ao violar o seu dever de segurança por não criar mecanismos que obstem transações bancárias com aparência de ilegalidade por destoarem do perfil de compra do consumidor.
> 10. Na hipótese, contudo, verifica-se que o consumidor é pessoa idosa, razão pela qual a imputação de responsabilidade há de ser feita sob as luzes do Estatuto do Idoso e da Convenção Interamericana sobre a Proteção dos Direitos Humanos dos Idosos, sempre considerando a sua peculiar situação de consumidor hipervulnerável.
> 11. Recurso especial provido. (REsp n. 1.995.458 – SP, relatora ministra Nancy Andrighi, Terceira Turma, julgado em 9/8/2022, *DJe* de 18/8/2022) (grifo nosso).

O episódio envolveu responsabilização na relação de consumo, requerida por um correntista contra seu banco, diante do chamado "golpe do motoboy"[118] (golpe de engenharia

[118] Reitere-se a referência ao REsp nº 2.015.732 – SP, igualmente relatado pela ministra Nancy, julgado posteriormente, em 20/6/2023, que versou sobre o mesmo assunto ("golpe do motoboy") para chegar à mesma conclusão, em confirmação de posicionamento da Terceira Turma pelo regime de responsabilidade objetiva, como se observa de sua ementa: PROCESSUAL CIVIL. RECURSO ESPECIAL. AÇÃO DE DECLARATÓRIA DE INEXIGIBILIDADE DE DÉBITOS POR DANOS MORAIS E MATERIAIS. CONSUMIDOR. GOLPE DO MOTOBOY. RESPONSABILIDADE CIVIL. USO DE CARTÃO E SENHA. DEVER DE SEGURANÇA. FALHA NA PRESTAÇÃO DE SERVIÇO. DANOS MORAIS. CONFIGURADOS. 1. Ação declaratória de inexigibilidade de débitos cumulada com indenização por danos morais e materiais, ajuizada em 05/11/2020, da qual foi extraído o presente recurso especial, interposto em 31/01/2022 e concluso ao gabinete em 14/12/2022. 2. O propósito recursal consiste em decidir se, quando o correntista é vítima do golpe do motoboy, (I) o banco responde objetivamente pela falha na prestação do serviço bancário e se (II) é cabível a indenização por danos morais. 3. Se comprovada a hipótese de vazamento de dados por culpa da instituição financeira, será dela, em regra, a responsabilidade pela reparação integral de eventuais danos. Do contrário, **naquilo que entende esta Terceira Turma, inexistindo elementos objetivos que comprovem esse nexo causal, não há que se falar em responsabilidade das instituições financeiras pelo vazamento de dados utilizados por estelionatários para a aplicação de golpes de engenharia social**. 4. O cartão magnético e a respectiva senha são de uso exclusivo do correntista, que deve tomar as devidas cautelas para impedir que terceiros tenham acesso a eles. Se as transações contestadas forem feitas com o cartão original e mediante uso de senha pessoal, passa a ser do consumidor a incumbência de comprovar que a instituição financeira agiu com negligência, imprudência ou imperícia ao efetivar a entrega de numerário a terceiros. Precedentes 5. **Nos termos da jurisprudência deste STJ, cabe às administradoras, em parceria com o restante da cadeia de fornecedores do serviço (proprietárias das bandeiras, adquirentes e estabelecimentos comerciais), a verificação da idoneidade das compras realizadas com cartões magnéticos, utilizando-se de meios que dificultem ou impossibilitem fraudes e transações realizadas por estranhos em nome de seus clientes, independentemente de qualquer ato do consumidor, tenha ou não ocorrido roubo ou furto**. 6. **O dever de adotar mecanismos que obstem operações totalmente atípicas em relação ao padrão de consumo dos consumidores enseja a responsabilidade do prestador de serviços**, que responderá pelo risco da atividade, pois a instituição financeira precisa se precaver a fim de evitar golpes desta natureza, cada vez mais frequentes no país. 7. Quando se trata de responsabilidade objetiva, a possibilidade de redução do montante indenizatório em face do grau de culpa do agente deve ser interpretada restritivamente, devendo ser admitida apenas naquelas hipóteses em que o agente, por meio de sua conduta, assume e potencializa, conscientemente, o risco de vir a sofrer danos ao contratar um serviço que seja perigoso. 8. Não é razoável afirmar que o consumidor assumiu conscientemente um risco ao digitar a senha pessoal no teclado de seu telefone depois de ouvir a confirmação de todos os seus dados pessoais e ao destruir parcialmente o seu cartão antes de entregá-lo a terceiro que dizia ser preposto do banco, porquanto agiu em razão da expectativa de confiança que detinha nos sistemas de segurança da instituição financeira. 9. **Entende a Terceira Turma deste STJ que o banco deve responder objetivamente pelo dano sofrido pelas vítimas do golpe do motoboy quando restar**

social), em que a vítima recebe telefonema de estelionatário, fornece sua senha, falso motorista colhe seu cartão e realiza compras em seu nome.

Embora a LGPD não seja citada na ementa (nem seja utilizada como fundamento central do julgamento), o acórdão abordou episódio de vazamento de dados pessoais, com o foco na responsabilização do banco como agente de tratamento. Os trechos mais relevantes foram os seguintes:

> 2.1 O vazamento de dados pessoais utilizados no estelionato:
>
> 16. Não obstante essa triste realidade, para sustentar **o nexo causal entre a atuação dos estelionatários e o vazamento de dados pessoais do sistema bancário no intuito de imputar responsabilidade à instituição financeira pelo vazamento de dados**, seria preciso superar que (i) não se sabe com exatidão quais são as informações que os estelionatários detinham para efetuar o golpe e que (ii) a origem da obtenção de dados pessoais não é necessariamente a instituição financeira, pois os dados pessoais são passíveis de serem adquiridos em diversos meios.
> 17. Conforme ensina a "Cartilha de Segurança para Internet: Fascículo vazamento de dados", da Autoridade Nacional de Proteção de Dados (Disponível em: https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf), **vazamentos de dados (data leak) ocorrem quando dados são indevidamente acessados, coletados e divulgados na Internet, ou repassados a terceiros**. A origem do vazamento pode ser o furto de dados por atacantes e códigos maliciosos que exploram vulnerabilidades em sistemas; o acesso a contas de usuários; as senhas fracas ou vazadas; a ação de funcionários ou ex-funcionários que coletam dados dos sistemas da empresa e os repassam a terceiros; o furto de equipamentos que contenham dados sigilosos; os erros ou a negligência de funcionários, como descartar mídias (discos e pen drives) sem os devidos cuidados, e outros. [...]
> 19. A dificuldade em saber a origem do vazamento é tamanha que a LGPD estabeleceu no artigo 55-J, como atribuição da Autoridade Nacional de Proteção de Dados (ANPD) a incumbência de "fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação" (inciso IV), bem como "realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do *caput* deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento" (inciso XVI).
> **20. Como ensina a jurista Laura Schertel Mendes, a Lei Geral de Proteção de Dados inaugura um modelo ex-ante de proteção de dados** (MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: os dois lados de uma mesma moeda. Internet & Regulação. coords.: Laura Schertel Mendes, Sérgio Garcia Alves, Danilo Doneda. – São Paulo: Saraiva Educação, 2021.) Nesta perspectiva, **o legislador criou uma série de deveres**

---

demonstrada a falha de sua prestação de serviço, por ter admitido transações que fogem do padrão de consumo do correntista. 10. Se demonstrada a existência de falha na prestação do serviço bancário, mesmo que causada por terceiro, e afastada a hipótese de culpa exclusiva da vítima, cabível a indenização por dano extrapatrimonial, fruto da exposição sofrida em nível excedente ao socialmente tolerável. 11. Recurso especial conhecido e provido. (REsp nº 2.015.732 – SP, relatora ministra Nancy Andrighi, Terceira Turma, julgado em 20/6/2023, *DJe* de 26/6/2023) (grifo nosso).

> **de conduta que impactarão na mensuração da responsabilidade dos agentes em eventual vazamento de dados.**
>
> 21. Assim, a Lei Geral de Proteção de Dados destina-se a indicar a responsabilidade dos agentes que detêm dados pessoais que foram vazados, **importando as medidas adotadas para evitar este vazamento, conforme estabelecidos nos artigos 43 e 44, da LGPD.**
> 22. Notório, portanto, **que a fim de imputar a responsabilidade das instituições financeiras no que tange ao vazamento de dados pessoais,** deve-se garantir que a **origem do vazamento foi o sistema bancário, bem como observar se as devidas medidas protetivas quanto aos dados pessoais sob domínio da instituição financeira foram adotadas** (grifo nosso).

Com elementos do voto-vista do ministro Ricardo Villas Bôas Cueva, o recurso foi julgado à unanimidade para dar provimento ao apelo e declarar a inexigibilidade de todas as transações não reconhecidas pelo consumidor, contando com os votos dos ministros Paulo de Tarso Sanseverino e Moura Ribeiro, pois impedido o ministro Marco Aurélio Bellizze.

O regime de responsabilidade civil ficou claramente indicado como sendo o objetivo[119], "exceto quando demonstrar a culpa exclusiva do consumidor ou de terceiros, naquilo que determina o art. 14 § 3º, II, do CDC", com possibilidade de aplicação da conduta concorrente entre autor e vítima (Precedentes: REsp nº 1.307.032/PR, Quarta Turma, *DJe* 1/8/2013, e REsp nº 712.591 – RS, Terceira Turma, *DJe* de 4/12/2006). A novidade foi a menção à teoria *ex-ante*, inaugurada pela LGPD e ensinada pela professora Laura Schertel Mendes, segundo a qual a mensuração da responsabilidade será determinada pelo atendimento (ou não) dos deveres de conduta de segurança do agente de tratamento[120].

O acórdão deixou clara a importância da criação e do constante aprimoramento de medidas a serem adotadas pelas instituições financeiras, em parceria com a cadeia de fornecedores (bandeiras, adquirentes e estabelecimentos comerciais), para evitar vazamentos e impedir transações com aparente ilegalidade, que destoem completamente do perfil do consumidor[121], como ocorreu na espécie, representando falha na prestação do serviço. Nesse ponto, os arts. 43 e 44 da LGPD (que tratam, respectivamente, sobre excludente de responsabilidade e tratamento irregular) foram lembrados.

---

[119] A Súmula 479/STJ ("As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias") também é memorada.

[120] Quanto às circunstâncias de responsabilização, por se tratar de consumidor idoso, o acórdão considera a necessidade de imputação à luz do Estatuto do Idoso e da Convenção Interamericana sobre a Proteção do Direitos Humanos dos Idosos (consumidor hipervulnerável).

[121] Diversas transações de altos valores em poucos minutos. No caso, fica consignado que, na esteira da jurisprudência do STJ, o fato de as compras terem sido realizadas no lapso temporal entre o furto e a comunicação ao banco não afasta a responsabilidade deste.

Outro ponto de destaque foi o nexo de causalidade entre a atuação dos estelionatários e o vazamento, indicado como elemento intrínseco à imputação da responsabilidade dos bancos, mais um dado a corroborar a opção pelo regime objetivo. Para a Terceira Turma, o nexo será comprovado pela identificação da forma de obtenção e dos tipos de dados em poder dos criminosos.

Por fim, quanto ao ônus da culpa, restou assentada a necessidade do dever de cautela do correntista no que se refere à senha pessoal e uso do cartão físico, de modo que se as transações indevidas forem feitas com ambos (senha e cartão), ainda que não espontânea, é dele consumidor a incumbência de comprovação de negligência, imprudência ou imperícia do banco, sob pena da aplicação da excludente de culpa exclusiva do consumidor ou de terceiro[122].

Considera-se que esse julgamento, exarado em agosto de 2022, possa ter servido como base para os Recursos Especiais abordados no tópico anterior (nºs 2.077.278 – SP, nº 2.092.096 – SP, nº 2.147.374 – SP e nº 2.121.904 –SP), proferidos entre outubro de 2023 e fevereiro de 2025, de modo à estabilizar a jurisprudência pela responsabilidade objetiva dos agentes de tratamento nos incidentes de tratamento em matéria consumerista.

[122] Citaram-se os precedentes REsp nº 1.633.785 – SP, Terceira Turma, *DJe* 30/10/2017 e AgInt no REsp nº 1914255 – AL, Terceira Turma, *DJe* 13/05/2021.

3.6.2 AREsp nº 2.311.731 – RS

Um último caso merece deferência. Trata-se do Agravo em Recurso Especial nº 2.311.731 – RS[123], em que a relatora, ministra Isabel Gallotti, componente da Quarta Turma, proferiu decisão monocrática em 24 de abril de 2023, posicionando-se sobre responsabilização das instituições financeiras em caso de vazamento de dados ocorrido mediante fraude, como se vê do seguinte trecho:

> Também não vejo como prosperar o recurso da parte agravante sob argumento de que há violação ao art. 46 da Lei n. 13.709/2018, em razão da falha na prestação dos serviços bancários, **já que a fraude perpetrada em telefone por agentes criminosos teria sido possibilitada em razão de eventual vazamento de dados da parte agravante.**
> Segundo a parte agravante, os fatos imputados deveriam incumbir à parte agravada, "que deveria demonstrar a inexistência de falhas, quais teriam sido as tentativas seguras de brecar o acesso e invasão de *rackers*, que não houve providências por parte da recorrente" (fl. 225 e-STJ).
> Alega, contudo, que a parte agravante "comprovou a comunicação à instituição financeira, a lavratura do BO (que, inicialmente, foi sugerido pelo próprio recorrido) e todas as outras medidas que estavam a seu alcance" (fl. 225 e-STJ).
> Por isso, afirma que há evidente falha na prestação do serviço bancário, **"no sentido de o recorrido não ter desconfiado e, consequentemente, barrado a ação criminosa"** (fl. 227 e-STJ).
> Com efeito, de fato, é entendimento pacífico desta Corte de que "as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias" (Súmula n. 479 do STJ). [...]
> Nos termos, contudo, do art. 14, §3º, II, do Código de Defesa do Consumidor, **a responsabilidade do fornecedor pelo fato do serviço pode ser afastada quando a culpa do consumidor ou de terceiro for exclusiva** (REsps 1.199.782/PR e 1.197.929/PR, Rel. Ministro Luis Felipe Salomão, Segunda Seção, julgados em 24/8/2011, *DJe* 12/9/2011). [...]
> Na hipótese dos autos, o Tribunal de origem afastou a responsabilidade da instituição financeira-agravada **por considerar que houve culpa exclusiva da vítima agravante ao fornecer senhas e dados pessoais no telefone, sem cautela suficiente para verificar que não se tratava de instituição financeira, mas sim de terceiro fraudador.** [...]
> Desta feita, considerando **que era obrigação da correntista, ora autora agravante, zelar pela guarda do código de cartão de segurança e sigilo da senha de acesso à sua conta, os quais foram fornecidos a terceiro fraudador, restam caracterizadas a culpa exclusiva da vítima**, nos moldes do art. 14, §3º, II, do Código de Defesa do Consumidor. [...] (grifo nosso).

[123] Disponível em: https://processo.stj.jus.br/processo/dj/documento/mediado/?tipo_documento=documento&componente=MON&sequencial=185457766&num_registro=202300658386&data=20230503&tipo=0. Acesso em: jul. 2024.

O caso guarda semelhanças com o do tópico anterior, na medida em que também envolveu correntista pleiteando indenização por danos materiais em razão de fraude, constituída por transferência ao fraudador, após ligação telefônica e acesso ao aplicativo do banco no celular.

O único artigo da LGPD citado foi o 46, que obriga os agentes de tratamento a adotarem medidas de segurança aptas à proteção dos dados pessoais. O dispositivo foi utilizado pela recorrente para embasar seu pedido, ao fundamento de que a instituição financeira deveria ter desconfiado da transação atípica, brecado o acesso e impedido a ação criminosa.

Contudo, a ministra entendeu que houve culpa exclusiva da vítima ao fornecer senhas e dados pessoais por telefone, sem a cautela de verificar não se tratar de ligação do banco[124]. Desse modo, consignou o dever do correntista de zelar pela guarda e sigilo de sua senha pessoal e do código de segurança (constante no cartão físico) e, aplicando a excludente de responsabilidade de culpa exclusiva da vítima, prevista no art. 14, § 3º, II, do CDC, negou provimento ao Recurso Especial.

Houve breve consideração sobre a inversão do ônus da prova do dano, requerida pelo correntista, porém negada pela magistrada, em sintonia com o Tribunal de origem, pela sua desnecessidade diante da inexistência de falha na prestação do serviço.

Por fim, quanto ao regime de responsabilização, a exemplo do REsp nº 2.077.278 – SP e REsp nº 1.995.458 – SP, houve explícita menção ao de natureza objetiva, primeiro para lembrar o disposto na Súmula nº 479 ("As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias") e, depois, para destacar trecho do acórdão recorrido, no sentido de que "não se pode confundir a responsabilidade civil objetiva com a integral, havendo expressa disposição legal de afastamento daquela quando se está diante de quebra de nexo causal entre a ação ou omissão do fornecedor e o prejuízo experimentado, nas hipóteses do mesmo art. 14, § 3º, inciso II".

Considerando que a ministra Gallotti compõe a Quarta Turma do Tribunal, entendeu-se ser esta decisão a primeira a expor a visão daquele órgão colegiado em matéria de responsabilidade civil do agente de tratamento de dados[125].

---

[124] Neste mesmo sentido havia se posicionado a Terceira Turma no julgamento do REsp nº 1.995.458 – SP.

[125] Poder-se-ia incluir o AgInt nos EDcl no REsp 2129504 / SP, muito recente, julgado em novembro de 2024 e relatado pelo ministro Raul Araújo, que envolveu pedido de responsabilização contra o Serasa por suposta disponibilização de dados sensíveis (CPF e histórico de crédito) na plataforma de consulta. Ali, a Quarta Turma, por unanimidade, manteve a decisão do Tribunal *a quo*, por entender que as informações são públicas, que os dados não são sensíveis e que o assunto já está sedimentado no Tribunal por meio do Tema Repetitivo 710.

3.7 Primeiros impactos

Este trabalho reforça sua utilidade prática, na medida em que fornece, ainda que superficialmente, indicativos dos primeiros impactos das decisões estudadas do Superior Tribunal de Justiça no âmbito estadual, tendo como parâmetro os Tribunais de Justiça dos Estados de São Paulo e do Paraná. Isso porque, embora essas decisões não tenham (em tese) efeito vinculante, imprescindível aferir se as instâncias inferiores estão (ou não) utilizando-as em suas fundamentações e, assim, contribuindo para o processo de consolidação da jurisprudência sobre o tema estudado[126].

3.7.1 AREsp nº 2.130.619 – SP

O AREsp nº 2.130.619 – SP, julgado em março de 2023, vem sendo referenciado em decisões de 2º grau, inclusive prolatadas ao longo daquele ano, como se observa nos seguintes julgados dos Tribunais de Justiça do Paraná e de São Paulo, listados em ordem cronológica de julgamento (Mendes; Fujimoto, 2004, p. 46; 90; 10):

> **Tribunal de Justiça do Paraná (TJ-PR)[127]:**
>
> **Recurso Inominado nº 0001164-79.2022.8.16.0075**
>
> **Terceira Turma Recursal**
>
> **Relatora:** Adriana de Lourdes Simette
>
> **Data de julgamento:** 19/6/2023
>
> **Ementa:** Recurso inominado. Ação de indenização por danos morais. Bancário. Contratação de empréstimo consignado através de agente intermediador. Vazamento de dados pessoais do autor. Fraude em outras instituições bancárias. Ausência de comprovação de que a instituição financeira ré divulgou informações sensíveis do autor. Mais de uma empresa na cadeia de tratamento de dados. Ausência de demonstração de ato ilícito pela parte ré. Autor não se desincumbiu de seu ônus probatório (art. 373, I, CPC). Dano moral não configurado. Sentença mantida por seus próprios

[126] Nessa parte do capítulo, centrou-se apenas nos acórdãos constantes dos itens 3.1, 3.2, 3.3, 3.4 e 3.5, pelo grau de relevância. De todo modo, quanto ao REsp nº 1.995.458 – SP (do item 3.6.1), localizou-se o acórdão do Recurso Cível Nº 5019290-63.2022.8.24.0045, do Tribunal de Justiça de Santa Catarina, julgado em fevereiro de 2024, que versou sobre pedido indenizatório decorrente de golpe "do falso colaborador" sofrido por correntista bancário, no qual o Banco foi responsabilizado em julgamento que utilizou o referido Recurso Especial como fundamento. Já no que tange ao AREsp nº 2.311.731 – RS (do item 3.6.2), localizou-se apenas uma sentença de 1º grau, de Conceição do Araguaia-PA, constante do processo nº 0800429-76.2024.8.14.0017, prolatada em junho de 2024, em caso que envolveu fornecimento de senha de correntista a criminoso no interior de agência bancária. Tal conduta foi classificada como culpa exclusiva da vítima, afastando a responsabilidade do banco, com base em jurisprudência do STJ, incluída a do AREsp nº 2.311.731 – RS.

[127] Disponível em: https://portal.tjpr.jus.br/jurisprudencia/j/2100000023729281/Ac%C3%B3rd%C3%A3o-0001164-79.2022.8.16.0075. Acesso em: abr. 2025.

> fundamentos. Aplicação do art. 46 da Lei Federal nº 9.099 /95. Recurso conhecido e não provido.

O recurso insurgiu-se contra sentença que julgou procedente ação de indenização por danos morais movida por contratante de empréstimo consignado com o banco Cetelem. No pleito, o autor alegou que houve vazamento de dados pessoais, tendo em vista que tomou conhecimento da existência de dois outros empréstimos não contratados com outras instituições financeiras.

A Turma Recursal do TJ-PR entendeu que não houve a devida comprovação da contratação do empréstimo (via canal oficial) e, mesmo tendo havido, a própria natureza do dano não é *in re ipsa,* conforme decisão recente do STJ, qual seja o AREsp nº 2.130.619 – SP.

Para o tribunal paranaense, "ainda que se possam presumir aborrecimentos sofridos em razão de fraude na contratação dos empréstimos consignados, inexiste prova inequívoca da ocorrência de ato ilícito por parte da ré, também inexistindo, consequentemente, o dever de indenizar".

> **Tribunal de Justiça de São Paulo (TJ-SP)[128]:**
>
> **Apelação Cível nº 1008710-70.2021.8.26.0320**
>
> **25ª Câmara de Direito Privado**
>
> **Relator:** Desembargador Almeida Sampaio
>
> **Data de julgamento:** 10/8/2023
>
> **Ementa:** APELAÇÃO CÍVEL – INDENIZAÇÃO – DANO MORAL – VAZAMENTO DE DADOS POR AÇÃO DE TERCEIROS – Ausência de prova do prejuízo – Dados não considerados sensíveis por definição legal – Apelo provido para julgar improcedente a ação.

O autor contratou seguro de vida com a seguradora Prudential, que o informou terem seus dados sido acessados por terceiros. O segurado pleiteou judicialmente indenização por dano moral, alegando ter tido ciência de que estelionatários estavam utilizando os referidos dados para compras.

Na defesa, a ré/apelada requereu a aplicação exclusiva da LGPD (e não do CDC) e, por conseguinte, do regime de responsabilidade subjetiva, com demonstração de culpa, o que

[128] Disponível em: https://esaj.tjsp.jus.br/cposg/show.do?processo.codigo=RI007BMZX0000#. Acesso em: abr. 2025.

entendia não ter ocorrido. Ademais, afirmou inexistir nexo de causalidade e prova do dano moral sofrido.

O tribunal paulista deu provimento ao apelo ao fundamento de que os dados vazados não eram sensíveis, estes sim merecedores de proteção especial por imposição do art. 11 da LGPD, citando explicitamente o AREsp nº 2.130.619 – SP e concluindo, quanto ao dano, não ter o apelante comprovado os prejuízos experimentados com a tentativa de estelionato.

Inconformado, o autor opôs embargos declaratórios, rejeitados pelo TJ-SP, que confirmou terem os vazamentos gerado meros aborrecimentos, não passíveis de responsabilização, pelo que interpôs recurso especial, inadmitido, por sua vez objeto de agravo, não conhecido[129].

Percebe-se que no mesmo ano de 2023, já surgiram decisões que utilizaram o julgamento do AREsp nº 2.130.619 – SP para denegar pleitos indenizatórios envolvendo dados pessoais comuns (não sensíveis), não comprovados pelos titulares de dados/consumidores.

Para o estudo IDP-Brasil, a replicação dos efeitos dessa decisão nos tribunais estaduais se configura como uma jurisprudência em formação, e releva uma tendência preocupante, uma vez que, ao vincular a possibilidade de reparação apenas ao vazamento de dados sensíveis ou íntimos, parece desconsiderar o paradigma da proteção de dados inaugurado com a LGPD, segundo o qual não existe dado pessoal insignificante, merecendo proteção qualquer dado pessoal, seja ele sensível ou não” (Mendes; Fujimoto, 2024, p. 108).

[129] Movimentação disponível em: https://cpe.web.stj.jus.br/#/processo/202401943576. Acesso em: abr. 2025.

3.7.2 REsp nº 2.077.278 – SP

Localizou-se julgamento do tribunal paulista aplicando o entendimento do REsp nº 2.077.278 – SP, como se observa do seguinte acórdão:

> **Tribunal de Justiça do Estado de São Paulo (TJ-SP):**[130]
>
> **Apelação nº 1013854-35.2023.8.26.0100**
>
> **14ª Câmara de Direito Privado**
>
> **Relator:** Des. Luis Fernando Camargo De Barros
>
> **Data de julgamento:** 24/1/2024.
>
> **Ementa:** Apelação. Declaratória e indenizatória. Parcial procedência. Apelo do autor. Cartão de crédito. Vazamento de dados pessoais e de consumo. Emissão de fatura mediante fraude. Alteração do código de barras. Cobranças discriminadas na fatura esperadas pelo consumidor. Pagamento de boa-fé. Falha na prestação do serviço relativamente à segurança das informações do consumidor. Responsabilidade objetiva. Súmula nº 479 do STJ e art. 14 do CDC. Danos morais evidenciados. Descumprimento do dever de pronta resolução do acidente de consumo. Desvio produtivo. Danos morais evidenciados em consonância ao REsp nº 2.077.278. Apontamento perante o Sistema de Informação de Crédito do Banco Central SCR. Inscrição que não se equipara às inserções desabonadoras em cadastros de inadimplentes. Recurso, do autor, parcialmente provido.

Tratou-se de ação indenizatória de cliente da Portoseg Financeira vítima de golpe da falsa fatura de cartão de crédito, com código de barras alterado. O fato gerou sua inadimplência com o banco e inclusão do nome em cadastro de proteção ao crédito. A sentença julgou procedente o pedido apenas para reconhecer a inexigibilidade do débito, sem, entretanto, condenar o banco à reparação por dano moral.

Inconformado, o consumidor apelou ao tribunal paulista aduzindo que a fraude decorreu de vazamento de dados e que graves danos foram gerados (bloqueio de cartão, ligações de cobranças indevidas, restrição de crédito etc.).

---

130 Disponível em: https://esaj.tjsp.jus.br/pastadigital/abrirPastaProcessoDigital.do?origemDocumento=P&nuProcesso=1013854-35.2023.8.26.0100&cdProcesso=RI007QNUC0000&cdForo=990&tpOrigem=2&flOrigem=S&nmAlias=SG5TJ&instanciaProcesso=SG&cdServico=190201&ticket=99QHsRpraNP3zaRWywOpBTbDmGLf%2FMwTyeWqRiDkbRjeBxdKdyk%2FYfy%2FDhiHd%2BmJiUx5wTeuh5Cn%2F5cOME%2F1pmCClIGJ4TaILNbJg1%2FleyZPrlfAaS0eLZjx6Zjg5skxSSa%2FaaSwdKVZgUo3VY5mVJXav8I0xIIxnkJKU8XBAhT1vZtkMsMoTCfZC2FQSIsdpu5I0oERzG8vZnF6zX%2B3tbWf0lgJ5KvdiRmS8I88YzUgGjXBWOcKra1PGlypZB9oTh9iQscDPddDS2TXZNz5czLm72Pep3dAK0DgAz9rGVLNHMpEZaJHRiQYETkAbmTR6CDVwtspJ%2FFaedoWNQ46Oa5fx8baeI%2BOs%2BG3%2BET6FUjnKRw3Oin0KsXCbHoTfutuGp4%2BM8gQ7FfQp8hK8%2F%2FFORS8xzQ2Pqoln9j3n%2BGS8qUQsbyV2VDcCDpKxGeeQVw4bG6sVmk8eWUhLOO9mCkoeBvieTmN5MmhIGQib0KPYWyq8QSIkNpi9oMEWuJSJFAIr7kgmyhxadPoe%2BNY4ISTpw%3D%3D. Acesso em: abr. 2025.

A Corte embasou sua decisão basicamente pelo teor do REsp nº 2.077.278 – SP, com ementa integralmente transcrita, para registrar que "é fato incontroverso que o autor foi vítima de fraude na emissão de boleto de fatura de cartão de crédito e, assim, o banco deverá suportar as consequências decorrentes do fortuito interno, consistente no vazamento de dados pessoais e bancários do cliente, nos termos da Súmula 479, do STJ e do art. 14, do CDC".

A vulnerabilidade do consumidor (que nem sequer teve resposta da instituição pela via administrativa), somada à circunstância do envolvimento de dados sensíveis, contribuiu para o provimento do recurso e condenação na reparação moral.

Registre-se que não houve menção à LGPD, mas tão somente ao CDC (arts. 6, VIII – inversão do ônus da prova – e art. 14 – reparação de dano por defeito na prestação do serviço).

3.7.3 REsp nº 2.092.096 – SP

Quanto ao REsp nº 2.092.096 – SP, não foram localizadas decisões no TJ-SP e TJ-PR que o utilizaram como fundamento.

3.7.4 REsp nº 2.147.374 – SP

Também não se identificaram decisões estaduais paulistas ou paranaenses que tenham utilizado o REsp nº 2.147.374 – SP como referência ou fundamento.

3.7.5 REsp nº 2.121.904 – SP

Embora o julgamento do REsp nº 2.121.904 – SP tenha ocorrido há pouco mais de três meses, localizou-se o recentíssimo acórdão do TRF da 4ª Região (Seção Judiciária do Paraná) nele fundamentado:

> **Tribunal Regional Federal da 4ª Região**[131]
> **Recurso Cível nº 5009402-80.2024.4.04.7000/PR**
> **Relator:** Juiz Federal Gerson Luiz Rocha
> **Data de julgamento:** 2/6//2025

[131] Disponível em: file:///C:/Users/PC/Downloads/Ac%C3%B3rd%C3%A3o%20-%20RECURSO%20C%C3%8DVEL%20n%C2%BA%205009402-80.2024.4.04.7000%20-%20PR.pdf. Acesso em: jun. 2025.

> **Ementa**: DIREITO ADMINISTRATIVO. RESPONSABILIDADE CIVIL DO ESTADO. VAZAMENTO DE DADOS PESSOAIS. SALÁRIO-MATERNIDADE. DANO MORAL PRESUMIDO. NEGA PROVIMENTO AO RECURSO.

O recurso foi interposto pelo Instituto Nacional do Seguro Social (INSS) contra sentença que o condenou ao pagamento de indenização por danos morais, em razão do vazamento de dados relacionados ao pedido administrativo de salário-maternidade da autora.

Evocando a responsabilidade civil do Estado (art. 37, § 6º, da CF), o direito constitucional à proteção de dados (EC nº 115/2022) e a jurisprudência do STJ, no caso o entendimento firmado no REsp nº 2.121.904 – SP, no qual o vazamento de dado sensível gera dano moral presumido, o Tribunal negou provimento ao recurso, para manter a sentença de 1º grau e condenar o INSS a indenizar a autora em dano moral.

Convém ponderar que a localização desses julgados utilizou o critério metodológico de busca em dois Tribunais de Justiça com grande volume de ações (São Paulo e Paraná), realizada nos portais de jurisprudência nacional (a exemplo do JusBrasil) e nas próprias plataformas dos tribunais estaduais. Contudo, aleatoriamente, encontrou-se julgamentos de outros tribunais estaduais, confirmando a percepção de que a 2ª instância judicial brasileira está se valendo dos julgamentos do STJ aqui mencionados para basear suas fundamentações em casos que envolvem incidentes de segurança.

Encontrou-se maior prevalência de decisões apoiadas no AREsp nº 2.130.619 – SP (no caso, três decisões), julgado em março de 2023, pela (i) não responsabilização de incidentes envolvendo dados comuns e, (ii) impossibilidade de dano presumido em matéria de proteção de dados.

Não se pode, todavia, inferir que seja uma tendência, de vez que as demais decisões pesquisadas (REsp nº 2.077.278 – SP; REsp nº 2.092.096 – SP; REsp nº 2.147.374 – SP; REsp nº 2.121.904 – SP), que adotaram a responsabilidade objetiva como regra e focaram no dever de segurança do agente de tratamento, são mais recentes (exaradas do fim de 2023 ao início de 2025) e, naturalmente, devem gerar maiores impactos jurisprudenciais a partir de agora.

Quanto aos julgados estaduais localizados, ficou claro que as fundamentações dos desembargadores ainda estão muito amparadas apenas no Código de Defesa do Consumidor, com parcas menções aos dispositivos da Lei Geral de Proteção de Dados, retrato igualmente observado no *Relatório LGPD nos Tribunais*, do IDP-Jus Brasil.

No mesmo sentido, todos os julgamentos do STJ pesquisados (AREsp nº 2.130.619 – SP; REsp nº 2.077.278 – SP; REsp nº 2.092.096 – SP; REsp nº 2.147.374 – SP; REsp nº

2.121.904 – SP; REsp nº 1.995.458 – SP; e AREsp nº 2.311.731 – RS), ainda aqueles que utilizaram a responsabilização da LGPD como tema central (os cinco primeiros), não deixaram de fazer alusão ao CDC, especialmente ao art. 14 e seu §1º, que versam sobre o defeito na prestação do serviço e a segurança esperada pelo consumidor, fato que corrobora o entendimento de que ambas as legislações se complementam e não podem ser analisadas de forma dissociada.

No sistema de precedentes qualificados do STJ, não há, até o momento, Recursos Representativos de Controvérsias (RRCs), Recursos Repetitivos, Incidentes de Assunção de Competência (IACs), Incidentes de Resolução de Demanda Repetitiva (IRDRs), Súmulas ou quaisquer outros instrumentos de uniformização de jurisprudência que versem sobre responsabilidade civil no âmbito de incidentes de segurança na vigência da LGPD (desde de 2020), tampouco sobre qualquer assunto envolvendo proteção de dados.

Merecem destaque, contudo, as Súmulas de nº 479 (de 2012, que aborda a responsabilidade objetiva dos bancos pelos danos causados por fortuitos internos relativos a fraudes de terceiros) e nº 550 (de 2015, que define ser escore de crédito não um banco de dados, mas um método estatístico de avaliação de risco, o que dispensa o consentimento do consumidor), por terem sido muito lembradas nos casos estudados.

CONCLUSÃO

A presente pesquisa objetivou perquirir os primeiros indicativos jurisprudenciais do Superior Tribunal de Justiça sobre a responsabilidade civil no âmbito da Lei Geral de Proteção de Dados, especialmente no que se refere aos danos causados por agentes de tratamento de dados em incidentes de vazamentos.

Após as conceituações e ponderações iniciais sobre os incidentes de segurança e o papel dos agentes de tratamento na lida com os dados pessoais, buscou-se concretizar o primeiro objetivo da pesquisa, qual seja, o de atualizar os posicionamentos doutrinários sobre o(s) regime(s) de responsabilidade civil na LGPD, partindo-se da interpretação dos seus arts. 42 a 45.

Restou clara a posição de defensores do regime subjetivo, como Gustavo Tepedino, Bruno Bioni e Daniel Dias, que, em suma, sustentam sua posição em decorrência do estímulo legislativo dado aos deveres de cuidado do agente de tratamento. Contudo, é cristalina a predominância de posições centradas na responsabilidade objetiva para a LGPD, notadamente pela vulnerabilidade a que os titulares de dados estão submetidos em um mundo marcado pela *big data*, tecnologias disruptivas e enviesadas e grandes assimetrias informacionais.

Ganha ênfase o posicionamento liderado por Laura Schertel Mendes e Danilo Doneda (2018a; 2018b), e reforçado por nomes como Caitlin Mulholland (2018), de que a obrigação de reparação dos danos é intrínseca à atividade de tratamento de dados, seja pela vulnerabilidade dos consumidores, seja pelas omissões das empresas em instituir sistemas eficazes de proteção da privacidade daqueles (dever de segurança – responsabilidade *ex-ante*). Esses juristas são, inclusive, citados em alguns julgados do STJ, como o REsp nº 1.995.458 – SP e REsp nº 2.147.374 – SP.

Decorrentes da responsabilidade objetiva, mereceram destaque as seguintes classificações: objetiva especial (de Rafael Dresch – dever de segurança centrado no defeito e não no risco), ativa ou proativa (de Maria Celina Bodin de Moraes – foco na prevenção e demonstração da efetividade das medidas de segurança do agente de tratamento) e mista (de Anderson Schreiber – objetiva para o tratamento irregular por fornecimento de segurança inferior à esperada e subjetiva para o tratamento irregular por inobservância da legislação ou a não adoção de medidas específicas do art. 46 – ou de Ana Frazão – objetiva para os casos que ultrapassem riscos ordinários e subjetiva para os de menor risco).

De todos os elementos normativos estudados, o mais lembrado pelos doutrinadores é a segurança esperada, base para o chamado tratamento irregular, previsto no art. 44 da lei, que

impõe aos agentes a adoção de técnicas eficazes de proteção. Além disso, a similaridade com a técnica adotada pelo CDC fica muito evidente, na medida em que esse diploma também utiliza como parâmetro de responsabilização a segurança esperada pelo consumidor (§ 1º do art. 14), tudo para nos levar à conclusão de uma forte facilitação da LGPD ao dever de indenizar e de uma opção pelo regime de natureza objetiva.

Antes de se adentrar nos julgamentos do STJ, teceram-se, em breves considerações, indicativos da jurisprudência dos tribunais estaduais sobre o tema em comento, tendo-se como suporte dados da pesquisa do IDP-JusBrasil, dissertações de mestrado e julgamentos em concreto de casos que, posteriormente, foram enfrentados pela Corte Superior. Nesse ponto, a conclusão alcançada foi a de que houve grande desarmonia entre as decisões de 2º grau quanto à responsabilidade civil dos agentes de tratamento, sem uma posição clara sobre o regime a ser adotado (se objetivo ou subjetivo).

Vale ressaltar dois aspectos muito relevantes visualizados no espectro da judicialização da LGPD no Brasil. O primeiro, de fácil percepção, é o da significativa quantidade de ações de reparação por danos morais sofridos nas relações de consumo (bancárias, com concessionárias de serviços públicos, telecomunicações, aplicativos de tecnologia, entre outras), em comparação com outros tipos de pleito.

O segundo, mais inesperado, é o fato de que os titulares de dados não estão embasando suas ações reparatórias corretamente com os artigos da LGPD, insistindo em substituí-los por dispositivos equivalentes do Código de Defesa do Consumidor. Essa peculiaridade foi observada nas decisões estaduais analisadas, em que desembargadores têm utilizado majoritariamente o CDC para basear suas fundamentações.

É importante lembrar que não se questiona a citação ou mesmo o embasamento no CDC nas decisões estudadas, seja por versarem sobre relações de consumo, seja pela própria referência que a LGPD faz ao diploma consumerista em seu art. 45. O que se observa é o fato de que, sendo a Lei Geral de Proteção de Dados uma lei específica, deveria, em regra, tratando do mesmo tema (responsabilidade civil), se sobressair em relação a uma lei geral (Código de Defesa do Consumidor), diante da aplicação concreta de casos envolvendo incidentes de dados pessoais.

O segundo objetivo, de análise dos julgamentos no STJ, foi alcançado, o que se deu não apenas com os sete acórdãos selecionados nos subitens do Capítulo 3 – resumidos em tabela anexa –, como com inúmeros outros citados ao longo do trabalho.

Dessa investigação, pode-se concluir quão polêmica foi a primeira decisão específica sobre a temática, o AREsp nº 2.130.619 – SP, relatado pelo Ministro Falcão, por ter optado pelo

regime de responsabilidade subjetiva, ao não admitir dano presumido, num caso envolvendo direito do consumidor - em que a regra é a responsabilidade objetiva - e incidente de dados comuns (não sensíveis). O julgado deu margem à interpretação de que o STJ estaria inovando ao adotar uma linha pela responsabilidade subjetiva em matéria consumerista no âmbito da LGPD. E mais: ao permitir a reparação apenas nos casos de vazamento de dados sensíveis, desconsiderou a importância dada, pela lei, à proteção dos dados comuns, influenciando julgamentos Brasil afora nesse sentido.

Contudo, a partir das decisões seguintes, no âmbito da Terceira Turma, restou clara a opção pela responsabilidade objetiva, com forte influência das posições da ministra Nancy Andrighi que, antes mesmo da vigência da LGPD, considerou dano moral presumido decorrente do dever de informação nos bancos de dados (REsp nº 1.758.799 – MG). Após a vigência da lei, relatou a quase totalidade dos julgados da Turma sobre o assunto (Recursos Especiais nº 1.995.458 – SP, nº 2.015.732 – SP, nº 2.077.278 – SP, nº 2.092.096 – SP e nº 2.121.904 – SP), sedimentando entendimento quanto i) ao dever de segurança do agente de tratamento; ii) à responsabilidade objetiva, inclusive nos casos de incidentes envolvendo dados pessoais comuns (não sensíveis); e iii) ao dano moral presumido (*in re ipsa*).

Ainda na Terceira Turma, é de se destacar o papel do Ministro Ricardo Villas Bôas Cueva pois, além de ter relatado o REsp nº 2.147.374 – SP, que inovou trazendo a responsabilidade proativa ao debate, muito contribuiu com a Ministra Nancy em votos-vista (como no REsp nº 1.995458-SP) e tem escrito artigos e livros importantes sobre a LGPD.

Já na Quarta Turma, a única decisão de relevância encontrada (AREsp nº 2.311.731 – RS), monocrática da ministra Isabel Gallotti, também se mostrou alinhada ao regime de natureza objetiva. Excetuado esse caso, fato interessante é que todas as demais decisões foram proferidas por unanimidade, o que denota coesão de ideias entre os membros de cada colegiado.

Sobre o terceiro e último objetivo da pesquisa, o de se explicitar o grau de vinculação das decisões do STJ às instâncias inferiores, o que se viu foi uma utilização, em claro "replicar" de tese, do AREsp 2.130.619 – SP, imagina-se que pelo seu pioneirismo, como se observou nos três acórdãos dos Tribunais de Justiça de São Paulo e Paraná prolatados nos meses seguintes ao do seu julgamento, todos no sentido de afastar a responsabilização de incidentes que não envolvam dados sensíveis, e de inadmitir a presunção de danos morais.

Quanto ao REsp nº 2.077.278 – SP, encontrou-se apenas um julgamento (do TJ-PR) que o utilizou como referência, número, portanto, inferior aos do AREsp 2.130.619 – SP, porém, bem fundamentado no sentido de responsabilizar a instituição financeira diante das falhas na prestação de serviço, que permitem a atuação de fraudadores.

Já no que se refere aos REsp nºs 2.092.096 – SP, 2.147.374 – SP e 2.121.904 – SP, em que pese a consistência de suas teses quanto à responsabilização objetiva e ao tratamento irregular decorrente da ausência do dever de segurança, curiosamente, foram pouco encontrados nos dois tribunais estaduais pesquisados. De todo modo, diante das suas recentidades, ainda é cedo para se firmar qualquer conclusão sobre seus graus vinculativos às instâncias inferiores.

Ainda que não haja o correto embasamento legal da LGPD nas ações reparatórias e nas próprias decisões judiciais, sua menção e conjugação com dispositivos do CDC e de outros diplomas, muito contribui para consolidar a eficácia da defesa da privacidade do consumidor/titular de dados.

Chega-se, portanto, à conclusão que a invocação da LGPD em juízo deve ocorrer ao lado de outras normas, como o CDC (citado no próprio art. 45 da LGPD), o Marco Civil da Internet, e outras que poderão vigorar (como a Lei de Inteligência Artificial), em interpretação sistemática de todas elas.

No caso do STJ, embora os julgamentos estudados advenham de relações de consumo distintas (fornecimento de energia, serviços bancários, investimento em bolsa e seguro de vida), quanto ao regime de responsabilidade civil, percebeu-se, a exemplo do que a doutrina capitaneada por Laura Schertel e Danilo Doneda já demonstrava, o esforço na utilização dos elementos normativos previstos nos artigos 42 a 44 da LGPD, para afastar a ideia de que apenas o art. 45 deveria ser aplicado às violações de dados em matéria consumerista.

Não se pretendeu exaurir a abordagem do tema no Tribunal da Cidadania, mas ficou clara a relevância do que a Corte já julgou, a nosso ver, com especial contribuição da Terceira Turma, seja pela quantidade de casos, seja pela profundidade e reiteração de argumentos, com cerne no dever de conduta dos agentes de tratamento.

De todo modo, inclusive pelo contexto histórico, é facilmente percebida a preocupação do STJ em dar efetividade à lei de proteção de dados, neste constante diálogo com outras fontes normativas, ampliando o patamar de proteção dos dados do indivíduo, mas sem dar guarida ao anonimato pleno, já que tem prevalecido o entendimento de identificação de responsáveis por atos ilícitos (Cueva, 2023, p. 100).

Em se confirmando a inclinação de julgamentos pela responsabilidade objetiva nos incidentes de vazamento na Terceira Turma, com possíveis reflexos nas demais Turmas, é possível que, num futuro não tão distante, o Tribunal, pelo sistema de precedentes qualificados, firme formalmente jurisprudência no sentido de responsabilizar objetivamente o agente de tratamento que não adote mecanismos de proteção, ainda que os dados envolvidos não sejam sensíveis.

Permite-se, por fim, concluir que esta opção pelo regime objetivo (ou quaisquer de suas variantes), mais do que dar efetividade à lei, está, no atual contexto de hiperconexão e vulnerabilidades, contribuindo fortemente para o exercício do direito constitucional à proteção de dados, ou, nas palavras de Ingo Wolfgang Sarlet, rendendo "homenagens à dignidade da pessoa humana, ao livre desenvolvimento da personalidade e à liberdade pessoal como autodeterminação".

REFERÊNCIAS

ANDRIGHI, Fatima Nancy; GUARIENTO, Daniel Bittencourt (org.). **A responsabilidade civil das redes sociais virtuais pelo conteúdo das informações veiculadas**. São Paulo: Atlas, 2014.

ÁVILA, Humberto. **Teoria dos princípios:** da definição à aplicação dos princípios jurídicos. 15. ed. São Paulo: Malheiros, 2014.

AZEVEDO, Álvaro Villaça. **Código Civil comentado**. São Paulo: Atlas, 2003.

BARBOSA MOREIRA, José Carlos. O direito em tempos de globalização. **Revista Brasileira de Direito Comparado**, Rio de Janeiro, 1982.

BELLEIL, Arnaud. **@ privacidade**: O mercado de dados pessoais – proteção da vida privada na idade da internet. Trad. Paula Rocha Vidalinc. Lisboa: Instituto Piaget, 2002.

BENJAMIN, Antônio Herman V; MARQUES, Claudia Lima; BESSA, Leonardo Roscoe. **Comentários ao código de defesa do consumidor.** 5. ed. rev., atual. e ampl. São Paulo: RT, 2013.

BENJAMIN, Antônio Herman V.; MARQUES, Claudia Lima; BESSA, Leonardo Roscoe. **Manual de Direito do Consumidor**. 7. ed. rev., atual. e ampl. São Paulo: RT, 2016.

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com**, Rio de Janeiro, ano 9, n. 3, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/662. Acesso em: jun. 2024.

BODIN DE MORAES, Maria Celina. LGPD: um novo regime de responsabilidade civil dito proativo. **Civilistica.com**, Rio de Janeiro, v. 8, n. 3, 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/448/377. Acesso em: dez. 2024.

BODIN DE MORAES, Maria Celina; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. **Cadernos Adenauer – Proteção de dados pessoais: privacidade versus avanço tecnológico**, Rio de Janeiro, ano XX, n. 3, p. 113-135, 2019.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text =EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento %20de%20dados%20pessoais. Acesso em: abr. 2024.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: maio/2024. Acesso em: maio 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: junho/2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/ l13709.htm. Acesso em: maio 2024.

BRASIL. Ministério da Justiça e Segurança Pública. **Resolução CD/ANPD nº 15, de 24/04/2024**. Aprova o Regulamento de Comunicação de Incidente de Segurança. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: nov. 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, de Maio de 2021.** Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: junho 2025.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. **The Guardian**, 17 mar. 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: out. 2024.

CALIXTO, Marcelo Junqueira. **A culpa na responsabilidade civil:** estrutura e função. Rio de Janeiro: Renovar, 2008.

CÂMARA DOS DEPUTADOS. **Tramitação do Projeto de Lei nº 2338/2023.** 2025. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?id Proposicao=2487262. Acesso em: maio 2025.

CAMBRICOLI, Fabiana. Nova falha do Ministério da Saúde expõe dados pessoais de mais de 200 milhões de brasileiros. **Estadão**, 2 dez. 2020. Disponível em: https://www.estadao.com.br/saude/nova-falha-do-ministerio-da-saude-expoe-dados-pessoais-de-mais-de-200-milhoes/. Acesso em: out. 2024.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. Cadernos Jurídicos, São Paulo, ano 21, n. 53, p. 167-170, jan./mar. 2020.

CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 9. ed. rev. ampl. São Paulo: Editora Atlas, 2010.

COMITÊ GESTOR DA INTERNET NO BRASIL – CGI.br. **Cartilha de Segurança para Internet.** Versão 4.0. São Paulo, 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: setembro/2024.

CORDEIRO, A. Barreto Menezes. Repercussões do RGPD sobre a responsabilidade civil. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 219-241.

CRUZ, Gisela Sampaio da; MEIRELES, Rose Melo Venceslau. Término do tratamento de dados. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 219-241.

CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 3ª ed. rev., atual. e ampl. São Paulo: Thomson Reuters, 2023. p. 80-100.

CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). **Compliance e Política de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço jurídico Journal of Law**, v. 12, p. 91-108, 2011. Disponível em: file:///C:/Users/PC/Downloads/1315-Texto%20do%20artigo-4614-4749-10-20111213.pdf. Acesso em: maio 2025.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**: responsabilidade civil. 33 ed. São Paulo: Saraiva, 2019.

DRESCH, Rafael de Freitas Valle. A especial responsabilidade civil da Lei Geral de Proteção de Dados. **Migalhas**, 2 jul. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/330019/a-especial-responsabilidade-civil-na-lei-geral-de-protecao-de-dados. Acesso em: maio/2024.

DRESCH, Rafael de Freitas Valle; FALEIROS JUNIOR, José. L. M. Reflexões sobre a Responsabilidade Civil na Lei Geral de Proteção de Dados (Lei nº 13.709/2018). *In:* ROSENVALD, Nelson; WESENDONCK, Tula; DRESCH, Rafael (org.). **Responsabilidade civil**: novos riscos. Indaiatuba-SP: Editora Foco, 2019. v. 1, p. 65-90.

DRESCH, Rafael de Freitas Valle; MELO, Gustavo da Silva. Comentários ao art. 43. *In:* BONNA, Alexandre Pereira; MARTINS, Guilherme Magalhães; ROZATTI LONGHI, João Victor; FALEIROS JÚNIOR, José Luiz de Moura (coord.). **Comentários à Lei Geral de Proteção de Dados Pessoais**. Indaiatuba-SP: Editora Foco, 2022.

DRESCH, Rafael de Freitas Valle; STEIN, Lilian Brandt. Direito fundamental à proteção de dados e responsabilidade civil. **Migalhas**, 27 nov. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/336997/direito-fundamental-a-protecao-de-dados-e-responsabilidade-civil. Acesso em: maio 2024.

EHRDARDT JR, Marcos. Comentários ao art. 42. *In:* BONNA, Alexandre Pereira; MARTINS, Guilherme Magalhães; ROZATTI LONGHI, João Victor; FALEIROS JÚNIOR, José Luiz de Moura (coord.). **Comentários à Lei Geral de Proteção de Dados Pessoais**. Indaiatuba-SP: Editora Foco, 2022.

FACHIN, Luiz Edson. Direito civil e a dignidade da pessoa humana: um diálogo constitucional contemporâneo. **Revista Forense**, Rio de Janeiro, v. 392, 2006.

FORSELL, João Carlos. **As interferências dos processos judiciais na proteção de dados pessoais.** Itanhaém: Ed. do Autor, 2018.
FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. Responsabilidade civil e ressarcimento de danos. *In*: FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. **Curso de proteção de dados pessoais**: fundamentos da LGPD. Rio de Janeiro: Forense, 2022. p. 423-443.

FRAZÃO, Ana; MULHOLLAND, Caitlin. Episódio 1: Vazamento de Dados. **PodCast Direito Digital**, 28 abr. 2021. Disponível em: https://creators.spotify.com/pod/profile/podcast-direito-digital/episodes/EP1-Vazamento-de-dados-evhkq4. Acesso em: out. 2024.

FUX, Luiz; BODART, Bruno. Notas sobre o princípio da motivação e a uniformização da jurisprudência no novo Código de Processo Civil à luz da análise econômica do direito. *In*: DANTAS, Bruno *et al*. **Questões relevantes sobre recursos, ações de impugnação e mecanismos de uniformização da jurisprudência**. São Paulo: RT, 2017.

GAMIZ, Mario Sergio de Freitas. **Privacidade e intimidade**: doutrina e jurisprudência. Curitiba: Juruá, 2012.

GOMES, Orlando. **Novos temas do direito civil**. Rio de Janeiro: Forense, 1983.

GROSSI, Bernardo Menicucci (org.). **Lei geral de proteção de dados:** uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial. Porto Alegre: Editora Fi, 2020.

GROSSI, Bernardo Menicucci. **O desafio da regulação dos dados pessoais**: entre a autonomia e a heteronomia. 2022. Tese (Doutorado em Direito) – Pontifícia Universidade Católica, Belo Horizonte, 2022. Disponível em: https://sucupira.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/view TrabalhoConclusao.jsf?popup=true&id_trabalho=11881884. Acesso em: out. 2024.

GUEDES, Gisela S. da Cruz; MEIRELES, Rose Melo Vencelau. Término do tratamento de dados. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais**. São Paulo: Revista dos Tribunais, 2019.

IBM. **Relatório do custo das violações de dados de 2024**. Disponível em: https://www.ibm.com/br-pt/reports/data-breach. Acesso em: nov. 2024.

JUNQUILHO, Tainá Aguiar. **Inteligência Artificial no Direito**: limites éticos. São Paulo: JusPodivm, 2022.

KALLAJIAN, Manuela Cibim. **Privacidade, informação e liberdade de expressão**: conflito de normas e critérios de ponderação. Curitiba: Juruá, 2019.

LANDIM NETO, José Emiliano Paes. **Responsabilidade civil dos agentes de tratamento à luz da Lei Geral de Proteção de Dados:** análise jurisprudencial dos tribunais estaduais. 2022. Dissertação (Mestrado Profissional em Direito Econômico e Desenvolvimento) – Instituto

Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2022. Disponível em: https://repositorio.idp.edu.br/bitstream/123456789/4234/5/DISSERTA%C3%87%C3%83O_Jos%C3%A9%20Emiliano%20Paes%20Landim%20Neto.pdf Acesso em: jul. 2024.

LAGES, Leandro Cardoso. **Direito do Consumidor: a lei, a jurisprudência e o cotidiano**. 4. ed. Rio de Janeiro: Lumen Juris, 2020.

LEME, Carolina da Silva. Proteção e tratamento de dados sob o prisma da legislação vigente. **Revista Fronteiras Interdisciplinares do Direito**, v. 1, n. 1, 2019.

LIMBERGER, Têmis; SARLET, Ingo Wolfgang (org.). **Direitos fundamentais, informática e comunicação**. Porto Alegre: Livraria do Advogado, 2007.

MADALENA, Juliano. **A responsabilidade civil decorrente do vazamento de dados pessoais.** *In:* DRESCH, Rafael de Freitas Valle; MENKE, Fabiano (org). **Lei Geral De Proteção de Dados**: aspectos relevantes. Indaiatuba-SP: Editora Foco, 2021. p. 250-261.

MAIMONE, Flávio Henrique Caetano de Paula. **Responsabilidade civil na LGPD:** efetividade na proteção de dados pessoais. Indaiatuba-SP: Editora Foco, 2022.

MARCON, Daniele Verza. Dano moral e vazamento de dados: o STJ escreveu certo por linhas tortas? **Conjur**, 9 abr. 2023. Disponível em: https://www.conjur.com.br/2023-abr-09/daniele-marcon-dano-moral-vazamento-dados. Acesso em: jul. 2024.

MARQUES, Claudia Lima; MUCELIN, Guilherme. Responsabilidade civil dos provedores de aplicação por violação de dados pessoais na internet: o método do diálogo das fontes e o regime do Código de Defesa do Consumidor. *In*: GOMES, Iviê A. M. Loureiro (coord.). **Contraponto Jurídico**: posicionamentos divergentes sobre grandes temas do direito. São Paulo: Revista dos Tribunais, 2018. p. 393-415.

MARQUES, Claudia Lima; MARTINS, Fernando Rodrigues; MAGALHÃES, Guilherme; BESSA, Leonardo Roscoe (coord.). **5 anos de LGPD**: estudos em homenagem a Danilo Doneda. São Paulo: Thomson Reuters Brasil, 2023.

MARQUES, Claudia Lima; MIRAGEM, Bruno. O necessário diálogo entre a LGPD e o Código de Defesa do Consumidor – titular de dados. *In:* MENDES, Laura; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otavio Luiz (coord). **Tratado de proteção de dados pessoais**. 2. ed. Rio de Janeiro: Forense, 2023.

MARTINS COSTA, Judith. **Comentários ao novo Código Civil**: do inadimplemento das obrigações. Rio de Janeiro: Forense, 2009. v. 5, tomo II.

MARTINS, Guilherme Magalhães. Responsabilidade civil, acidente de consumo e a proteção do titular de dados na internet. *In*: SILVEIRA, Ana Cristina de Melo (coord). **Proteção de dados pessoais na sociedade de informação**: entre dados e danos. Indaiatuba-SP: Editora Foco, 2021. p. 77-89.

MARTINS, Guilherme Magalhães. Comentários ao art. 45. *In:* BONNA, Alexandre Pereira; MARTINS, Guilherme Magalhães; ROZATTI LONGHI, João Victor; FALEIROS JÚNIOR,

José Luiz de Moura (coord.). **Comentários à Lei Geral de Proteção de Dados Pessoais**. Indaiatuba-SP: Editora Foco, 2022. p. 423-430.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José L. M. Compliance digital e responsabilidade civil na Lei de Proteção de Dados. *In*: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (coord). **Responsabilidade civil e novas tecnologias**. Indaiatuba-SP: Foco, 2020.

MALDONADO, Viviane Nobrega; OPICE BLUM, Renato (coord.). **LGPD:** Lei Geral de Proteção de Dados comentada. 4. ed. rev. e atual. São Paulo: Thomson Reuters Brasil, 2022. p. 346-359.

MEDON, Filipe. Decisões automatizadas: o necessário diálogo entre a Inteligência Artificial e a proteção de dados pessoais para a tutela de direitos fundamentais. *In*: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (org.). **O Direito Civil na era da inteligência artificial**. São Paulo: Thomson Reuters Brasil, 2020a. p. 337-370.

MEDON, Filipe. **Inteligência Artificial e Responsabilidade Civil**: autonomia, riscos e solidariedade. Salvador: Editora JusPodivm, 2020b.

MEDON, Filipe. Inteligência Artificial e Direito Civil: desafios ao direito à imagem e à Responsabilidade Civil. *In*: PINHO, Anna Carolina (org.). **Manual de Direito na Era Digital Civil**. Indaiatuba-SP: Foco, 2022a. p. 271-288.

MEDON, Filipe. Solidariedade como diretriz para a Responsabilidade Civil na sociedade de riscos *In*: MEDON, Filipe. **Inteligência Artificial e Responsabilidade Civil**: autonomia, riscos e solidariedade. 2. ed. revista, atualizada e ampliada. São Paulo: JusPodivm, 2022b.

MEDON, Filipe; FALEIROS JUNIOR, José L. M. Discriminação algorítmica de preços, perfilização e responsabilidade civil nas relações de consumo. **Revista de Direito da Responsabilidade**, v. 1, p. 947-969, 2021.

MELLO, Alexandre Schmitt da Silva; MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (org.). **Lei Geral de Proteção de Dados**: aspectos relevantes. Indaiatuba-SP: Editora Foco, 2021. 344 p. ISBN 978-65-5515-251-7.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 12. ed. São Paulo: Saraiva, 2017.

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

MENDES, Laura Schertel. A lei geral de proteção dos dados pessoais: um modelo de aplicação em três níveis. *In*: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). **Caderno Especial**: Lei Geral de Proteção dos Dados (LGPD). São Paulo: Revista dos Tribunais, 2019. p. 35-56.

MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. **Jota**, 10 maio 2020. Disponível em: https://www.jota.info/artigos/decisao-

historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais. Acesso em: nov. 2024.

MENDES, Laura Schertel (coord.). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 120, p. 469-483, nov./dez. 2018a.
MENDES, Laura Schertel; DONEDA, Danilo. Comentários à nova Lei Geral de Proteção de Dados (Lei nº 14.709/2018): o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, São Paulo, v. 27, p. 555-587, nov./dez. 2018b.

MENDES, Laura Schertel; FUJIMOTO, Mônica (org.). **Painel LGPD nos Tribunais.** Brasília: IDP, 2024. Disponível em: https://wpcdn.idp.edu.br/idpsiteportal/2024/06/Relatorio-LGPD-nos-Tribunais-1a-edicao.pdf. Acesso em: jul. 2024.

MILHÕES de brasileiros foram vítimas de vazamento ilegal de dados de celulares. **G1**, 10 fev. 2021. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2021/02/10/milhoes-de-brasileiros-foram-vitimas-de-vazamento-ilegal-de-dados-de-celulares.ghtml. Acesso em: out. 2024.

MIRANDA, Marcelo. **Lei Geral de Proteção de Dados – LGPD.** [*S. l.*: *s. n.*], 2019. Disponível em: https://www.academia.edu/40367651/Lei_Geral_de_Prote%C3%A7%C3%A3o_de_Dados_LGPD. Acesso em: out. 2024.

MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018). **Revista de Direitos e Garantias Fundamentais**, v. 19, n. 3, p. 159-180, 2018. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf. Acesso em: dez. 2024.

NUNES, Ana Luisa Tarter. **O regime dual de responsabilidade civil pelo tratamento irregular de dados pessoais**. *In*: MARQUES, Claudia Lima. **5 anos de LGPD**: estudos em homenagem a Danilo Doneda. São Paulo: Thomson Reuters Brasil, 2023a. p. 27-39.

NUNES, Ana Luisa Tarter. **O regime dual de responsabilidade civil na LGPD.** 2023. 296 f. Tese (Doutorado em Direito) – Universidade de Brasília, Brasília, 2023b.

OPICE BLUM, Renato. **Proteção de dados**: desafios e soluções na adequação à lei. Rio de Janeiro: Forense, 2020.

PAGANELLA, Victoria Dickow. Responsabilidade Civil na Lei Geral de Proteção de Dados: uma análise do nexo de imputação. *In*: DRESCH, Rafael de Freitas Valle; MENKE, Fabiano (org.). **Lei Geral de Proteção de Dados**: aspectos relevantes. Indaiatuba-SP: Editora Foco, 2021.

PICELLI, Roberto Ricomini. **A dimensão política da privacidade no direito brasileiro**. Rio de Janeiro: Lumen Juris, 2018.

RODRIGUES, Caio Cesar. STJ e LGPD: dano moral por vazamento de dados deve ser comprovado. **Conjur**, 7 jun. 2023. Disponível em: https://www.conjur.com.br/2023-jun-07/caio-cesar-dano-moral-vazamento-dados-comprovado#:~:text=De%20forma%20clara%20e%20acertada,de%20gerar%20dano%20moral%20indeniz%C3%A1vel. Acesso em: jul. 2024.

RODRIGUEZ, Daniel Piñeiro. **O direito fundamental à proteção de dados**: vigilância, privacidade e regulação. Rio de Janeiro: Lumen Juris, 2021.

ROSENVALD, Nelson. **As funções da responsabilidade civil**: a reparação e a pena civil. São Paulo: Saraiva, 2017.

SADEK. Maria Teresa. Direitos e sua concretização: judicialização e meios extrajudiciais. **Cadernos FGV Projetos**, v. 30, p. 38-50, 2017. Disponível em: https://fgvprojetos.fgv.br/sites/fgvprojetos.fgv.br/files/cadernosfgvprojetos_30_solucaodeconflitos_0.pdf. Acesso em: nov. 2024.

SANSEVERINO, Paulo de Tarso Vieira. **Princípio da reparação integral.** São Paulo: Saraiva, 2011.

SANTOS, Romualdo Baptista dos. **Responsabilidade civil por dano enorme**. Curitiba: Juruá, 2018.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. 13. ed. Porto Alegre: Livraria do Advogado, 2018.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 14, n. 42, p. 179-218, jan./jun. 2020. Disponível em: https://repositorio.pucrs.br/dspace/bitstream/10923/18864/2/PROTEO_DE_DADOS_PESSOAIS_COMO_DIREITO_FUNDAMENTAL_NA_CONSTITUIO_FEDERAL_BRASILEIRA_DE_1988.pdf. Acesso em: abr. 2025.

SCHMITT, Cristiano Heineck. Vazamento de dados e a responsabilidade civil do fornecedor. In: MARQUES, Claudia Lima. **5 anos de LGPD**: estudos em homenagem a Danilo Doneda. São Paulo: Thomson Reuters Brasil, 2023. p. 67-74.

SCHREIBER, Anderson. **Novas paradigmas da responsabilidade civil:** da erosão dos filtros de reparação à diluição dos danos. São Paulo: Atlas, 2009.

SCHREIBER, Anderson. Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. *In:* MENDES, Laura; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otavio Luiz; BIONI, Bruno (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 319-338.

SCHREIBER, Anderson; MARTINS, Guilherme Magalhães; CARPENA, Heloisa (coord.). **Direitos fundamentais e sociedade tecnológica**. São Paulo: Editora Foco, 2021.

SILVEIRA, Ana Cristina de Melo; LONGHI, João Victor Rozatti; FALERIOS JÚNIOR, José Luiz de Moura; GUGLIARA, Rodrigo (coord.). **Proteção de dados pessoais na sociedade da informação**: entre dados e danos. Indaiatuba-SP: Editora Foco, 2021.

SOUSA, Fabio Torres de. A Lei Geral de Proteção de Dados e a defesa do consumidor na efetividade da jurisprudência dos tribunais. *In*: MARQUES, Claudia Lima. **5 anos de LGPD**: estudos em homenagem a Danilo Doneda. São Paulo: Thomson Reuters Brasil, 2023. p. 111-121.

SUPERIOR TRIBUNAL DE JUSTIÇA – STJ. **Para presidente do STJ, ação do Judiciário ajudará na efetivação dos direitos previstos na LGPD**. 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/21092020-Para-presidente-do-STJ--acao-do-Judiciario-ajudara-na-efetivacao-dos-direitos-previstos-na-LGPD.aspx. Acesso em: fev. 2025.

SUPREMO TRIBUNAL FEDERAL – STF. **OAB questiona decreto presidencial sobre compartilhamento de dados dos cidadãos.** 2021. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=459125&ori=1. Acesso em: nov. 2024.

TAMER, Maurício. **LGPD comentada artigo por artigo**: interpretação e aplicação da lei. 2. ed. São Paulo: Rideel, 2022.

TAMER, Maurício. STJ e a ausência de dano moral *in re ipsa* em vazamentos de dados. **Migalhas**, 22 mar. 2023. Disponível em: https://www.migalhas.com.br/depeso/383463/stj-e-a-ausencia-de-dano-moral-in-re-ipsa-em-vazamentos-de-dados. Acesso em: maio 2024.

TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. **Cadernos Jurídicos – Direito digital e proteção de dados pessoais**, São Paulo, ano 21, n. 53, jan./mar. 2020.

TERADA, Michelle Toshiko**.** Obrigações e responsabilidade dos agentes de tratamento de dados. *In*: MARINHO, Gustavo; VALIM, Rafael; SIMÃO, Valdir; WARDE, Walfrido (org.). **Aspectos relevantes da Lei Geral de Proteção de Dados**. São Paulo: Editora Contracorrente, 2021. p. 161-180.

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. Responsabilidades e ressarcimento de danos por violação às regras previstas na LGPD. *In*: LIMA, Cintia Rosa Pereira de (coord.). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020.

TEIXEIRA, Tarcísio; MAGRO, Américo Ribeiro (coord.). **Proteção de dados**: fundamentos jurídicos. Salvador: Juspodivm, 2020.

TEPEDINO, Gustavo; TERRA, Aline de Miranda V.; GUEDES, Gisela S. da Cruz. **Fundamentos de direito civil**. 2. ed. Rio de Janeiro: Forense, 2021. v. 4, p. 285-294.

TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO – TRF 3. **União, Caixa, Dataprev e ANPD devem indenizar cidadãos que tiveram dados pessoais vazados em 2022**. 2 out.

2023. Disponível em: https://web.trf3.jus.br/noticias-sjsp/Noticiar/ExibirNoticia/1020-uniao-caixa-dataprev-e-anpd-devem-indenizar-cidadaos. Acesso em: abr. 2025.

UNIÃO EUROPEIA. **General Data Protection Regulation**. Parlamento Europeu. Bélgica, 27 abr. 2016. Disponível em: https://gdprinfo.eu/pt-pt/pt-pt-article-4. Acesso em: out. 2024.

ZANATTA, Rafael A. F. Agentes de tratamento de dados, atribuições e diálogo com o Código de Defesa do Consumidor. *In:* INSTITUTO DE TECNOLOGIA E SOCIEDADE. **Coletânea sobre a Lei Geral de Proteção de Dados Pessoais**. São Paulo, Revista dos Tribunais, 2019.

ZANATTA, Rafael A. F. Comentários ao art. 44. *In:* BONNA, Alexandre Pereira; MARTINS, Guilherme Magalhães; ROZATTI LONGHI, João Victor; FALEIROS JÚNIOR, José Luiz de Moura (coord.). **Comentários à Lei Geral de Proteção de Dados Pessoais**. Indaiatuba-SP: Editora Foco, 2022.

ANEXO 1 – TABELA RESUMO: JULGAMENTOS DO SUPERIOR TRIBUNAL DE JUSTIÇA EM MATÉRIA DE RESPONSABILIDADE CIVIL NO ÂMBITO DA LEI GERAL DE PROTEÇÃO DE DADOS (ordem cronológica)[132]:

Nº	Processo / Relator(a) / Órgão julgador	Partes	Data do Julgamento	Assunto(s)	Aspectos relevantes	Artigos da LGPD citados	Regime de responsabilidade civil do agente de tratamento
ANTES DA VIGÊNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS (JULGAMENTOS RELEVANTES EM MATÉRIA DE PROTEÇÃO DE DADOS)							
1	REsp nº 22.337-9- RS / Ministro Ruy Rosado de Aguiar / Quarta Turma	Clube de Diretores Lojistas de Passo Fundo x José Orivaldo M. Branco	13/2/1995	Definição de prazo para cancelamento de registro no SPC.	Preocupação com a colheita indiscriminada de informações nos bancos de dados. Referência à autodeterminação informativa do direito alemão como garantia fundamental.	--	Não definido
2	REsp nº 306.570-SP / Ministra Eliana Calmon / Segunda Turma	Regina Célia R. da S. Furtado x Nelson Antônio Barrico	18/10/2001	Requisição de informação bancária (endereço) do réu devedor ao Banco Central.	Definição da privacidade em relação aos dados pessoais do titular de conta bancária. Possibilidade de quebra de sigilo apenas em situações excepcionais.	--	Não definido

[132] Pelo grau de relevância, compõem esta tabela apenas os julgamentos abordados no corpo do texto da pesquisa, excetuando-se os mencionados em notas de rodapé, cujas considerações foram ali incluídas.

3	REsp nº 1.168.547-RJ / Ministro Luis Felipe Salomão / Quarta Turma	World Company Dance Show x Patrícia C. de Lima Santos	11/5/2010	Utilização de imagem indevida em site, com pedido de indenização por dano material e moral.	A intangibilidade das informações armazenadas e transmitidas na rede mundial de computadores, a fugacidade e instantaneidade com que as conexões são estabelecidas e encerradas e seu alcance global, constituem-se peculiaridades inerentes a esta nova tecnologia, abrindo ensejo à prática de condutas indevidas, pelo que se exige um novo conceito de privacidade, centrado no direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações, nelas incluindo o direito à imagem utilizada indevidamente.	--	Não definido
4	REsp nº 1.758.799 - MG / Ministra Nancy Andrighi / Terceira Turma	Procob S/A x José Galvão da Silva	12/11/2019	Exclusão de informações cadastrais em banco de dados e indenização por dano moral.	A gestão de banco de dados, ainda que não sigilosos, exige dever de informação aos consumidores (art. 43, §2º, CDC e art. 4º, §4º, Lei do Cadastro Positivo – nº 12.414/2011) e gera a estes, direito de acesso aos dados armazenados e à retificação das informações incorretas. O não consentimento do titular de dados, somado à facilitação de acesso a terceiros, favorece a prática de atos ilícitos ou contratações fraudulentas e gera dano moral presumido.	--	Objetiva, por dano presumido
NA VIGÊNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS							
5	REsp nº 1.995.458-SP / Ministra Nancy Andrighi / Terceira Turma	Reginald Jose Costa x Banco Itaucard	9/8/2022	Pleito de responsabilidade civil de correntista idoso vítima do “golpe do motoboy” (telefonema de estelionatário, fornecimento de senha, falso motorista que colhe o cartão e realiza compras).	Há falha na prestação do serviço de instituição financeira que não age com dever de segurança para impedir transações que destoem do perfil do consumidor. Os tipos de dados e a forma de obtenção dos estelionatários levam ao nexo de causalidade com o vazamento. Aplica-se excludente de culpa exclusiva do consumidor ou de terceiro quando o correntista não age com dever de cautela no que se refere à senha pessoal e uso do cartão físico. Imputação	Art.43, Art. 44, Art. 55-J.	Objetiva / *Ex-ante*

					de responsabilidade de incidente contra idoso deve ser feita à luz do Estatuto do Idoso.		
6	AREsp nº 2.130.619–SP / Ministro Francisco Falcão / Segunda Turma	Eletropaulo x Maria Edite de Souza	7/3/2023	Indenização por danos morais, em decorrência de vazamento de dados pessoais constantes da conta de energia.	O vazamento de dados, embora falha indesejável no tratamento de dados, não tem o condão, por si só, de gerar dano moral indenizável. O dano moral não é presumido, sendo necessário que o titular de dados comprove o dano.	Art. 5º, II, Art. 11.	Subjetiva
7	AREsp nº 2.311.731-RS / Ministra Isabel Gallotti / Decisão monocrática	Lucia Regina D. Dell Aglio x Banco do Estado do Rio Grande do Sul	24/4/2023	Indenização por danos materiais em razão de fraude (transferência ao fraudador após ligação telefônica e acesso ao aplicativo bancário do celular da vítima).	Não há falha na prestação do serviço bancário quando o vazamento de dados decorre de culpa exclusiva da vítima (fornecimento de senhas e dados pessoais por telefone, sem a cautela de verificar se a ligação, de fato, é originada do banco). O correntista deve zelar pela guarda e sigilo da senha e do código de segurança.	Art. 46.	Objetiva
8	REsp nº 2.077.278-SP / Ministra Nancy Andrighi / Terceira Turma	Daniela Ferreira Ramos x BV Financeira	3/10/2023	Declaração de inexigibilidade de débito cumulada com indenização por danos morais, em virtude de vazamento de dados de financiamento bancário (“golpe do boleto” praticado por estelionatários).	É imprescindível a verificação dos tipos de dados em posse dos estelionatários para a confirmação do nexo de causalidade com o incidente de vazamento e, por conseguinte, de responsabilização do banco. O tratamento de dados será irregular quando não oferecer o dever de segurança que o consumidor espera. Responsabilidade pela reparação dos danos, independentemente de culpa.	Art. 5º, II, Art. 17, Art. 43, Art. 44, Art. 45.	Objetiva
9	REsp nº 2.092.096–SP / Ministra Nancy Andrighi / Terceira Turma	B3 x Jose A. Bortoluzzo Neto	12/12/2023	Obrigação de exclusão de dados indevidamente inseridos por fraudadores na conta de investidor da plataforma virtual da Bolsa de Valores.	A Bolsa de Valores, ao armazenar e utilizar dados dos investidores na plataforma virtual, realiza típica operação de tratamento de dados, devendo observar os princípios de adequação e segurança. Na qualidade de provedora de aplicação de internet, obriga-se a excluir dados cadastrais inverídicos inseridos por terceiros e a fornecer o detalhamento do acesso fraudulento.	Art. 3º, Art. 5º, I e X, Art. 6º, II e VII, Art. 18, IV, Art. 42 Art. 43, III, Arts. 46 a 49.	Objetiva

10	REsp nº 2.147.374-SP / Ministro Ricardo Villas Bôas Cueva / Terceira Turma	Eletropaulo x Thayna Nayara da Silva Queiroz	3/12/2024	Obrigação de apresentação de lista de dados vazados, origem, finalidade de tratamento e informações sobre compartilhamento, em ataque *hacke*r envolvendo concessionária de energia.	Necessidade de *compliance* de dados pelo agente de tratamento (boas práticas, regras de governança, mecanismos internos de supervisão e *accontability).* Responsabilidade proativa por ataque *hacker*, que gera vazamento de dados, inclusive não sensíveis. É direito do titular de dados ter acesso às informações sobre os dados vazados.	Art. 5º, Art. 6º, X Art. 17 Art. 18, VII, Art. 19, II, Arts. 20 a 22, Art. 42, §2º, Art. 43, III, Art. 44, III, Arts. 45, 49, 49 e 50.	Objetiva
11	REsp nº 2.121.904 – SP / Ministra Nancy Andrighi / Terceira Turma	Prudential do Brasil Seguros de Vida S/A x Pedro Henrique Camiloti	11/2/2025	Indenização por dano moral decorrente de vazamento de dados sensíveis de contrato de seguro de vida, com informações sobre saúde e filhos menores.	O vazamento de dados pessoais sensíveis fornecidos para a contratação de seguro de vida, por si só, submete o consumidor a riscos diversos (honra, imagem, intimidade, patrimônio, integridade física e segurança pessoal), representa falha na prestação do serviço e gera responsabilização objetiva da seguradora e dano moral presumido ao segurado.	Art. 2º, Art. 5º, I e II, Art. 6º, I, II, VI e X, Art. 7º, V, Art. 8º, §2º, Art. 11, Art. 14, §1º, Art. 42, §2º, Art. 43, Art. 44, Art. 45, Art. 48, §3º.	Objetiva