

A RESPONSABILIDADE CIVIL PELO VAZAMENTO DE DADOS NAS PLATAFORMAS DIGITAIS

Civil liability for data leaks on digital platforms

Jailson de Souza Araújo¹

André Rambo Batistella²

RESUMO

O presente estudo buscou analisar como se dá a responsabilização civil pelo vazamento de dados nas plataformas digitais. A pesquisa objetivou analisar de que forma o ordenamento jurídico brasileiro, em conjunto com o posicionamento jurisprudencial do Superior Tribunal de Justiça (STJ), contribui para a efetivação da responsabilização civil nas hipóteses de violações à privacidade resultantes do vazamento de dados pessoais em plataformas digitais. Para tanto, o artigo empregou o método hipotético dedutivo e a pesquisa descritiva, bibliográfica e de caráter qualitativo. Foi realizada, ainda, uma análise jurisprudencial de decisões proferidas entre 2022 e 2025 pelo STJ sobre a temática da responsabilização por violação de dados pessoais. A seleção das decisões concentrou-se nos

ABSTRACT

This study aimed to analyze how civil liability is assigned in cases of data breaches on digital platforms. It examined how the Brazilian legal framework, along with the case law of the Superior Court of Justice (STJ), contributes to the enforcement of civil liability in situations involving privacy violations resulting from the leakage of personal data online. The research adopted the hypothetical-deductive method and employed descriptive, bibliographic, and qualitative approaches. A case law review was also conducted, focusing on STJ decisions issued between 2022 and 2025 related to liability for personal data breaches. The selection was limited to the most recent three years, a period marked by the enforcement of the General Data Protection Law (LGPD – Law No. 13,709/2018) and the enactment of Constitutional Amendment No. 115/2022, which formally recognized the

-
- ¹ Doutor em Direito Econômico e Desenvolvimento pela PUC/PR (aprovado em Defesa Pública de Tese de Doutorado em 24.02.2021). Mestre em Direito Socioambiental e Sustentabilidade pela PUC/PR (aprovado em Defesa Pública de Dissertação de Mestrado em 26.03.2010). Professor permanente do Mestrado em Direito UNINTER. Professor de especialização e graduação (presencial e EAD). Ex-coordenador do programa de graduação em Direito do Centro Universitário Internacional UNINTER (2015-2022). E-mail para contato: jailson.a@uninter.com
 - ² Advogado OAB/RS 131.600. Especialista em Direito Notarial e Registral pela Faculdade Educamaís (2025). Especialista em Direito Civil e Processo Civil pela Faculdade de Direito da Fundação Escola Superior do Ministério Público do Rio Grande do Sul (2024). Bacharel em Direito pela Universidade de Cruz Alta (2023).

últimos três anos, critério justificado pela necessidade de examinar entendimentos mais recentes da Corte, já sob a vigência da Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018) e à luz da Emenda Constitucional nº 115/2022, que consagrou expressamente a proteção de dados pessoais como direito fundamental no ordenamento jurídico brasileiro. Pelo exame da jurisprudência do STJ, verificou-se que a Corte tem firmado o entendimento de que a exposição indevida de informações pessoais gera o dever de indenizar e configura dano moral presumido. No contexto das relações de consumo, a Corte aplica a responsabilidade objetiva do fornecedor, nos termos do artigo 14 do Código de Defesa do Consumidor (CDC) e do artigo 42 da LGPD, considerando que a falta de segurança no tratamento e na guarda dos dados pessoais caracteriza falha na prestação do serviço.

Palavras-chave: LGPD; Marco Civil da Internet; Responsabilidade civil objetiva; Dano moral presumido.

protection of personal data as a fundamental right under Brazilian law. The analysis revealed that the STJ has consistently ruled that the improper exposure of personal data gives rise to presumed moral damage and a corresponding duty to compensate. In consumer relations, the Court applies the principle of strict liability, as provided in Article 14 of the Consumer Protection Code (CDC) and Article 42 of the LGPD, recognizing that failures in data security and storage constitute service deficiencies.

Keywords: LGPD; Marco Civil da Internet; Strict civil liability; Presumed moral damages.

SUMÁRIO

1. INTRODUÇÃO. 2. FUNDAMENTOS JURÍDICOS DA PROTEÇÃO DE DADOS NO BRASIL.
3. A RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS.
4. REPARAÇÃO DE DANOS NA PERSPECTIVA DO SUPERIOR TRIBUNAL DE JUSTIÇA (STJ).
5. CONSIDERAÇÕES FINAIS. REFERÊNCIAS.

1 INTRODUÇÃO

Na sociedade contemporânea, marcada pela interconexão e pelo uso extensivo de tecnologias digitais, os dados pessoais assumem um expressivo valor econômico e estratégico. Informações pessoais são empregadas para impulsionar o desenvolvimento de produtos, promover cam-

panhas publicitárias, otimizar processos e ampliar o alcance de atividades empresariais e até governamentais. Todavia, o valor dos dados pessoais vai muito além de sua dimensão econômica, eis que está diretamente relacionado à privacidade, à autonomia individual e à dignidade da pessoa humana.

Nesta sociedade digital, proteger os dados pessoais é preservar os direitos fundamentais. Quando as informações circulam de forma massiva, o descuido ou o uso indevido de dados pessoais expõe o indivíduo a riscos de fraudes, discriminações e constrangimentos, que podem caracterizar danos materiais e morais. Assim, a Constituição da República Federativa do Brasil de 1988, em conjunto com a legislação infraconstitucional, desempenha um papel essencial ao detalhar e operacionalizar o tratamento de dados pessoais no Brasil, pois busca promover a transparência, segurança e responsabilização dos agentes públicos e privados.

Diante dos riscos provenientes do vazamento de informações pessoais, também cabe ao Poder Judiciário uma atuação proativa na garantia do direito à proteção dos dados pessoais. Essa atuação materializa-se, notadamente, pela responsabilização civil dos agentes de tratamento de dados que atuem em descumprimento com os deveres de segurança cibernética.

Assim, o estudo baseou-se no seguinte questionamento: em que medida o ordenamento jurídico brasileiro e o posicionamento do Superior Tribunal de Justiça (STJ) contribuem na responsabilização das violações de privacidade decorrentes do vazamento de dados pessoais em plataformas digitais? A pesquisa objetivou analisar de que forma o ordenamento jurídico brasileiro, em conjunto com o posicionamento jurisprudencial do Superior Tribunal de Justiça (STJ), contribui para a efetivação da responsabilização civil nas hipóteses de violações à privacidade resultantes do vazamento de dados pessoais em plataformas digitais.

Como objetivos específicos, a pesquisa buscou investigar os fundamentos jurídicos da proteção de dados pessoais no ordenamento brasileiro, analisar o regime de responsabilização civil previsto na Lei Geral de Proteção de Dados (LGPD) e examinar o posicionamento jurisprudencial

do Superior Tribunal de Justiça (STJ) sobre a responsabilização civil por vazamento de dados pessoais.

O tema em discussão possui relevância jurídica, econômica e social. Do ponto de vista jurídico, trata-se da efetivação de direitos fundamentais, como a privacidade, a dignidade da pessoa humana, notadamente após a consagração constitucional promovida pela Emenda nº 115/2022 e a vigência da Lei Geral de Proteção de Dados (LGPD). Economicamente, a proteção inadequada de dados pessoais representa um risco concreto para a reputação e a sustentabilidade das organizações, que podem sofrer sanções legais e perda de confiança por parte do mercado e dos consumidores. No plano social, os vazamentos de dados afetam diretamente a segurança e a integridade dos indivíduos, expondo-os a fraudes, discriminações e violações de direitos.

A pesquisa utilizou como principais fontes legais a Constituição Federal de 1988 e a Lei Geral de Proteção de Dados (LGPD), em conjunto com contribuições doutrinárias, tais como, Doneda (2011; 2018) e Mendes (2019). Destacou-se também a atuação da Ministra Nancy Andrigli no Superior Tribunal de Justiça (STJ), cujos votos têm sido fundamentais para firmar entendimentos sobre responsabilidade civil pelo vazamento de dados.

Para tanto, o artigo abordou, primeiramente, os fundamentos jurídicos da proteção de dados no Brasil e destacou a evolução normativa e constitucional do tema. Abordou-se, ainda, os marcos legais mais relevantes, como a Constituição Federal de 1988, o Marco Civil da Internet (Lei nº 12.965/2014), que introduziu os primeiros princípios sobre privacidade e proteção de dados na esfera digital, e, sobretudo, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), que consolidou um regime específico e abrangente para o tratamento de dados pessoais.

Em um segundo momento, versou quanto ao sistema de responsabilização civil na Lei Geral de Proteção de Dados (LGPD). Analisou-se as disposições legais que tratam das obrigações dos agentes de tratamento, bem como as hipóteses de responsabilização, as excludentes de responsabilidade e a possibilidade de inversão do ônus da prova, sendo também evidenciada a complementariedade entre a LGPD e o Código de Defesa do Consumidor (CDC).

Por fim, discorreu-se quanto ao posicionamento do Superior Tribunal de Justiça (STJ), no que diz respeito a reparação de danos ocasionados pelo vazamento de dados pessoais. A análise concentrou-se nas decisões mais recentes da Corte, proferidas entre 2022 e 2025, com o objetivo de identificar os critérios adotados para a fixação de indenizações e a interpretação das normas da LGPD em casos concretos.

O estudo realizou-se por intermédio do método hipotético dedutivo e da pesquisa descritiva, de caráter qualitativo. Ainda, o trabalho empregou a pesquisa bibliográfica, na qual empreendeu-se na coleta de informações em livros, artigos de revista e legislação. A análise jurisprudencial, por sua vez, consistiu em um estudo das principais decisões do Superior Tribunal de Justiça (STJ), alusivas a responsabilidade civil no caso de vazamento de dados, bem como dos argumentos utilizados pelos Ministros em seus votos. A seleção das decisões concentrou-se nos últimos três anos, critério justificado pela necessidade de examinar entendimentos mais recentes da Corte, já sob a vigência da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e à luz da Emenda Constitucional nº 115/2022.

Embora o ordenamento jurídico brasileiro tenha evoluído com a promulgação da Lei Geral de Proteção de Dados (LGPD) e do reconhecimento da proteção de dados como direito fundamental, ainda apresenta deficiências na efetiva responsabilização e reparação por vazamentos de dados em plataformas digitais, seja por lacunas normativas, seja por dificuldades estruturais na fiscalização e aplicação das sanções previstas.

2 FUNDAMENTOS JURÍDICOS DA PROTEÇÃO DE DADOS NO BRASIL

Em uma sociedade cada vez mais digital e conectada, os dados pessoais tornaram-se ativos valiosos. Informações pessoais são, constantemente, coletadas por empresas e instituições nos ambientes *on-line*³, cujo objetivo concentra-se em oferecer serviços personalizados, desenvolver

³ Do inglês, que traduzido significa conectado (tradução livre).

produtos e direcionar campanhas publicitárias. Esses dados alimentam algoritmos⁴ de inteligência artificial, movimentam a economia digital e influenciam decisões em diversas áreas, tais como, saúde, segurança e educação.

Esse desenvolvimento tecnológico tem provocado transformações significativas nas garantias fundamentais e nos direitos da personalidade. As inovações, ao ampliarem o fluxo de informações e as formas de expressão, também impõem novos desafios à privacidade e ao tratamento de dados pessoais, consolidando a necessidade de um diálogo permanente entre tecnologia e proteção da dignidade humana, o que representa uma das maiores preocupações dos juristas modernos (Doneda *et al.*, 2018).

Nesse sentido, proteger essas informações é essencial, não somente para garantir a privacidade dos indivíduos, mas também para evitar abusos, fraudes e práticas discriminatórias que podem decorrer do uso indevido ou não autorizado desses dados. Nesse sentido, Doneda (2011, p. 92):

O tratamento de dados pessoais, em particular por processos automatizados, é, no entanto, uma atividade de risco. Risco que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais [...]. Daí resulta ser necessária a instituição de mecanismos que possibilitem à pessoa deter conhecimento e controle sobre seus próprios dados – que, no fundo, são expressão direta de sua própria personalidade. Por este motivo, a proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito fundamental.

⁴ Os algoritmos, de acordo com o Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (2023, s/p.), “[...] levam em conta, principalmente, o comportamento e a interação do usuário com o seu conteúdo. Se o usuário interage, comentando, curtindo ou compartilhando suas publicações, maiores as chances do seu conteúdo continuar aparecendo na linha do tempo dele [...]”.

No direito brasileiro, a proteção dos dados pessoais pode ser vista tanto na seara constitucional quanto infraconstitucional. A Constituição da República Federativa do Brasil de 1988, passou a prever, expressamente, a proteção de dados como um direito fundamental, por intermédio da Emenda Constitucional nº 115, de 2022 (Brasil, 2022), que adicionou o inciso LXXIX⁵ ao artigo 5º (Brasil, 1988). A Emenda estabeleceu que a competência para organizar e fiscalizar a proteção e tratamento de dados pessoais será da União⁶, assim como, privativa da União⁷, para legislar quanto a proteção e o tratamento de dados pessoais (Brasil, 2022).

Todavia, mesmo antes da Emenda Constitucional nº 115/2022 (BRASIL, 2022), a proteção de dados pessoais já era compreendida como direito fundamental. A inviolabilidade da intimidade e da vida privada são tratados pela Constituição Federal de 1988 como direitos fundamentais, nos termos do artigo 5º, inciso X⁸, que também assegura uma indenização pelo dano moral ou material em caso de violação de tal direito. Da mesma forma, o inciso XII⁹, do artigo 5º do Texto Constitucional prevê a inviolabilidade do sigilo de dados (Brasil, 1988).

A compreensão da proteção de dados enquanto direito fundamental, antes da Emenda Constitucional nº 115/2022 (Brasil, 2022), também é reconhecida pelo Supremo Tribunal Federal (STF). Entre os dias 06 e 07 de maio de 2022, a Corte Suprema julgou a Ação Direta de Inconstitucio-

⁵ LXXIX. É assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais (Brasil, 2022, s/p.).

⁶ Artigo 21. Compete à União: [...] XXVI. Organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei (Brasil, 2022, s/p.).

⁷ Artigo 22. Compete privativamente à União legislar sobre: [...] XXX. Proteção e tratamento de dados pessoais (Brasil, 2022, s/p.).

⁸ Artigo 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X. São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (Brasil, 1988, s/p.).

⁹ XII. É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (Brasil, 1988, s/p.).

nalidade 6.387, na qual, por dez votos a um, reconheceu-se a existência de um direito fundamental a proteção de dados (Fachin, 2022).

No julgamento, o Ministro Gilmar Mendes afirmou que o direito à proteção de dados como direito fundamental partia de uma compreensão integrada da Constituição Federal de 1988 (Brasil, 1988), notadamente, pelo direito fundamental a dignidade da pessoa humana, da proteção constitucional a intimidade, bem como, do reconhecimento do *Habeas Data* como mecanismo de autodeterminação informativa (Brasil, 2022).

Ainda de acordo com Gilmar Mendes, a afirmação da proteção de dados pessoais como direito fundamental é uma necessidade nas sociedades atuais, sobretudo, face ao crescimento das comunicações e interações pela internet. Neste ambiente digital que coleta, armazena e processa informações pessoais de seus usuários, a proteção de dados pessoais é indispensável para a proteção da dignidade da pessoa humana (Brasil, 2022).

Como característica dos direitos fundamentais estão a eficácia direta e imediata, com aplicabilidade em dois planos distintos: a eficácia vertical, correspondente a relação entre o Estado e o indivíduo, e a eficácia horizontal, que compreende a relação entre particulares, a fim de evitar abusos tanto nas relações públicas quanto privadas (Moraes, 2023).

Nesse sentido, o direito à proteção de dados possui eficácia horizontal, sendo aplicável tanto no setor público quanto no privado. A aplicabilidade no setor privado é concretizada também pelo Código de Defesa do Consumidor (CDC), no artigo 43¹⁰ (BRASIL, 1990), o qual determina o acesso do consumidor aos seus dados pessoais arquivados em fichas ou cadastros (Mendes, 2018).

A proteção de dados pessoais também foi objeto de regulamentação legal em âmbito Federal. Em 23 de abril de 2014 promulgou-se a Lei Federal nº 12.965, denominada de Marco Civil da Internet, que regula a proteção de dados pessoais, direito e deveres do uso da Internet no Brasil. A le-

¹⁰ Artigo 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 (Brasil, 1990, s/p.).

gislação trouxe como um de seus princípios a proteção de dados pessoais, estabelecendo ainda que guarda desses dados devem preservar a intimidade, honra, vida privada e imagem das pessoas envolvidas, seja direta ou indiretamente (Brasil, 2014).

Como grande marco da legislação infraconstitucional, destaca-se a Lei Geral de Proteção de Dados (LGPD), promulgada em 14 de agosto de 2018, para dispor sobre o tratamento de dados pessoais no Brasil, seja ele feito por pessoa natural ou pessoa jurídica, de direito público ou de direito privado. Salienta-se que a Lei Federal foi fortemente influenciada pelo Regulamento Geral de Proteção de Dados Europeu, de maio de 2018 (TARUCE, 2023), e parte do princípio que todo dado pessoal possui valor. Por esta razão, adota um conceito amplo de dado pessoal, nos mesmos termos do Regulamento Europeu, definindo-o como a informação relacionada a uma pessoa natural identificada ou identificável (Teffé; Viola, 2020).

A legislação também adota um tratamento especial para aqueles dados pessoais considerados sensíveis. De acordo com o artigo 5º, inciso II (Brasil, 2018), da Lei Geral de Proteção de Dados (LGPD), considera-se como dado pessoal sensível aquele relacionado a “[...] 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”. Assim, nota-se que o dado sobre aspectos íntimos goza de especial proteção legislativa, tendo em vista que, por sua natureza, são capazes de gerar discriminação ou violação de direitos fundamentais, caso utilizada de forma inadequada.

A Lei Geral de Proteção de Dados (LGPD) foi elaborada em modelo preventivo de proteção de dados (Teffé; Viola, 2020), o que se manifesta em diversos mecanismos e obrigações impostas aos agentes de tratamento, como a necessidade de implementação de medidas técnicas e administrativas para proteger os dados pessoais, a realização de Relatórios de Impacto à Proteção de Dados Pessoais (DPIA) e a exigência de consentimento para o tratamento em determinadas hipóteses.

Dessa forma, os fundamentos jurídicos da proteção de dados no Brasil, alicerçados, principalmente, na Constituição Federal de 1988, no Marco Civil da Internet e na Lei Geral de Proteção de Dados (LGPD), estabelecem uma base normativa robusta na garantia do direito à proteção de dados pessoais. Contudo, para que tais direitos sejam efetivamente garantidos, é essencial analisar como o ordenamento jurídico brasileiro estrutura a responsabilidade civil aplicável em casos de violação à Lei Geral de Proteção de Dados (LGPD).

3 A RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A responsabilidade civil e a reparação de danos receberam tratamento na Seção III do capítulo VI da Lei Geral de Proteção de Dados (LGPD). Tais disposições, todavia, não possuem aplicação em todos os casos de responsabilização civil por vazamento de dados, podendo ceder espaço para aplicação de outras normas, de natureza mais específica a depender da relação jurídica em análise, como no caso das relações consumeristas, as quais demandam a aplicação do Código de Defesa do Consumidor (Capanema, 2020).

O artigo 42¹¹ da Lei Geral de Proteção de Dados (LGPD), trata da responsabilidade civil dos agentes de tratamento (controlador e operador) em caso de danos causados aos titulares de dados pessoais. O dispositivo estabelece que, nesses casos, o agente é obrigado a reparar o dano causado, inclusive, com a responsabilidade solidária entre operador

¹¹ Artigo 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. Parágrafo 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 (Brasil, 2018, s/p.).

e controlador, sempre que este descumprir as obrigações legais ou não seguir as instruções lícitas do controlador. Ademais, caso haja mais de um controlador diretamente envolvido no tratamento que deu origem ao dano, todos responderão solidariamente, exceto se puderem demonstrar que não houve culpa (Brasil, 2018).

Ainda no artigo 42, o parágrafo segundo¹² prevê a possibilidade de inversão do ônus da prova em favor do titular dos dados, a critério do Juiz, quando a alegação parecer verossímil, o titular for hipossuficiente para produzir provas, ou quando a produção dessas provas for excessivamente onerosa ao titular. A Lei Geral de Proteção de Dados (LGPD) também foi sensível a possibilidade ajuizamento de ações coletivas para reparação de dados, conforme previsão do parágrafo terceiro¹³ (Brasil, 2018).

A Lei também estabelece situações de exclusão de responsabilidade no artigo 43¹⁴. O dispositivo elenca três excludentes legais: quando provarem que não realizaram o tratamento de dados pessoais que lhes foi atribuído; quando, mesmo tendo realizado o tratamento, não houver violação à Lei Geral de Proteção de Dados (LGPD); ou, ainda, quando o dano decorrer exclusivamente de culpa do titular dos dados ou de terceiros (Brasil, 2018).

Portanto, percebe-se que as hipóteses de exclusão de responsabilidade são alinhadas com o sistema de responsabilidade civil, haja vista que o dever de reparação do dano só existe quando há nexo causal entre a conduta do agente de tratamento e o dano ocorrido (Soler, 2022).

¹² Parágrafo 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 (Brasil, s/p.).

¹³ Parágrafo 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 (Brasil, 2018, s/p.).

¹⁴ Artigo 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 (Brasil, 2018, s/p.).

Ainda, o artigo 45 da Lei Geral de Proteção de Dados (LGPD)¹⁵ prescreve que, no caso das relações de consumo, a violação do direito do titular de dados permanece sujeita às regras previstas na legislação específica. Nota-se, neste caso, a complementariedade das previsões da Lei Geral de Proteção de Dados (LGPD) com aquelas do Código de Defesa do Consumidor, notadamente, quanto a responsabilidade objetiva (Brasil, 2018).

Assim, no contexto das relações privadas regidas pelo Código Civil, prevalece o sistema de responsabilidade civil subjetiva¹⁶, o qual exige a demonstração de culpa do agente como condição para a responsabilização. A responsabilização depende da comprovação de uma violação de dever jurídico com dolo ou negligência. A Lei Geral de Proteção de Dados (LGPD), ao tratar das relações jurídicas envolvendo o tratamento de dados pessoais no âmbito privado, adota esse mesmo entendimento ao exigir, em regra, a verificação de culpa como pressuposto da responsabilidade (TASSO, 2020).

Dessa forma, nas hipóteses de tratamento de dados pessoais por particulares, a responsabilidade do agente de tratamento será reconhecida apenas mediante a comprovação de que este descumpriu um dever legal previsto na própria Lei Geral de Proteção de Dados (LGPD). No mesmo sentido, as excludentes de responsabilidade civil também seguirão as mesmas diretrizes do Código Civil, demonstrando a coerência entre os dois diplomas normativos (Tasso, 2020).

Importa ainda destacar os limites da aplicação territorial da Lei Geral de Proteção de Dados (LGPD). O artigo 3º da Lei estabelece a aplicação do alusivo preceito legal a qualquer operação de tratamento de dados pessoais, realizada por pessoa natural ou jurídica, de direito público ou

¹⁵ Artigo 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 (Brasil, 2018, s/p.).

¹⁶ Artigo 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 (Brasil, 2002, s/p.).

[...]

Artigo 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo (Brasil, 2002, s/p.).

privado, independentemente do meio utilizado, do País ou do local onde situa-se a organização ou o armazenamento dos dados (Brasil, 2018).

Logo, três situações promovem a aplicação da Lei Geral de Proteção de Dados (LGPD), quais sejam: primeiro, quando o tratamento de dados ocorre dentro do território brasileiro; segundo, quando o tratamento tem como finalidade oferecer bens, serviços ou tratar dados de indivíduos que estejam localizados no Brasil; e, por fim, quando os dados pessoais, objeto do tratamento, tenham sido coletados no Brasil (Brasil 2018).

O artigo 4º da Lei Geral de Proteção de Dados (LGPD), aborda as hipóteses de exclusão do seu alcance. Primeiramente, tal norma não se aplica ao tratamento de dados realizado por pessoa natural para fins, exclusivamente, particulares e sem finalidade econômica. Ademais, estão excluídos do âmbito da Lei Geral de Proteção de Dados (LGPD) os tratamentos de dados realizados com finalidades exclusivamente jornalísticas, artísticas ou acadêmicas (Brasil, 2018).

A Lei Geral de Proteção de Dados (LGPD) também não se aplica ao tratamento de dados destinados, unicamente, à segurança pública, à defesa nacional, à segurança do Estado ou a atividades de investigação e repressão de infrações penais. Além disso, exclui-se do escopo da Lei o tratamento de dados provenientes do exterior, desde que esses dados não sejam objeto de comunicação ou compartilhamento com agentes de tratamento localizados no Brasil, nem transferidos internacionalmente para outros Países, e contanto que o País de origem assegure um nível de proteção adequado e compatível com o previsto na norma supracitada (Brasil, 2018).

Outro fator de influência na responsabilização e prevenção de danos é o risco à imagem e reputação da empresa. O descumprimento das normas da Lei Geral de Proteção de Dados (LGPD) pode funcionar como uma forma exclusão da empresa em relações comerciais, tendo em vista que os *players* do mercado tendem a evitar riscos de responsabilização por ilícitos cometidos por terceiros na sua cadeia de negócios (Soler, 2022).

A Lei Geral de Proteção de Dados (LGPD) promoveu uma nova visão a respeito do regime da responsabilização civil. Nesse sentido, defen-

de-se a adoção de um regime diferenciado de reponsabilidade, pautada na aplicação de medidas concretas e proativas na proteção dos dados pessoais, sendo que, segundo Moraes e Queiroz (2019, p. 129), tal diploma legal *introduz*, indiretamente, ao secundar

[...] o regulamento europeu, uma mudança profunda em termos de responsabilização. Trata-se da sua união ao conceito de “prestação de contas”. Esse novo sistema de responsabilidade, que vem sendo chamado de “responsabilidade ativa” ou “responsabilidade proativa” encontra-se indicada no inciso X do art. 6º, que determina que às empresas que não é suficiente cumprir os artigos da lei; será necessário também “demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas. Portanto, “não descumprir a lei, não é mais suficiente”.

Assim, a regulamentação da responsabilidade civil no âmbito da Lei Geral de Proteção de Dados (LGPD) fornece o arcabouço normativo para reparação de danos na violação de dados pessoais nas plataformas digitais. Portanto, passa-se a análise dos posicionamentos do Superior Tribunal de Justiça (STJ) nas ações de responsabilidade civil por vazamento de dados pessoais.

4 REPARAÇÃO DE DANOS NA PERSPECTIVA DO SUPERIOR TRIBUNAL DE JUSTIÇA (STJ)

O Agravo em Recurso Especial nº 2.130.619/SP, julgado pela Segunda Turma do Superior Tribunal de Justiça (STJ) em 07/03/2023, trata de ação de indenização por danos morais ajuizada contra uma concessionária de energia elétrica, diante do vazamento e acesso de dados pessoais de particular por terceiros. No Tribunal de origem (Tribunal de Justiça do Estado de São Paulo), a sentença de primeiro grau foi reformada para julgar procedente a ação de indenização, sob o fundamento que o vazamento de dados represente falha na prestação de serviço capaz de gerar dever de indenizar (Superior Tribunal de Justiça, 2023).

No julgamento do Agravo em Recurso Especial, todavia, foi definido pelos Ministros que o vazamento de dados pessoais, por si só, não gera dano moral indenizável. Assim, não se trata de hipótese de dano moral presumido, sendo imprescindível que o titular dos dados demonstre o dano ocorrido pelo vazamento das informações pessoais (Superior Tribunal de Justiça, 2023).

No voto do Relator, Ministro Francisco Falcão, o qual foi acompanhado por unanimidade pela Segunda Turma, prevaleceu o entendimento de que os dados vazados se referiam aqueles corriqueiramente fornecidos em qualquer cadastro, não se enquadrando no conceito de dado pessoal sensível previsto no artigo 5º da Lei Geral de Proteção de Dados (LGPD). Por conseguinte, o conhecimento de tais dados por terceiros não causa de violação dos direitos de personalidade. Contudo, o Ministro Relator também afirmou que a situação seria diferente caso os dados pessoais vazados pelo concessionário de energia fossem classificados como dados pessoais sensíveis, capazes de expor a intimidade da pessoa natural (Superior Tribunal de Justiça, 2023):

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.

[...] 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. [...]

(AREsp n. 2.130.619/SP, relator Ministro Francisco Falcão, Segunda Turma, julgado em 7/3/2023, DJe de 10/3/2023.)

Outro julgamento relevante foi proferido nos autos do Recurso Especial nº 2115461/SP, em 08/10/2024, pela Terceira Turma do Superior Tribunal de Justiça (STJ). Tratava-se de uma ação de obrigação de fazer cumulada com indenização por danos morais diante de suposta comercialização de dados sem consentimento prévio da consumidora (Superior Tribunal de Justiça, 2024).

No Tribunal de origem (Tribunal de Justiça do Estado de São Paulo) foi mantida a decisão de primeiro grau que julgou improcedente a ação, sob o fundamento de que os dados pessoais divulgados não seriam considerados sensíveis, havendo a possibilidade de tratamento dessas informações para proteção do crédito (Superior Tribunal de Justiça, 2024).

Conforme entendimento firmado pela Terceira Turma do Superior Tribunal de Justiça (STJ), sob a relatoria da Ministra Nancy Andrighi e acolhido de forma unânime pelos demais integrantes do colegiado, ainda que a Lei Geral de Proteção de Dados (LGPD) autorize o tratamento de dados pessoais não sensíveis para fins de proteção ao crédito, mesmo sem o consentimento do titular, tal prerrogativa não se estende à disponibilização irrestrita dessas informações a quaisquer consulentes (Superior Tribunal de Justiça, 2024).

Assim, entenderam os Ministros que, diante da reconhecida divulgação indevida de dados pessoais para terceiros, há a ocorrência de dano moral presumido. Na ocasião, o patamar indenizatório adotado foi de R\$11.000,00 (onze mil reais) (Superior Tribunal de Justiça 2024):

CIVIL, CONSUMIDOR E PROCESSUAL CIVIL. RECURSO ESPECIAL. AÇÃO DE OBRIGAÇÃO DE FAZER C/C INDENIZAÇÃO POR DANOS MORAIS. [...] INOBSERVÂNCIA QUANTO AOS DEVERES LEGAIS DE TRATAMENTO DE DADOS PELO GESTOR DE BANCO DE DADOS. DISPONIBILIZAÇÃO INDEVIDA DE DADOS DO CADASTRO. DANO MORAL PRESUMIDO. RESPONSABILIDADE OBJETIVA DO GESTOR DE BANCO DE DADOS. CONFIGURAÇÃO.

[...] 10. A disponibilização indevida de dados pessoais pelos bancos de dados para terceiros caracteriza dano moral presumido (in re ipsa) ao cadastrado titular dos dados, diante, sobretudo, da forte sensação de insegurança por ele experimentada. [...]

(REsp n. 2.115.461/SP, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 8/10/2024, DJe de 14/10/2024.)

No Recurso Especial nº 2.147.374/SP, julgado em 03/12/2024, o Superior Tribunal de Justiça (STJ) voltou a analisar a controvérsia envolvendo o vazamento de dados pessoais não sensíveis e a consequente responsabilidade civil do agente de tratamento. A ação tratava de uma exposição de dados pessoais em decorrência de um incidente de segurança cibernética envolvendo uma concessionária de energia elétrica (Superior Tribunal de Justiça, 2024).

O Relator, Ministro Ricardo Villas Bôas Cueva, seguido por unanimidade pelo colegiado, destacou que a proteção de dados pessoais possui estatura de direito fundamental. Deste modo, devem os agentes de tratamento adotar todas as medidas de segurança necessários para proteção dos dados pessoais sob sua responsabilidade (Superior Tribunal de Justiça, 2024).

No caso, o tratamento de dados pessoais pela empresa ré foi irregular quando não ofereceu a segurança adequada. De acordo com os entendimentos dos Ministros, a mera alegação de ataque cibernético não afasta, por si só, a responsabilidade do agente de tratamento, sobretudo quando não há comprovação inequívoca de que todas as medidas de segurança exigíveis foram efetivamente implementadas. Portanto, a indenização por danos morais foi fixada em R\$10.000,00 (dez mil reais) (Superior Tribunal de Justiça, 2024):

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 EX-

CLUSIVA DE TERCEIRO. NÃO COMPROVADA. RESPONSABILIDADE CIVIL PROATIVA. EXPECTATIVA DE LEGÍTIMA PROTEÇÃO. COMPLIANCE E REGULAÇÃO DE RISCO DA ATIVIDADE. DIREITOS DO TITULAR. CONCRETIZAÇÃO. APLICABILIDADE.

[...]

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.

[...]

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).

[...]

(REsp n. 2.147.374/SP, relator Ministro Ricardo Villas Bôas Cueva, Terceira Turma, julgado em 3/12/2024, DJEN de 6/12/2024.)

Nos autos Recurso Especial nº 2121904/SP, julgado em 11/2/2025, o Superior Tribunal de Justiça (STJ) voltou a se debruçar sobre a responsabilidade civil por vazamento de dados. O caso concreto tratava de ação de obrigação de fazer cumulada com indenização por danos morais e materiais ajuizada em face de uma seguradora, diante da exposição de

dados pessoais e sensíveis do consumidor a terceiros (Superior Tribunal de Justiça, 2025).

No Tribunal de origem (Tribunal de Justiça do Estado de São Paulo) foi reconhecido que o vazamento de dados pessoais configura dano moral presumido, independentemente da comprovação de danos. Na oportunidade, fixou-se indenização por danos morais em favor do consumidor no patamar de R\$15.000,00 (quinze mil reais) (Superior Tribunal de Justiça, 2025).

No julgamento perante a terceira turma do Superior Tribunal de Justiça (STJ), a Ministra Relatora Nancy Andrighi, seguida por unanimidade no mérito, utilizou-se do Código de Defesa do Consumidor e da Lei Geral de Proteção de Dados (LGPD) para fundamentação do seu voto, aplicando ambas as legislações de maneira não excludente. A Relatora destacou a aplicação dos princípios da Lei Geral de Proteção de Dados (LGPD) no caso, sobretudo, o princípio da finalidade, da adequação e da transparência. Além disso, tratando-se de uma relação de consumo, a responsabilidade do fornecedor de serviços possui caráter objetivo, independentemente da demonstração de dolo ou culpa, tal como ensina o artigo 14 do C¹⁷ (Superior Tribunal de Justiça, 2025).

A Relatora pontuou que o terceira turma no Superior Tribunal de Justiça (STJ) possui entendimento de que a transferência de dados pessoais a terceiros, mesmo aqueles não sensíveis, quando realizados sem o consentimento do titular, acarreta a responsabilização do fornecedor. Todavia, tal responsabilização se torna ainda mais evidente e rigoroso quando se trata do vazamento de dados pessoais sensíveis (Superior Tribunal de Justiça, 2025).

Assim, restou definido pelo julgado que o vazamento de dados sensíveis gera a responsabilização objetiva do fornecedor e é razão suficiente para caracterização de dano moral presumido. Quanto ao patamar indenizatório pelos danos morais sofridos pelo consumidor diante da exposi-

¹⁷ Artigo 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 (Brasil, 1990, s/p.).

ção de suas informações pessoais, foi mantido o valor fixado na origem, de R\$15.000,00 (quinze mil reais) (Superior Tribunal de Justiça, 2025):

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.

[...] 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.

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.

[...] (REsp n. 2.121.904/SP, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 11/2/2025, DJEN de 17/2/2025.)

Ademais, o Superior Tribunal de Justiça (STJ) já enfrentou a controvérsia a respeito da responsabilidade civil por fraude bancária viabilizada pelo prévio vazamento de dados pessoais. No julgamento do Recurso Especial nº 2.187.854/SP, julgado pela Terceira Turma da Corte em 06/05/2025, estabeleceu que a ocorrência de fraude bancária, isoladamente, não gera dano moral indenizável. Contudo, quando estiver relacionada ao vazamento prévio de dados pessoais, utilizados pelos criminosos para aplicação do golpe, resta caracterizado o dano extrapatrimonial, cabendo a devida compensação (Superior Tribunal de Justiça, 2025).

O caso em exame tratava-se de uma fraude bancária contra a consumidora, na qual os criminosos utilizaram-se de informações sobre as operações bancárias e dados pessoais da vítima, obtidos da instituição financeira devido a falhas na rede de segurança, configurando falha na prestação do serviço (Superior Tribunal de Justiça, 2025).

A Relatora, Ministra Nancy Andrigli, seguida por unanimidade pelo colegiado, apontou que o vazamento de dados pessoais é situação praticamente irreparável, capaz de gerar uma sensação de insegurança e favorecer a prática de ilícitos por terceiros, o que não pode ser considerado como um mero dissabor. Na fundamentação do voto, destacou-se a responsabilidade objetiva do fornecedor no caso de vazamento de dados pessoais, assim como, a dispensa da necessidade de comprovação de prejuízo para a indenização por dano moral. Quanto a compensação por danos morais, restou fixada a condenação no valor de R\$ 8.000,00 (oito mil reais) (Superior Tribunal de Justiça, 2025):

DIREITO DO CONSUMIDOR. RECURSO ESPECIAL. FRAUDE BANCÁRIA. ATUAÇÃO CRIMINOSA. VAZAMENTO PRÉVIO DE DADOS PESSOAIS. DANOS EXTRAPATRIMONIAIS. PRESUMIDOS. SENSACÃO DE INSEGURANÇA. REFORMA DO ACÓRDÃO [...]

3. Embora a fraude bancária, por si só, não configure o dano moral indenizável, nos termos da jurisprudência desta Corte, quando o referido ilícito estiver associado ao prévio vazamento de dados pessoais - que possibilitaram aos falsários o conhecimento de informações privilegiadas sobre o titular da conta - caracteriza-se o dano extrapatrimonial, com o conseqüente dever de compensá-lo.

4. A configuração do dano moral decorre do evidente sentimento de insegurança experimentado pela parte ao perceber que seus dados foram disponibilizados indevidamente para terceiros, favorecendo a prática de atos ilícitos ou contratações fraudulentas por eventuais terceiros de má-fé.

[...]

(REsp n. 2.187.854/SP, relatora Ministra Nancy Andrigli, Terceira Turma, julgado em 6/5/2025, DJEN de 13/5/2025.)

Portanto, percebe-se que o Superior Tribunal de Justiça (STJ) já enfrentou a questão da responsabilização civil do agente de tratamento no caso de vazamento de dados pessoais em algumas oportunidades. Cons-

tatou-se, por intermédio dos julgamentos selecionados, que a Corte Superior tem compreendido que a exposição de informações pessoais gera danos morais presumidos, ou seja, independentemente de demonstração de dano, além dos danos materiais eventualmente sofridos. Por sua vez, no que concerne ao patamar indenizatório, observou-se que este tem oscilado entre R\$8.000,00 (oito mil reais) e R\$15.000,00 (quinze mil reais), a título de reparação por danos morais.

5 CONSIDERAÇÕES FINAIS

O direito à proteção de dados pessoais se encontra consolidado no ordenamento jurídico brasileiro como um direito fundamental, tanto pelo reconhecimento do Supremo Tribunal Federal em sede jurisprudencial, quanto pela expressa inclusão do direito à proteção de dados pessoais no rol de direitos e garantias fundamentais, promovida pela Emenda Constitucional nº 115/2022.

No cenário infraconstitucional, destaca-se o Marco Civil da Internet, por intermédio da Lei Federal nº 12.965/2014, como uma das primeiras legislações a estabelecer princípios e garantias para o uso da internet no Brasil. Nesse sentido, a Lei Geral de Proteção de Dados (LGPD), a Lei Federal nº 13.709/2018, representa o grande marco infraconstitucional sobre a proteção de dados pessoais, ao estabelecer regras específicas para o tratamento de dados pessoais e mecanismos de responsabilização em caso de descumprimento.

A Lei Geral de Proteção de Dados (LGPD) também disciplina expressamente as hipóteses de responsabilização civil dos agentes de tratamento em caso de violação das suas normas, especialmente no caso de vazamento de dados pessoais. Além disso, a legislação possui harmonia com o Código de Defesa do Consumidor (CDC), quando o tratamento de dados ocorre no âmbito de uma relação de consumo.

Pela análise das jurisprudências do Superior Tribunal de Justiça (STJ), notou-se que a Corte tem adotado o entendimento de que a exposição indevida de dados pessoais é suficiente para ensejar a condenação

por danos morais presumidos, independentemente da demonstração de prejuízo concreto, além da possibilidade de reparação por eventuais danos materiais sofridos.

Nos casos envolvendo relação de consumo, o Superior Tribunal de Justiça (STJ) tem aplicado a responsabilidade objetiva do fornecedor, fundamentada na falha na prestação do serviço, especialmente quanto à ausência de segurança no tratamento de dados, em consonância com o Código de Defesa do Consumidor (CDC). Nesse contexto, a Corte reconhece a existência de um diálogo normativo e complementaridade entre a Lei Geral de Proteção de Dados (LGPD) e o Código de Defesa do Consumidor (CDC).

Em relação ao valor das indenizações por danos morais fixadas pela jurisprudência do Superior Tribunal de Justiça (STJ), observa-se uma variação entre R\$ 8.000,00 (oito mil reais) e R\$ 15.000,00 (quinze mil reais), a depender das particularidades do caso. A gravidade da responsabilidade é potencializada quando se trata de vazamento de dados pessoais sensíveis, os quais gozam de proteção reforçada pela Lei Geral de Proteção de Dados (LGPD). Todavia, conforme entendimento mais recente da Corte, mesmo o vazamento de dados pessoais não sensíveis pode ensejar a indenização por danos morais.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 20 jun. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da República Federativa do Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/12965.htm. Acesso em: 23 jun. 2025.

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

em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 20 jun. 2025.

BRASIL. Superior Tribunal de Justiça. **Agravo em Recurso Especial nº 2.130.619/SP**. Brasília, DF: Superior Tribunal de Justiça, 2023. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202201522622&dt_publicacao=10/03/2023. Acesso em: 01 jul. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2115461/SP**. Brasília, DF: Superior Tribunal de Justiça, 2024. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202304537984&dt_publicacao=14/10/2024. Acesso em: 01 jul. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2.147.374/SP**. Brasília, DF: Superior Tribunal de Justiça, 2024. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202202209228&dt_publicacao=06/12/2024. Acesso em: 03 jul. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2.187.854/SP**. Brasília, DF: Superior Tribunal de Justiça, 2025. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202404690272&dt_publicacao=13/05/2025. Acesso em: 02 jul. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2121904/SP**. Brasília, DF: Superior Tribunal de Justiça, 2025. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202400312927&dt_publicacao=17/02/2025. Acesso em: 01 jul. 2025.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6.387/DF**. Brasília, DF: Supremo Tribunal Federal, 2020. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629>. Acesso em: 23 jun. 2025.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos**, a. 21, n. 53, p. 163-170, 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf. Acesso em: 22 jun. 2025.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico, Journal of Law**, v. 12, n. 2, p. 91-108, 2011. Disponível em: <https://dialnet.unirioja.es/servlet/articulo?codigo=4555153>. Acesso em 24 jul. 2025.

DONEDA, Danido *et al.* Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Pensar: Revista de Ciência Jurídica**, v. 23 n. 4, 2018. Disponível em: <https://ojs.unifor.br/rpen/article/view/8257/pdf>. Acesso em: 05 ago. 2025.

FACHIN, Zulmar. O direito fundamental à proteção de dados pessoais: análise da decisão paradigmática do STF na ADI 6.387-DF. **Revista Videre**, v. 14, n. 29, p. 298–313, 2022. Disponível em: <https://ojs.ufgd.edu.br/videre/article/view/15629>. Acesso em: 23 jun. 2025.

MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 12, n. 39, p. 185–216, 2019. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/655>. Acesso em: 30 jun. 2025.

MORAES, Alexandre de. **Direito Constitucional**. Rio de Janeiro, RJ: Atlas, 2023. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786559774944/>. Acesso em: 30 jun. 2025.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa. *In*: Proteção de dados pessoais: Privacidade versus avanço tecnológico. **Cadernos Adenauer**, a. XX, n. 3, p. 113-135, 2019.

Serviço Brasileiro de Apoio às Micro e Pequenas Empresas. **Como funcionam os algoritmos das redes sociais**. Brasília, DF: Sebrae, 2023. Disponível em: <https://sebrae.com.br/sites/PortalSebrae/artigos/como-funcionam-os-algoritmos-das-redes-sociais,d747b240aba76810VgnVCM1000001b00320aRCRD>. Acesso em: 30 jun. 2025.

SOLER, Fernanda Galera. **Proteção de dados**: reflexões práticas e rápidas sobre a LGPD. Rio de Janeiro, RJ: Expressa, 2022. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786553622500/>. Acesso em: 30 jun. 2025.

TARTUCE, Flávio. **Manual de Direito Civil**. Rio de Janeiro, RJ: Grupo GEN, 2023.

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**, a. 21, n. 53, p. 97-115, 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/download/662/506/1387>. Acesso em: 20 jun. 2025.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**, v. 9, n. 1, p. 1-38, 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/510>. Acesso em: 23 jun. 2025.

Recebido em 28 de agosto de 2025

Aprovado em 12 de setembro de 2025