IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS V

D598

Direito, governança e novas tecnologias V [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Vivianne Rigoldi; Jéssica Fachin; Rosane Teresinha Porto – Florianópolis: CONPEDI, 2026.

Inclui bibliografia
ISBN: 978-65-5274-589-7
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Direito. 3. Governança e novas tecnologias. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34

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

IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS V

Apresentação

O Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI), referência na difusão de pesquisas que abordam os novos fenômenos envolvendo o Direito, firma-se como espaço qualificado para apresentação de pesquisas produzidas na área das novas tecnologias em face do Direito.

O tema, recorrente nos artigos apresentados - o uso da inteligência artificial no âmbito jurídico, demonstra que a maior sociedade científica na área jurídica do Brasil se mantém atenta às inovações tecnológicas, ao avanço de diversas tecnologias, novas experiências no judiciário e nos escritórios de advocacia. Artigos, de alta relevância acadêmica e científica, destacam que o Direito não está imune a essas transformações e reiteram a necessidade de atenção aos desafios regulatórios do uso da inteligência artificial no mundo jurídico.

Diferentes pesquisas, apresentadas no Grupo de Trabalho 'Direito, Governança e Novas Tecnologias V', alertam para os efeitos deletérios da opacidade algorítmica,

referindo-se à falta de transparência sobre como sistemas de inteligência artificial e seus algoritmos produzem decisões, dentro e fora do judiciário. Nos textos, a governança

digital é debatida, com rigorosa visão científica, objetivando garantir o uso estratégico de tecnologias de informação e comunicação para gerir serviços, promover a segurança

de dados e integrar processos, de forma transparente, eficiente, com foco na participação ativa do cidadão na tomada de decisões.

algorítmico e tecnológico do sistema de justiça, englobando a investigação de cibercrimes, a digitalização de procedimentos policiais e judiciais, provas digitais e a

regulação de plataformas para combater conteúdos ilícitos.

Destarte, os artigos apresentados e os debates produzidos no Grupo de Trabalho ‘Direito, Governança e Novas Tecnologias V’ são essenciais para o

fortalecimento das diretrizes nacionais de regulação das novas tecnologias, pela formação de parâmetros normativos e procedimentais adequados à proteção dos

direitos humanos e fundamentais, à garantia da segurança da informação, à gestão de riscos e ao fortalecimento da transparência e do alinhamento legal no uso das novas

tecnologias no âmbito jurídico.

Por essas razões, as coordenadoras do GT convidam para a leitura do teor integral dos artigos, agradecendo a participação dos autores pesquisadores desta edição.

Vivianne Rigoldi/Jéssica Fachin/Rosane Porto

RESPONSABILIDADE CIVIL POR VAZAMENTO DE DADOS EM INSTITUIÇÕES FINANCEIRAS: CRITÉRIOS DO STJ APÓS A LGPD

CIVIL LIABILITY FOR DATA BREACHES IN FINANCIAL INSTITUTIONS: STJ CRITERIA AFTER THE LGPD

Eduardo Augusto do Rosário Contani
Fernanda Alves de Quadros

Resumo

No século XXI, a digitalização dos serviços financeiros transformou os dados pessoais em elemento permanente da relação entre consumidores e instituições bancárias, em que informações agora circulam em aplicativos e plataformas de pagamento. Nessa ótica, o vazamento de dados em instituições financeiras gera um conflito jurídico relevante, pois nem todo incidente informacional autoriza indenização automática, embora a ausência de prova imediata do prejuízo também não possa servir para enfraquecer a proteção do consumidor bancário. Diante disso, o problema que orienta este artigo é saber quais critérios vêm sendo utilizados pelo Superior Tribunal de Justiça, após a Lei Geral de Proteção de Dados Pessoais, para reconhecer ou afastar o dever de indenizar nesses casos. Em consonância com o problema, o objetivo é analisar os parâmetros adotados pelo STJ para a configuração da responsabilidade civil das instituições financeiras em hipóteses de vazamento de dados pessoais, com atenção à natureza das informações expostas, ao nexo causal, à falha na prestação do serviço e à demonstração do dano. Para tal fim, a pesquisa possui natureza qualitativa, finalidade exploratória e explicativa, com uso do método dedutivo. Quanto aos procedimentos, desenvolve-se por meio de pesquisa bibliográfica, legislativa e jurisprudencial, com análise da LGPD, do Código de Defesa do Consumidor, do Código Civil, da Lei Complementar nº 105/2001, de normas regulatórias do Banco Central e de julgados recentes do STJ.

Palavras-chave: Segurança da informação, Consumidor bancário, Privacidade, Proteção de dados, Jurisprudência

Law, to recognize or dismiss the duty to compensate in such cases. In line with this problem, the objective is to analyze the parameters adopted by the STJ for establishing the civil liability of financial institutions in cases involving personal data breaches, with attention to the nature of the information exposed, the causal link, the failure in service provision, and the demonstration of harm. To this end, the research is qualitative in nature, with exploratory and explanatory purposes, and adopts the deductive method. As for the procedures, it is developed through bibliographic, legislative, and case-law research, with an analysis of the LGPD, the Consumer Protection Code, the Civil Code, Complementary Law No. 105/2001, regulatory rules issued by the Central Bank, and recent decisions of the STJ.

Keywords/Palabras-claves/Mots-clés: Information security, Banking consumer, Privacy, Data protection, Case law

INTRODUÇÃO

A digitalização dos serviços financeiros alterou a forma como bancos, *fintechs* e demais instituições autorizadas lidam com seus clientes. A relação bancária, antes concentrada em contratos físicos, atendimento presencial e operações documentadas em papel, hoje em dia depende de cadastros digitais, autenticações remotas, aplicativos, armazenamento em nuvem, interoperabilidade de sistemas e circulação contínua de informações pessoais (Simões; Pedrosa, 2022).

Manzato e Maia (2024) explicam que, nesse ambiente, os dados do consumidor no século XXI integram a própria dinâmica de prestação do serviço, viabilizando a abertura de contas, a concessão de crédito, a prevenção a fraudes, a análise de perfil econômico e a execução de transações em tempo real.

Essa transformação, conquanto isso, aumentou os riscos decorrentes do tratamento inadequado de informações pessoais. Em instituições financeiras, o vazamento de dados pode expor elementos vinculados à vida econômica do cliente, à sua capacidade patrimonial, aos seus hábitos de consumo e à sua identidade civil (Lucena; Cruvinel, 2024). A partir da Lei Geral de Proteção de Dados Pessoais - LGPD, a discussão sobre responsabilidade civil ganhou novo enquadramento, visto que a segurança da informação agora dialoga com deveres de prevenção, transparência, governança, controle de riscos e resposta adequada a incidentes (BRASIL, 2018).

Perante essa realidade, surge o problema que orienta este artigo: quais critérios vêm sendo utilizados pelo Superior Tribunal de Justiça, após a LGPD, para reconhecer ou afastar o dever de indenizar em casos de vazamento de dados envolvendo instituições financeiras?

A questão exige cuidado porque nem todo incidente de segurança gera, automaticamente, dano indenizável, do mesmo modo que a alegação de ausência de prejuízo não pode servir para esvaziar a proteção jurídica do consumidor bancário. Entre esses dois extremos, o STJ tem construído parâmetros sobre prova do dano, natureza dos dados expostos, risco da atividade, falha na prestação do serviço, nexo causal e extensão da responsabilidade.

Nesse âmago, o objetivo deste artigo é analisar os critérios adotados pelo Superior Tribunal de Justiça, no período posterior à vigência da LGPD, para a configuração da responsabilidade civil das instituições financeiras em casos de vazamento de dados pessoais, com atenção à distinção entre mero incidente, exposição juridicamente relevante e dano passível de reparação.

Para tanto, a pesquisa adota natureza qualitativa, com finalidade exploratória e explicativa, uma vez que busca compreender a formação dos critérios jurídicos aplicados pelo

STJ e interpretar seus efeitos sobre a responsabilização das instituições financeiras. O método utilizado é o dedutivo, partindo-se do regime jurídico da proteção de dados, da responsabilidade civil e da defesa do consumidor para, em seguida, analisar sua aplicação em decisões judiciais concretas.

Quanto aos procedimentos, o estudo desenvolve-se por meio de pesquisa bibliográfica, legislativa e jurisprudencial, com consulta à LGPD, ao Código de Defesa do Consumidor, ao Código Civil, às normas regulatórias aplicáveis ao setor financeiro e aos julgados do STJ que tratam de vazamento de dados, dever de segurança e indenização por danos decorrentes de incidentes informacionais.

Ao fim, a relevância deste trabalho está em discutir um tema que se tornou recorrente na vida social e econômica, porém, que ainda apresenta grande incerteza na prática judicial. A definição dos critérios de responsabilização interessa ao consumidor, que precisa ter sua esfera informacional protegida; às instituições financeiras, que devem compreender o padrão jurídico de cuidado exigível; e ao próprio sistema de justiça, que precisa distinguir situações de risco abstrato, falha comprovada, dano presumível e dano demonstrado.

1 FORMAÇÃO HISTÓRICA E CONCEITUAL DO DIREITO À PRIVACIDADE

A ideia de vida privada foi se formando à medida que a convivência social passou a separar o que poderia ser exposto publicamente daquilo que deveria permanecer resguardado no espaço da pessoa, da família e das relações de confiança. Para Cancelier (2017), essa separação ganhou maior presença na modernidade, principalmente com a vida urbana, caracterizada por contatos mais frequentes, maior circulação de notícias e novas formas de observação sobre a conduta individual. De tal maneira, foi uma reação jurídica e moral ao desconforto provocado pelo olhar de terceiros, pela curiosidade social e pela conversão da vida pessoal em objeto de exposição pública.

A formulação moderna mais conhecida do direito à privacidade costuma ser associada ao artigo *The Right to Privacy*, publicado por Samuel Warren e Louis Brandeis na *Harvard Law Review*, em 15 de dezembro de 1890. O texto surgiu em um contexto muito marcado pelo avanço da imprensa sensacionalista, pela fotografia instantânea e pela circulação de notícias sobre a vida social das famílias norte-americanas, levando os autores a defenderem uma tutela contra a apropriação pública de aspectos da personalidade. A expressão *right to be let alone*, que se tornou clássica, traduzia uma privacidade de feição defensiva, voltada a impedir

intromissões indevidas na vida doméstica, afetiva e moral do indivíduo (Warren; Brandeis, 1890).

Essa origem ajuda a compreender que a privacidade moderna nasceu ligada ao conflito entre personalidade e publicidade. Naquele primeiro momento não se tratava de controlar bancos de dados, algoritmos ou fluxos informacionais, todavia, de preservar uma esfera de recolhimento diante da expansão de meios capazes de tornar pública uma informação antes restrita ao convívio privado. A preocupação recaía sobre cartas, fotografias, hábitos familiares, comentários íntimos e fatos da vida pessoal expostos sem consentimento, de modo que a privacidade era pensada como limite à curiosidade social e à exploração comercial da intimidade (Costa, 2019).

Com o tempo, essa concepção defensiva mostrou seus limites, considerando que a sociedade industrial e burocrática aumentou a capacidade de registro da vida das pessoas por empresas, repartições públicas, bancos, seguradoras, hospitais e escolas, de modo que a ameaça à privacidade já não vinha exclusivamente da imprensa ou da invasão física do lar. Com efeito, o problema passou a envolver cadastros, cruzamento de informações, vigilância administrativa e uso secundário de dados obtidos para uma finalidade e empregados para outra (Bolesina; Gervasoni, 2022).

Alan Westin foi terminante nessa virada conceitual ao compreender a privacidade como a possibilidade de o indivíduo, o grupo ou a instituição determinar quando, como e em que medida informações sobre si serão comunicadas a outras pessoas. Essa definição, formulada em 1967, ampliou o campo da privacidade, haja vista que retirou o tema da pura clausura doméstica e o conectou à circulação social da informação, permitindo perceber que uma informação pode ser conhecida por alguém e, ainda assim, continuar protegida contra usos incompatíveis com a relação que justificou sua entrega (Westin, 1967).

A experiência alemã também marcou esse processo. No julgamento sobre o censo populacional de 1983, o Tribunal Constitucional Federal alemão desenvolveu a noção de *informationelle Selbstbestimmung*, traduzida entre nós como autodeterminação informativa, a partir da dignidade da pessoa humana e do livre desenvolvimento da personalidade. A decisão identificou que a coleta e o tratamento estatal de dados, quando realizados sem limites, podem produzir efeitos de conformação do comportamento, já que o cidadão que não sabe quem conhece seus dados, para qual finalidade e por quanto tempo tende a ajustar sua conduta ao medo de ser observado (BVerfG, 1983).

No direito brasileiro, a Constituição de 1988 já continha um modelo de proteção da vida privada antes mesmo da positivação expressa da proteção de dados pessoais. O art. 5º, X,

assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem, com direito à indenização pelo dano material ou moral decorrente de sua violação, enquanto o art. 5º, XII, protege o sigilo da correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas. Posteriormente, a Emenda Constitucional nº 115, de 2022, acrescentou o inciso LXXIX ao art. 5º, assegurando, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais, além de fixar competência privativa da União para legislar sobre proteção e tratamento de dados pessoais (BRASIL, 1988).

Em 2018, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709 /2018) deu conteúdo normativo a esse movimento disciplinando o tratamento de dados pessoais em meios físicos e digitais, por pessoas naturais e jurídicas, de direito público e privado. Primeiramente, seu art. 1º já deixa claro a proteção dos direitos de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural, enquanto o art. 2º apresenta, entre seus fundamentos, o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico, a livre iniciativa, a defesa do consumidor e os direitos humanos (BRASIL, 2018).

Essa passagem da privacidade para a proteção de dados não elimina a intimidade nem a vida privada, porém, altera a forma de enxergar sua tutela. À luz dessa ótica, o saudoso Danilo Cesar Maganhoto Doneda trabalhou essa transição ao defender que a proteção de dados pessoais nasce quando a informação pessoal passa a ter circulação autônoma em sistemas técnicos, administrativos e econômicos, podendo afetar a pessoa mesmo sem exposição pública direta. Nesse ínterim, o dado pessoal é uma representação fragmentada da pessoa e pode orientar decisões sobre crédito, consumo, trabalho, saúde, segurança, educação e acesso a serviços (Doneda, 2021).

Na sociedade informacional, a lesão à privacidade pode ocorrer sem escândalo, sem publicação em jornal e sem violação do domicílio, podendo surgir de uma classificação automatizada, de uma inferência estatística, de uma base cadastral mal protegida, de uma transferência sem finalidade clara ou de um perfil comportamental usado para influenciar escolhas. Por essa razão, Bruno Bioni explica que a proteção de dados pessoais não pode ficar reduzida ao consentimento formal, uma vez que a assimetria entre titular e controlador muitas vezes impede que a vontade individual funcione como garantia real de autonomia (Bioni, 2021).

Por esse motivo, a doutrina contemporânea busca tratar a privacidade como categoria plural. Nesse prisma, Solove (2008) critica a busca por uma definição única e fechada, propondo uma compreensão por “semelhanças de família”, na qual diversas situações são reconhecidas como problemas de privacidade por compartilharem certos traços, ainda que não

tenham uma essência comum. Como por exemplo, podemos citar a vigilância, agregação, identificação, uso secundário, insegurança, exposição, divulgação e distorção em danos informacionais.

Essa leitura também pode ser usada para diferenciar privacidade e intimidade no direito brasileiro. Na doutrina de Pedro Lenza, a intimidade costuma remeter ao núcleo mais reservado da pessoa, ligado à vida afetiva, familiar, sexual, psíquica, corporal e espiritual, onde a exposição indevida pode atingir de forma pior a dignidade da pessoa humana. A vida privada, no que lhe concerne, alcança uma esfera mais ampla de autonomia, convivência, hábitos, escolhas, relações pessoais e informações que, embora não pertençam ao círculo mais secreto da pessoa, não devem ser apropriadas, devassadas ou utilizadas sem base jurídica adequada (Lenza, 2025).

José Afonso da Silva, ao tratar dos direitos da personalidade no plano constitucional, aproxima intimidade e vida privada, contudo, reconhece que a primeira se refere a um espaço mais interno da subjetividade, enquanto a segunda envolve a reserva da vida pessoal em sentido mais largo (Silva, 2014).

No plano civil, tal distinção dialoga com os arts. 20 e 21 do Código Civil. O art. 20 permite impedir a divulgação de escritos, transmissão da palavra, publicação, exposição ou utilização da imagem quando atingirem honra, boa fama, respeitabilidade ou finalidade comercial não autorizada, ressalvadas hipóteses legais. Outrossim, o art. 21 afirma que a vida privada da pessoa natural é inviolável, autorizando o juiz, a requerimento do interessado, a adotar providências para impedir ou fazer cessar ato contrário a essa norma (BRASIL, 2002).

O Código Civil, nessa seara, preserva uma tutela clássica da personalidade, ainda orientada por exposição, imagem, palavra e vida privada, enquanto a LGPD acrescenta uma visão informacional voltada ao tratamento, à finalidade, à necessidade, à segurança e à responsabilização.

A jurisprudência do Supremo Tribunal Federal também acompanhou essa mudança. Na ADI 6387, julgada em conjunto com as ADIs 6388, 6389, 6390 e 6393, o Plenário suspendeu a eficácia da Medida Provisória nº 954/2020, que determinava o compartilhamento, por empresas de telecomunicações, de nomes, números telefônicos e endereços de milhões de usuários com o IBGE, para produção de estatística oficial durante a pandemia de Covid-19. A relatora, ministra Rosa Weber, entendeu que não tinha critérios sobre finalidade, necessidade, segurança e responsabilização, reconhecendo a privacidade e a autodeterminação informativa como projeções dos direitos da personalidade e como fundamentos específicos da proteção de dados pessoais (BRASIL, 2020).

Outro precedente pertinente aqui é o RE 1.055.941/SP, Tema 990 da repercussão geral, no qual o STF admitiu o compartilhamento, sem autorização judicial prévia, de relatórios de inteligência financeira da UIF e de dados fiscais da Receita Federal com o Ministério Público e a polícia, desde que preservadas comunicações formais, sigilo, certificação do destinatário e mecanismos de controle. Ora, o caso é importante porque não trata a privacidade como barreira absoluta, porém, exige que a circulação de informações sensíveis observe finalidade institucional, rastreabilidade e controle contra desvios (BRASIL, 2019).

Desse percurso resulta uma compreensão mais refinada da privacidade. Em sua origem moderna, ela foi concebida como defesa contra a invasão do olhar público, o abuso da imprensa e a transformação da vida pessoal em espetáculo. Posteriormente, incorporou a proteção contra cadastros, vigilância, cruzamentos indevidos e usos secundários de informações.

Hoje, na sociedade informacional, a privacidade conserva seu conteúdo de reserva, recato e liberdade pessoal, ganhando uma dimensão de controle, transparência, finalidade e responsabilidade no tratamento de dados pessoais.

2 VAZAMENTO DE DADOS EM INSTITUIÇÕES FINANCEIRAS APÓS A LGPD

A vida econômica contemporânea deixou de se organizar tão-somente em torno da moeda, do contrato em papel e do atendimento presencial na agência bancária. Hoje, operações antes marcadas pela presença física passaram a ocorrer por meio de cadastros digitais, autenticações remotas, aplicativos e bases de dados integradas que acompanham o cliente em quase todas as etapas de sua relação com o sistema financeiro.

Diante disso, no século XXI, o cliente bancário entrega à instituição financeira parcelas sensíveis de sua identidade civil, de seus hábitos de consumo, de sua capacidade econômica, de seus vínculos sociais e de sua rotina cotidiana. Nesse caminho, a proteção de dados pessoais faz parte próprio padrão jurídico de qualidade do serviço bancário, haja vista que a segurança da relação financeira depende, cada vez mais, da forma como a instituição coleta, utiliza, guarda e protege as informações de seus clientes (Bacellar; Toporoski, 2024).

Para Beltrao (2025), essa transformação altera a compreensão tradicional da segurança bancária. Durante muito tempo, a segurança era associada à guarda de numerário, à prevenção de assaltos, à inviolabilidade de cofres e à integridade dos registros contábeis. Hoje, embora esses elementos permaneçam, a vulnerabilidade mais recorrente está na circulação informacional que permite identificar, perfilar, abordar e fraudar consumidores.

A instituição financeira, ao atuar em ambiente digital, administra uma infraestrutura de confiança, e essa confiança depende da preservação da confidencialidade, da integridade e da disponibilidade dos dados e sistemas que sustentam a relação bancária, questões essas presentes expressamente na Resolução BCB nº 85, de 8 de abril de 2021, ao exigir política de segurança cibernética compatível com o porte, o perfil de risco, o modelo de negócio, a natureza das atividades e a sensibilidade dos dados sob responsabilidade da instituição (BRASIL, 2021a).

No setor financeiro, consoante Tasso (2024), os dados cadastrais e os dados financeiros não possuem o mesmo grau de exposição jurídica, embora ambos sejam aptos a produzir prejuízos quando tratados de modo inseguro. Primeiramente, os dados cadastrais incluem nome, CPF, telefone, e-mail, endereço, agência, conta, instituição de relacionamento e chaves de pagamento, enquanto dados financeiros alcançam saldos, extratos, operações, limites de crédito, histórico de transações, investimentos, renda presumida, perfil de risco e comportamento de consumo.

A distinção é necessária porque nem todo vazamento envolve senha, saldo ou extrato, porém a exposição de dados aparentemente simples pode abastecer golpes de engenharia social, abertura indevida de contas, contratação fraudulenta de crédito e ataques direcionados ao consumidor, em dinâmica conhecida como *phishing*, *spoofing* e *account takeover* (Geldenhuys, 2024)

Os incidentes envolvendo o Pix são exemplos dessa zona de risco. Em setembro de 2021, o Banco Central comunicou acesso indevido a dados cadastrais vinculados a chaves Pix sob responsabilidade do Banco do Estado de Sergipe, caso que alcançou centenas de milhares de chaves. Em janeiro de 2022, nova comunicação pública envolveu 160.147 chaves Pix sob guarda da Acesso Soluções de Pagamento, com exposição de nome do usuário, CPF, instituição de relacionamento, agência e número de conta, em ocorrência verificada entre 3 e 5 de dezembro de 2021. O Banco Central registrou que não houve exposição de senhas, saldos ou extratos, todavia, a própria necessidade de comunicação pública mostrou que dados cadastrais, no ecossistema financeiro digital, possuem aptidão lesiva quando associados a serviços de pagamento instantâneo (Agência Brasil, 2022).

O consumidor não escolhe o modelo de segurança do aplicativo, não audita APIs, não analisa contratos de *cloud computing*, não controla *logs* de acesso, não avalia políticas de autenticação multifator e, em geral, sequer sabe quantos operadores participam do tratamento de seus dados. De tal forma, a vulnerabilidade é técnica, informacional e estrutural, conforme a leitura consumerista desenvolvida a partir do art. 4º, I, do Código de Defesa do Consumidor, que reconhece a posição desigual do consumidor no mercado de consumo (Marques, 2022).

A LGPD, no art. 6º, VII, adota a segurança como princípio do tratamento de dados pessoais, exigindo medidas técnicas e administrativas aptas a proteger os dados contra acessos não autorizados e situações acidentais ou ilícitas. O art. 46, por sua vez, transforma essa diretriz em dever concreto dos agentes de tratamento, enquanto o art. 50 estimula regras de boas práticas e governança que levem em conta a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos relacionados ao tratamento (BRASIL, 2018).

No setor financeiro, esses comandos precisam ser interpretados com maior exigência prática, visto que a atividade bancária envolve coleta massiva, tratamento continuado e alto potencial de dano patrimonial e extrapatrimonial (Manzato; Maia, 2024).

Levando isso em consideração, na acepção de Cavoukian (2011), o dever jurídico de segurança exige governança de dados desde a concepção do produto, com mapeamento de fluxos informacionais, classificação de bases, controle de acesso por necessidade funcional, segregação de ambientes, criptografia, retenção adequada de *logs*, gestão de vulnerabilidades, testes periódicos, plano de resposta a incidentes, treinamento de equipes e avaliação criteriosa de terceiros.

Isto é, trata-se de incorporar *privacy by design* e *security by design* à rotina da instituição, evitando que a proteção de dados apareça somente depois do incidente, como resposta reputacional ou formalidade regulatória (Cavoukian, 2011).

A Resolução CMN nº 4.893, de 26 de fevereiro de 2021, segue a mesma linha ao disciplinar a política de segurança cibernética e os requisitos para contratação de serviços de processamento, armazenamento de dados e computação em nuvem pelas instituições financeiras autorizadas a funcionar pelo Banco Central. Para isso, a norma exige estrutura documental, procedimentos de prevenção e resposta, avaliação de riscos na terceirização e mecanismos de acompanhamento, aproximando a segurança informacional da governança prudencial do sistema financeiro (BRASIL, 2021b).

Dito de outra forma, a proteção de dados bancários não se atém à relação individual entre banco e cliente, já que falhas sucessivas de segurança podem afetar a confiança pública nos meios digitais de pagamento e na própria higidez do mercado financeiro (Jarude; Silveira, 2021).

No Pix, o Manual de Segurança, em versão de 5 de junho de 2025, descreve requisitos voltados à criptografia da comunicação, autenticação, assinatura digital, gestão de certificados, segurança de APIs, QR Codes dinâmicos e manutenção de *logs* de auditoria. O documento também vincula registros de auditoria à rastreabilidade das mensagens e das transações no ecossistema de pagamentos instantâneos, deixando claro que segurança, prova e

responsabilização caminham juntas no ambiente financeiro digital (Banco Central do Brasil, 2025).

A partir dessas premissas, quando a exposição de dados bancários ultrapassa o campo da irregularidade informacional e ingressa no terreno do dano indenizável? Essa questão exige cautela, pois a responsabilização não pode decorrer de uma fórmula automática, nem pode esvaziar a proteção do consumidor diante de riscos que ele não controla.

É nessa nuance que se abre o capítulo seguinte. Depois de analisados os deveres de segurança, prevenção e governança aplicáveis às instituições financeiras, é preciso compreender como o Superior Tribunal de Justiça vem delimitando o dever de indenizar após a LGPD, especialmente quanto à prova do dano, ao nexo causal, à falha do serviço e à vulnerabilidade do consumidor no ambiente bancário digital.

3 RESPONSABILIDADE CIVIL E CRITÉRIOS DO STJ PARA O DEVER DE INDENIZAR

Nessa parte final do artigo, a responsabilização civil por incidentes de dados no setor financeiro só pode ser compreendida a partir da mudança silenciosa que atingiu a própria experiência bancária. O banco, antes associado ao espaço físico, ao gerente, ao contrato impresso e ao sigilo guardado em arquivos internos, hoje em dia é um ambiente de circulação contínua de informações no ambiente *online*.

A proteção de dados, nessa toada, está próxima da tutela da personalidade, considerando que a informação pessoal agora integra a projeção social do indivíduo em ambientes automatizados de decisão, classificação e risco (Doneda, 2021).

Essa mutação explica por que a Lei Geral de Proteção de Dados não deve ser trata de forma isolada. No campo bancário, ela incide ao lado do Código de Defesa do Consumidor, da Lei Complementar nº 105/2001, da regulação prudencial do Banco Central e da jurisprudência histórica do Superior Tribunal de Justiça sobre risco da atividade financeira.

O art. 14 do Código de Defesa do Consumidor já atribuía ao fornecedor de serviços responsabilidade objetiva pelos defeitos relativos à segurança da atividade prestada, independentemente da demonstração de culpa. Essa lógica foi posteriormente aproximada do regime de proteção de dados pessoais, especialmente porque o art. 44 da LGPD considera irregular o tratamento que deixa de oferecer a segurança que o titular pode legitimamente esperar, à luz da forma de realização do tratamento, de seus resultados e dos riscos envolvidos (BRASIL, 2018).

No setor bancário, a Súmula 479 do STJ radicou o entendimento de que fraudes e delitos praticados por terceiros, quando vinculados ao funcionamento da atividade financeira, integram o fortuito interno da instituição, afastando a tentativa de transferir ao consumidor os riscos próprios do serviço prestado (BRASIL, 2012).

A maior mudança está no modo como o STJ passou a construir critérios após a vigência da LGPD. Para tanto, a Corte não tem adotado uma visão automática segundo a qual todo vazamento gera dano moral, nem uma posição oposta que esvazie a proteção do titular. O caminho jurisprudencial tem sido casuístico, com atenção à natureza dos dados, à origem provável do vazamento, ao nexo entre a falha informacional e a fraude, ao grau de sigilo das informações, à existência de dano patrimonial ou moral demonstrável e, em certos contextos, à possibilidade de dano moral presumido.

O primeiro marco desse percurso recente aparece no AREsp 2.130.619/SP, julgado pela Segunda Turma, sob relatoria do ministro Francisco Falcão, em decisão divulgada em 17 de março de 2023. O caso envolvia a Eletropaulo e o vazamento de dados como nome, data de nascimento, endereço e número de documento de identificação. O Tribunal de Justiça de São Paulo havia fixado indenização de R$ 5 mil, mas o STJ reformou o acórdão, entendendo que esses elementos eram dados pessoais comuns, não sensíveis, e que o dano moral não poderia ser presumido só pelo risco abstrato de fraude ou incômodo (BRASIL, 2023).

O critério extraído do precedente afasta a indenização automática quando a exposição atinge dados ordinários, sem prova de repercussão concreta sobre a esfera da personalidade. A Segunda Turma afirmou que, salvo no caso de informações sensíveis, o vazamento de dados pessoais não gera, por si só, dano moral indenizável, exigindo prova do efetivo prejuízo.

Malgrado isso, tal precedente não pode ser movido mecanicamente para o setor bancário. Dados cadastrais comuns, como nome e CPF, circulam em inúmeras bases públicas e privadas, enquanto dados bancários, financeiros e transacionais possuem outra espessura jurídica, pois indicam relações de crédito, saldo devedor, produto contratado, parcelas, operações ativas e passivas, canais de atendimento e, muitas vezes, o momento exato de vulnerabilidade do consumidor.

A Lei Complementar nº 105/2001, em seu art. 1º, determina que as instituições financeiras conservem sigilo em suas operações ativas, passivas e serviços prestados (Brasil, 2001). Em ambiente bancário, é preciso verificar se a informação exposta estava sob guarda da instituição em razão exclusiva ou predominante da atividade financeira por ela exercida. O próprio STJ registrou, no REsp 2.077.278/SP, que informações sobre operações bancárias são,

em regra, de tratamento exclusivo por instituições financeiras e que seu armazenamento inadequado pode caracterizar defeito do serviço.

O REsp 2.077.278/SP, julgado em 3 de outubro de 2023 pela Terceira Turma, sob relatoria da ministra Nancy Andrighi, é o precedente mais importante para o tema específico das instituições financeiras após a LGPD. O caso tratou do chamado "golpe do boleto". A consumidora buscava quitar dívida decorrente de financiamento, mas efetuou pagamento de boleto falso emitido por estelionatários que conheciam informações específicas de sua relação com o banco (BRASIL, 2023).

A peculiaridade do caso estava no grau de precisão dos dados utilizados pelos criminosos, pois eles sabiam que a vítima era cliente da instituição, tinham conhecimento do *e-mail* encaminhado para quitação da dívida e dominavam informações do financiamento, como quantidade de parcelas em aberto e saldo devedor. A Terceira Turma concluiu, por unanimidade, que o tratamento indevido de dados pessoais bancários configura defeito na prestação do serviço quando essas informações facilitam a fraude contra o consumidor. No acórdão, votaram com a relatora os ministros Humberto Martins, Ricardo Villas Bôas Cueva e Moura Ribeiro, com ausência justificada do ministro Marco Aurélio Bellizze.

Ou seja, para imputar o dano à instituição financeira, não basta afirmar que houve vazamento, sendo necessário analisar quais dados estavam em poder dos criminosos, tendo em vista que a natureza da informação permite reconstruir a origem provável da falha. Dados genéricos podem ter múltiplas fontes, enquanto dados bancários individualizados, vinculados a contrato, saldo, parcela, canal de negociação ou operação financeira, indicam uma trilha causal muito mais próxima da instituição.

A ministra Nancy Andrighi foi precisa ao afirmar que os nexos de causalidade e imputação dependem da hipótese concretamente analisada, exigindo averiguação exata dos dados detidos pelos estelionatários. A partir daí, impede a banalização indenizatória e a blindagem excessiva dos bancos diante de fraudes sofisticadas. O critério, em linguagem de *common law*, aproxima-se de uma espécie de *data provenance test*, ou seja, um teste de procedência dos dados, já que a origem provável da informação passa a orientar a imputação civil.

A LGPD entra nesse raciocínio como parâmetro de defeito. Para isso, o art. 42 prevê reparação por dano patrimonial, moral, individual ou coletivo causado em violação à legislação de proteção de dados, enquanto o art. 44 move a atenção para a segurança esperada no tratamento. No setor financeiro, essa segurança esperada é mais elevada, haja vista que o banco

atua em atividade de risco, administra informações protegidas por sigilo legal e dispõe de capacidade técnica superior para prevenir incidentes (BRASIL, 2018).

A partir desse quadro, os critérios do STJ podem ser organizados em uma sequência lógica. O primeiro é a classificação do dado, onde dados comuns, como nome, endereço e documento, em regra exigem prova do dano, salvo quando associados a uma forma ilícita de disponibilização capaz de afetar a personalidade. Já os dados sensíveis, definidos no art. 5º, II, da LGPD, recebem proteção maior, uma vez que dizem respeito à origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, saúde, vida sexual, genética ou biometria.

Os dados bancários não são automaticamente sensíveis no sentido técnico da LGPD, mas carregam sigilo próprio por força da LC nº 105/2001 e podem adquirir alta carga lesiva quando associados a operações financeiras reais. O erro está em tratar dado bancário como uma singela informação cadastral, pois uma coisa é o nome do consumidor, outra é o conjunto formado por contrato ativo, saldo devedor, parcelas pendentes e intenção de quitação.

O segundo critério é a vinculação funcional entre a informação exposta e a atividade bancária. No REsp 2.077.278/SP, a responsabilidade foi reconhecida porque os dados usados no golpe pertenciam ao núcleo da operação financeira e eram conhecidos pelos fraudadores de modo incompatível com uma obtenção casual. Já nos casos em que o consumidor apenas afirma que golpistas possuíam nome, telefone ou CPF, sem demonstrar conexão com dados sigilosos do serviço bancário, o nexo é enfraquecido.

Tal distinção dialoga com a teoria do risco do empreendimento, considerando que a responsabilidade objetiva não transforma o banco em segurador universal de todos os fatos ilícitos praticados contra seus clientes, embora imponha reparação quando a fraude utiliza brechas informacionais ligadas ao serviço prestado (Miragem, 2024).

O terceiro critério é a prova do nexo causal em ambiente de engenharia social. É possível afirmar que fraudes bancárias contemporâneas raramente decorrem de um único ato, combinando vazamento de dados, manipulação psicológica, simulação de atendimento, boletos adulterados, falsas centrais telefônicas, dispositivos cadastrados e operações fora do padrão. O STJ passou a observar se a instituição financeira poderia ter percebido a anormalidade do comportamento transacional.

Esse ponto ganhou importância nos REsp 2.222.059/SP e REsp 2.229.519/SP, julgados pela Terceira Turma, sob relatoria do ministro Ricardo Villas Bôas Cueva, em decisão divulgada em 21 de outubro de 2025. Os casos tratavam do golpe da falsa central de atendimento, com prejuízo de R$ 143 mil em pagamentos indevidos em um dos processos, contratação de

empréstimo de R$ 13 mil e pagamento de boleto de R$ 11 mil na função crédito, tudo em contraste com o perfil de um correntista que realizava poucas movimentações mensais. O STJ concluiu que bancos e instituições de pagamento devem indenizar quando falhas de segurança ou de detecção de operações suspeitas viabilizam a fraude.

Nesses julgados de 2025, a Corte ampliou o olhar para além do vazamento em sentido estrito. O dever de segurança passa a incluir mecanismos de identificação de transações atípicas, com análise de valor, horário, local, intervalo entre operações, sequência de atos, meio utilizado e contratação de empréstimos imediatamente antes de pagamentos suspeitos. A validação acrítica de operações incompatíveis com o perfil do cliente, especialmente quando combinada com indícios de engenharia social, é considerado pelo STJ um defeito de serviço.

O quarto critério está relacionado ao dano. A jurisprudência atual diferencia dano patrimonial, dano moral comprovado e dano moral presumido. No vazamento de dados pessoais comuns, a orientação do AREsp 2.130.619/SP exige demonstração efetiva de prejuízo ou abalo. Já no vazamento de dados sensíveis, a Terceira Turma caminhou em sentido mais protetivo no REsp 2.121.904/SP, julgado em 11 de fevereiro de 2025, sob relatoria da ministra Nancy Andrighi, envolvendo contrato de seguro de vida.

O consumidor havia contratado seguro em julho de 2018 e, dois anos depois, foi informado sobre incidente de cibersegurança que expôs dados de propostas, incluindo nome, CPF, endereço, dados de saúde, bens, beneficiários e, em alguns casos, conta-corrente e agência. A condenação, fixada em R$ 10 mil no primeiro grau e majorada para R$ 15 mil pelo TJSP, foi mantida pelo STJ, que reconheceu responsabilidade objetiva e dano moral presumido diante da exposição de dados sensíveis (BRASIL, 2025).

O Informativo 842 do STJ registrou a tese de que, no vazamento de dados pessoais sensíveis fornecidos para contratação de seguro de vida, há responsabilização objetiva da seguradora e dano moral presumido.

Embora esse precedente envolva seguradora, sua lógica interessa ao setor financeiro considerando que muitas instituições lidam com dados híbridos, financeiros e pessoais, em produtos de crédito, previdência, seguros, investimentos e cadastro de risco. Quando a base exposta contém informações sobre saúde financeira, beneficiários, renda, patrimônio, investimentos, endividamento ou padrões de consumo, o exame do dano não pode ficar preso à etiqueta formal de dado comum.

Dessarte, nem todo dado financeiro é sensível em sentido legal, mas certos conjuntos informacionais podem produzir vulnerabilidade equivalente ou até superior à exposição de

dados considerados sensíveis, especialmente quando permitem fraude direcionada, extorsão, discriminação de crédito ou abordagem criminosa personalizada.

A tensão mais recente aparece nos julgados sobre bancos de dados de crédito. No REsp 2.201.694/SP, a Terceira Turma, por maioria, sob voto vencedor da ministra Nancy Andrighi, decidiu que a disponibilização a terceiros de informações pessoais armazenadas em banco de dados, sem comunicação prévia e sem consentimento quando exigido, viola direitos da personalidade e justifica dano moral presumido (BRASIL, 2025).

O caso em questão envolveu agência de informações de crédito e divulgação de dados como telefone. A Corte destacou que, no regime da Lei nº 12.414/2011, o gestor pode fornecer o *score* sem consentimento prévio e o histórico de crédito com autorização específica, mas não pode repassar diretamente informações cadastrais e de adimplemento fora dos limites legais. Para a maioria, a disponibilização indevida produz sensação de insegurança bastante para justificar reparação, caracterizando dano moral presumido e responsabilidade objetiva nesse cenário (BRASIL, 2025).

Poucos meses depois, a Quarta Turma adotou leitura mais restritiva no REsp 2.221.650/SP, julgado sob relatoria da ministra Isabel Gallotti e divulgado em 13 de fevereiro de 2026. A Turma decidiu que a simples disponibilização de dados pessoais não sensíveis no âmbito do cadastro positivo não gera, por si só, indenização por dano moral. O consumidor alegava comercialização de dados por serviços como "Acerta Essencial" e "*Data Plus*", requereu exclusão das informações e pediu R$ 11 mil por danos morais, mas a Corte exigiu prova de que houve disponibilização, compartilhamento ou comercialização indevida e de que isso causou abalo aos direitos de personalidade (BRASIL, 2026).

Esse aparente desencontro entre Terceira e Quarta Turmas deixou claro que a matéria ainda está em fase de acomodação jurisprudencial. A Quarta Turma afirmou que, para indenização, o titular deve comprovar efetiva disponibilização ou uso indevido e abalo relevante, afastando o dano moral presumido em dados não sensíveis no cadastro positivo (BRASIL, 2026).

Para as instituições financeiras, o dever de indenizar pode ser reconhecido quando a fraude ou a exposição decorre de informações bancárias que só poderiam estar sob guarda qualificada da instituição, quando operações atípicas foram validadas sem controles adequados, quando dados sensíveis ou de alta carga lesiva foram expostos, ou quando o banco de dados foi utilizado em desconformidade com as limitações legais de compartilhamento.

Em sentido oposto, a indenização pode ser afastada quando há apenas vazamento de dados comuns, sem prova de dano, sem demonstração de origem bancária, sem nexo com a

fraude e sem repercussão concreta sobre a personalidade do consumidor. Diante disso, os critérios do STJ após a LGPD podem ser sintetizados em cinco eixos.

a. a natureza do dado exposto, com distinção entre dados comuns, sensíveis, sigilosos bancários e conjuntos informacionais de alta lesividade;
b. a origem provável do vazamento, apurada pela especificidade das informações em poder dos criminosos;
c. o nexo entre falha informacional, fraude e prejuízo, sem presunções frágeis, mas com atenção à assimetria técnica entre consumidor e instituição;
d. o padrão de segurança esperado, definido pelo CDC, pela LGPD, pela LC nº 105/2001 e pela regulação cibernética do Banco Central;
e. a forma de comprovação do dano, que varia entre prova concreta, presunção em hipóteses de dados sensíveis ou exposição indevida qualificada, e reparação patrimonial quando há perda econômica demonstrada.

A jurisprudência ainda não alcançou estabilização plena, principalmente no confronto entre Terceira e Quarta Turmas quanto ao dano moral presumido em bancos de dados de crédito. Mesmo assim, já existe uma diretriz elementar para o setor bancário.

O dever de indenizar nasce da falha demonstrável na cadeia de tratamento, segurança ou resposta, associada a dados cuja natureza, origem e uso revelam risco juridicamente intolerável. Em matéria financeira, essa exigência é ainda mais severa, porque o consumidor entrega ao banco algo mais delicado que dinheiro, que é sua vida econômica traduzida em dados, e essa confiança, quando quebrada por deficiência imputável à instituição, reclama reparação à altura do risco assumido.

CONSIDERAÇÕES FINAIS

Ao longo do presente artigo, ficou notório que o vazamento de dados em instituições financeiras não pode ser tratado como um episódio comum da vida digital, nem como um fato que sempre gera indenização de modo automático. Entre esses dois extremos, encontra-se o ponto mais sensível da questão, que é saber quando a exposição de informações atinge a segurança, a confiança e a vida econômica do consumidor.

A conclusão a que se chega é que o STJ vem caminhando para uma interpretação mais cuidadosa da responsabilidade civil após a LGPD, averiguando quais dados foram expostos, de onde eles provavelmente vieram, como foram utilizados, que relação guardam com a atividade bancária e se contribuíram para uma fraude ou para uma violação real da esfera pessoal do

cliente. Com efeito, tal movimento evita a banalização das indenizações e a proteção insuficiente diante de falhas graves.

No ambiente financeiro, a confiança alcança também a forma como a instituição protege os rastros digitais da vida econômica do cliente. Por isso, quando dados bancários específicos são utilizados por fraudadores, quando operações incompatíveis com o perfil do consumidor são aceitas sem reação adequada ou quando a instituição falha em seus deveres de segurança, a reparação é consequência jurídica do risco assumido.

Portanto, o dever de indenizar deve acontecer quando a falha informacional supera o mero aborrecimento e atinge a posição de vulnerabilidade do consumidor, expondo-o a prejuízos, fraudes, constrangimentos ou insegurança real. Em uma sociedade em que a identidade financeira circula em bases digitais, proteger dados bancários é proteger a própria liberdade do cliente de participar da vida econômica sem ter sua confiança transformada em ponto de exploração.

REFERÊNCIAS

AGÊNCIA BRASIL. **BC comunica vazamento de dados de 160,1 mil chaves Pix**. Brasília, DF, 21 jan. 2022. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2022-01/bc-comunica-vazamento-de-dados-de-1601-mil-chaves-pix. Acesso em: 23 abr. 2026.

BACELLAR, Leandro Wünsche; TOPOROSKI, Elizeu Luiz. Clonagem de cartão de crédito sob a perspectiva da Lei Geral de Proteção de Dados. **Academia de Direito**, v. 6, p. 4374-4388, 2024.

BANCO CENTRAL DO BRASIL. **Manual de Segurança do Pix**. Versão 3.7. Brasília, DF: Banco Central do Brasil, 2025. Disponível em: https://www.bcb.gov.br/content/estabilidadefinanceira/cedsfn/Manual_de_Seguranca_PIX.pdf . Acesso em: 21 abr. 2026.

BANCO CENTRAL DO BRASIL. **Resolução BCB nº 85, de 8 de abril de 2021**. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem. Brasília, DF: Banco Central do Brasil, 2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=85&tipo=Resolu%C3%A7%C3%A3o%20BCB. Acesso em: 22 abr. 2026.

BELTRAO, Raquel Cesario. O controle e consentimento: os desafios da implantação da LGPD nas instituições financeiras no brasil e sua gestão de riscos. **Revista Ibmec de Direito**, v. 1, n. 2, 2025.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BOLESINA, Iuri; GERVASONI, Tássia Aparecida. A proteção do Direito Fundamental à privacidade na era digital e a responsabilidade civil por violação do direito à extimidade. **Novos Estudos Juridicos**, v. 27, n. 1, p. 87-109, 2022.

BRASIL. Conselho Monetário Nacional. **Resolução CMN nº 4.893, de 26 de fevereiro de 2021**. Dispõe sobre a política de segurança cibernética e sobre os requisitos para contratação de serviços de processamento, armazenamento de dados e computação em nuvem. Brasília, DF: Banco Central do Brasil, 2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893. Acesso em: 21 abr. 2026.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 abr. 2026.

BRASIL. **Lei Complementar nº 105, de 10 de janeiro de 2001**. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Brasília, DF: Presidência da República, 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm. Acesso em: 22 abr. 2026.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 22 abr. 2026.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 24 abr. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 abr. 2026.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 19 abr. 2026.

BRASIL. Superior Tribunal de Justiça. **Agravo em Recurso Especial nº 2.130.619/SP**. Relator: Ministro Francisco Falcão. Segunda Turma. Julgado em: 7 mar. 2023. DJe: 10 mar. 2023. Brasília, DF: Superior Tribunal de Justiça, 2023. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?CodOrgaoJgdr=&SeqCgrmaSessao=&dt=20230310&formato=PDF&nreg=202201522622&salvar=false&seq=178204788&tipo=5. Acesso em: 23 abr. 2026.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2.015.732/SP**. Relatora: Ministra Nancy Andrighi. Terceira Turma. Julgado em: 20 jun. 2023. DJe: 26 jun. 2023. Brasília, DF: Superior Tribunal de Justiça, 2023. Disponível em:

https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/07122023-Pesquisa-Pronta-destaca-responsabilidade-por-vazamento-de-dados-de-instituicao-financeira-.aspx. Acesso em: 23 abr. 2026.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2.077.278/SP**. Relatora: Ministra Nancy Andrighi. Terceira Turma. Julgado em: 3 out. 2023. DJe: 9 out. 2023. Brasília, DF: Superior Tribunal de Justiça, 2023. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?CodOrgaoJgdr=&SeqCgrmaSessao=&dt=20231009&formato=PDF&nreg=202301909798&salvar=false&seq=211820560&tipo=5. Acesso em: 23 abr. 2026.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2.121.904/SP**. Relatora: Ministra Nancy Andrighi. Terceira Turma. Julgado em: 11 fev. 2025. DJEN: 17 fev. 2025. Brasília, DF: Superior Tribunal de Justiça, 2025. Disponível em: https://scon.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisar&livre=%28%22REsp%22+adj+%28%222121904%22+ou+%222121904%22-SP+ou+%222121904%22%2FSP+ou+%222.121.904%22+ou+%222.121.904%22-SP+ou+%222.121.904%22%2FSP%29%29.prec%2Ctext. Acesso em: 25 abr. 2026.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2.201.694/SP**. Relatora: Ministra Nancy Andrighi. Terceira Turma. Julgado em: 2025. Brasília, DF: Superior Tribunal de Justiça, 2025. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2025/05092025-Disponibilizacao-indevida-de-informacoes-pessoais-em-banco-de-dados-gera-dano-moral-presumido.aspx. Acesso em: 25 abr. 2026.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2.221.650/SP**. Relatora: Ministra Maria Isabel Gallotti. Quarta Turma. Julgado em: 4 nov. 2025. Brasília, DF: Superior Tribunal de Justiça, 2025. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2026/13022026-Disponibilizacao-nao-autorizada-de-dados-pessoais-nao-sensiveis-em-cadastro-positivo-nao-gera-dano-moral-presumido.aspx. Acesso em: 25 abr. 2026.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2.222.059/SP**. Relator: Ministro Ricardo Villas Bôas Cueva. Terceira Turma. Julgado em: 7 out. 2025. Brasília, DF: Superior Tribunal de Justiça, 2025. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2025/21102025-Bancos-e-instituicoes-de-pagamento-devem-indenizar-clientes-por-falhas-que-viabilizam-golpe-da-falsa-central.aspx. Acesso em: 25 abr. 2026.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2.229.519/DF**. Relator: Ministro Ricardo Villas Bôas Cueva. Terceira Turma. Julgado em: 7 out. 2025. Brasília, DF: Superior Tribunal de Justiça, 2025. Disponível em: https://www.migalhas.com.br/arquivos/2025/10/BD61F8A920806B_RESP2229519.pdf. Acesso em: 25 abr. 2026.

BRASIL. Superior Tribunal de Justiça. **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. Brasília, DF: Superior Tribunal de Justiça, 2012. Disponível em:

https://scon.stj.jus.br/SCON/sumanot/toc.jsp?livre=%28sumula%20adj1%20479%29.sub. Acesso em: 26 abr. 2026.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6.387 MC-Ref/DF**. Tribunal Pleno. Relatora: Ministra Rosa Weber. Julgado em: 7 maio 2020. Brasília, DF: Supremo Tribunal Federal, 2020. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 25 abr. 2026.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 1.055.941/SP**. Tema 990 da repercussão geral. Tribunal Pleno. Relator: Ministro Dias Toffoli. Julgado em: 4 dez. 2019. Brasília, DF: Supremo Tribunal Federal, 2019. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5213056. Acesso em: 25 abr. 2026.

BUNDESVERFASSUNGSGERICHT. **Urteil vom 15. Dezember 1983 – 1 BvR 209/83 u. a.** Volkszählungsurteil. BVerfGE 65, 1. Karlsruhe: Bundesverfassungsgericht, 1983. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html. Acesso em: 25 abr. 2026.

CANCELIER, Mikhail Vieira de Lorenzi. O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. **Sequência (Florianópolis)**, p. 213-239, 2017.

CAVOUKIAN, Ann. **Privacy by Design:** The 7 Foundational Principles. Toronto: Information and Privacy Commissioner of Ontario, 2011.

COSTA, Mateus Stallivieri. **O Desenvolvimento Histórico da Privacidade–Análise da construção do conceito como pilar da dignidade humana**. Grupo Multifoco: Rio de Janeiro, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

GELDENHUYS, Kotie. SPOOFING UNMASKED Cheating criminals shatter trust. **Servamus Community-based Safety and Security Magazine**, v. 117, n. 10, p. 20-23, 2024.

JARUDE, Jamile Nazaré Duarte Moreno; SILVEIRA, Daniel. O sistema financeiro aberto (open banking) sob a perspectiva da regulação bancária e da lei geral de proteção de dados (LGPD). **Revista Jurídica da FA7**, v. 18, n. 2, p. 77-90, 2021.

LENZA, Pedro. **Direito constitucional**. 29. ed. São Paulo: SaraivaJur, 2025.

LUCENA, Emerson Yuri Rodrigues de Carvalho; CRUVINEL, Marcelo Pereira. **Proteção de dados nas instituições financeiras:** desafios e soluções. Ensaios Jurídicos: vol. 2. 1. ed. Belo Horizonte: Expert Editora, 2024.

MANZATO, Welington Júnior Jorge; MAIA, Isadora Candido. Respeito à privacidade: Implicações da LGPD para o mercado financeiro e direitos individuais. In: **Anais do CDU-Congresso de Direito UniCesumar**. 2024. p. 752-754.

MARQUES, Claudia Lima. **Contratos no Código de Defesa do Consumidor**: o novo regime das relações contratuais. 9. ed. São Paulo: Thomson Reuters Brasil, 2022.

MIRAGEM, Bruno. **Curso de direito do consumidor**. 9. ed. São Paulo: Thomson Reuters Brasil, 2024.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 37. ed. São Paulo: Malheiros, 2014.

SIMÕES, Lorena Soares Silva; PEDROSA, Lucas Silva. Os benefícios da digitalização dos serviços bancários. **Revista Interface Tecnológica**, v. 19, n. 2, p. 18-34, 2022.

SOLOVE, Daniel J. **Understanding privacy**. Cambridge: Harvard University Press, 2008.

TASSO, Fernando Antonio. **Sistemas Regulatórios de Dados Pessoais--2024**. Editora Foco, 2024.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, Cambridge, v. 4, n. 5, p. 193-220, 1890.

WESTIN, Alan F. **Privacy and freedom**. New York: Atheneum, 1967.