ReGeo
ISSN: 2177-3246

A (IN)APLICABILIDADE AUTOMÁTICA DO CÓDIGO DE DEFESA DO CONSUMIDOR PARA RESPONSABILIZAÇÃO CIVIL EM CASO DE VAZAMENTO DE DADOS PESSOAIS NO BRASIL

THE AUTOMATIC (IN)APPLICABILITY OF THE CONSUMER PROTECTION CODE FOR CIVIL LIABILITY IN CASE OF PERSONAL DATA LEAKS IN BRAZIL

LA (IN)APLICABILIDAD AUTOMÁTICA DEL CÓDIGO DE DEFENSA DEL CONSUMIDOR PARA LA RESPONSABILIDAD CIVIL EN CASO DE FUGAS DE DATOS PERSONALES EN BRASIL

10.56238/revgeov17n1-111

Camila de Cássia Batista
Mestranda em Direito
Instituição: Universidade Federal de Minas Gerais (UFMG)
E-mail: camila@valladao.com.br

Tereza Cristina Sorice Baracho Thibau
Doutora em Direito
Instituição: Universidade Federal de Minas Gerais (UFMG)
E-mail: tthibau@gmail.com

RESUMO
O presente artigo analisa a natureza da responsabilidade civil no ordenamento jurídico brasileiro nos casos de vazamento de dados pessoais, com especial enfoque na controvérsia acerca da aplicabilidade automática do Código de Defesa do Consumidor em face das disposições da Lei Geral de Proteção de Dados Pessoais. Partindo do contexto da sociedade da informação e do aumento significativo de incidentes de segurança no ambiente digital, examina-se o regime jurídico instituído pela LGPD, especialmente no que se refere aos agentes de tratamento, aos deveres de segurança e às hipóteses de responsabilização civil previstas nos artigos 42 a 45. Em seguida, investiga-se a incidência do microssistema consumerista nos casos de vazamento de dados pessoais, a partir da conceituação de consumidor e fornecedor, da adoção da teoria do risco do empreendimento e das excludentes legais aptas a romper o nexo causal. A pesquisa adota abordagem qualitativa, de natureza teórico-dogmática, sob o viés do método dedutivo, fundamentando-se em análise legislativa, doutrinária e jurisprudencial. No campo jurisprudencial, são examinadas decisões de tribunais estaduais e do Superior Tribunal de Justiça, evidenciando a ausência de uniformidade quanto à configuração da responsabilidade civil, à exigência de prova do dano e à caracterização do dano moral presumido, sobretudo diante da distinção entre dados pessoais comuns e sensíveis. Ao final, conclui-se que a aplicação do Código de Defesa do Consumidor aos casos de vazamento de dados pessoais não deve ocorrer de forma automática, devendo ser precedida da verificação concreta da existência de relação de consumo, em leitura sistemática e complementar com a LGPD, de modo a assegurar a efetiva proteção dos direitos fundamentais dos titulares dos dados, sem esvaziar a autonomia normativa do regime de proteção de dados pessoais.

Palavras-chave: Responsabilidade Civil. Vazamento de Dados Pessoais. Lei Geral de Proteção de Dados. Código de Defesa do Consumidor. Relação de Consumo.

ABSTRACT
This article analyzes the nature of civil liability in the Brazilian legal system in cases of personal data leaks, with a special focus on the controversy surrounding the automatic applicability of the Consumer Protection Code in light of the provisions of the General Personal Data Protection Law. Starting from the context of the information society and the significant increase in security incidents in the digital environment, we examine the legal regime established by the LGPD, especially with regard to processing agents, security duties, and the cases of civil liability provided for in Articles 42 to 45. Next, the incidence of the consumerist microsystem in cases of personal data leaks is investigated, based on the conceptualization of consumer and supplier, the adoption of the theory of business risk, and the legal exclusions capable of breaking the causal link. The research adopts a qualitative approach, of a theoretical-dogmatic nature, using the deductive method, based on legislative, doctrinal, and jurisprudential analysis. In the field of jurisprudence, decisions by state courts and the Superior Court of Justice are examined, highlighting the lack of uniformity regarding the configuration of civil liability, the requirement of proof of damage, and the characterization of presumed moral damage, especially in view of the distinction between common and sensitive personal data. In conclusion, it is concluded that the application of the Consumer Protection Code to cases of personal data leaks should not occur automatically, but should be preceded by a concrete verification of the existence of a consumer relationship, in a systematic and complementary reading with the LGPD, in order to ensure the effective protection of the fundamental rights of data subjects, without undermining the regulatory autonomy of the personal data protection regime.

Keywords: Civil Liability. Personal Data Leakage. General Data Protection Law. Consumer Protection Code. Consumer Relations.

RESUMEN
El presente artículo analiza la naturaleza de la responsabilidad civil en el ordenamiento jurídico brasileño en los casos de filtración de datos personales, con especial énfasis en la controversia sobre la aplicabilidad automática del Código de Defensa del Consumidor frente a las disposiciones de la Ley General de Protección de Datos Personales. Partiendo del contexto de la sociedad de la información y del aumento significativo de los incidentes de seguridad en el entorno digital, se examina el régimen jurídico establecido por la LGPD, especialmente en lo que se refiere a los agentes de tratamiento, las obligaciones de seguridad y los supuestos de responsabilidad civil previstos en los artículos 42 a 45. A continuación, se investiga la incidencia del microsistema consumista en los casos de fuga de datos personales, a partir de la conceptualización de consumidor y proveedor, de la adopción de la teoría del riesgo de la empresa y de las excepciones legales aptas para romper el nexo causal. La investigación adopta un enfoque cualitativo, de naturaleza teórico-dogmática, bajo el prisma del método deductivo, basándose en el análisis legislativo, doctrinal y jurisprudencial. En el campo jurisprudencial, se examinan las decisiones de los tribunales estatales y del Tribunal Superior de Justicia, poniendo de manifiesto la falta de uniformidad en cuanto a la configuración de la responsabilidad civil, la exigencia de prueba del daño y la caracterización del daño moral presunto, sobre todo ante la distinción entre datos personales comunes y sensibles. En definitiva, se concluye que la aplicación del Código de Defensa del Consumidor a los casos de fuga de datos personales no debe producirse de forma automática, sino que debe ir precedida de la verificación concreta de la existencia de una relación de consumo, en lectura sistemática y complementaria con la LGPD, a fin de garantizar la protección efectiva de los derechos fundamentales de los titulares de los datos, sin menoscabar la autonomía normativa del régimen de protección de datos personales.

Palabras clave: Responsabilidad Civil. Fuga de Datos Personales. Ley General de Protección de Datos. Código de Defensa del Consumidor. Relación de Consumo.

1 INTRODUÇÃO

As novas tecnologias digitais, especialmente as redes sociais, têm exercido papel significativo no aumento do número de dados pessoais que circulam no ambiente virtual, principalmente, em razão da forma como são estruturadas. Os usuários, que nas mídias tradicionais, como rádio e televisão, figuravam, tão somente, como meros expectadores, na internet, passaram a ser estimulados, por meio de ferramentas digitais, a compartilharem, cada vez mais, conteúdos sobre a sua vida pessoal e profissional, postando indiscriminadamente fotos, vídeos, comentários, links, etc.

Nesse contexto, nos últimos anos, os debates envolvendo a segurança cibernética intensificaram-se em todo mundo, especialmente, porque se tornaram frequentes incidentes de risco a segurança, como o vazamento de dados pessoais na internet, caracterizado pela exposição, divulgação e compartilhamento indevidos e não autorizados pelos usuários de seus dados no ambiente virtual. No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei 13.709/2018) representou um marco importante, pois foi implementada, justamente, com a finalidade de disciplinar o tratamento de dados pessoais e proteger os seus titulares de eventuais violações aos seus direitos fundamentais.

No tocante à responsabilização civil dos agentes de tratamento de dados pessoais em razão desse tipo de ocorrência, a coexistência da Lei Geral de Proteção de Dados Pessoais e do Código de Defesa do Consumidor (CDC) no ordenamento jurídico brasileiro suscita questionamentos relevantes quanto à forma de articulação entre esses diplomas legais, especialmente diante da diversidade de relações jurídicas nas quais o tratamento de dados pode ocorrer. Diante disso, o artigo propõe analisar se, nos casos de vazamento de dados pessoais na internet, a aplicação do Código de Defesa do Consumidor à responsabilização civil[1] deve ocorrer de maneira automática, ou se depende da verificação concreta dos elementos caracterizadores da relação de consumo, à luz das disposições da LGPD. Busca-se, assim, investigar os critérios jurídicos que orientam essa escolha normativa, sem prejuízo da proteção efetiva dos direitos dos titulares dos dados pessoais.

A pesquisa se pautou por uma abordagem qualitativa, de natureza teórico-dogmática, com base na doutrina, documentos e jurisprudências atinente ao tema em discussão. Partindo-se dos fundamentos normativos da Lei Geral de Proteção de Dados Pessoais e do Código de Defesa do Consumidor, adotou-se o método dedutivo, para analisar sua incidência nas hipóteses concretas.

Para tanto, o artigo estrutura-se da seguinte forma: após breve introdução, o segundo capítulo investiga sobre o vazamento de dados pessoais como fenômeno da sociedade informacional. No terceiro capítulo se analisa as disposições da LGPD, relativas ao vazamento de dados pessoais e ao regime de responsabilidade civil dos agentes de tratamento; o quarto capítulo examina como se dá a aplicação do Código de Defesa do Consumidor a esses casos; já no quinto capítulo se discute quanto

[1] "Savatier define a responsabilidade civil como sendo a obrigação que incumbe a uma pessoa de reparar o dano causado a outrem por ato seu, ou pelo ato de pessoas ou fato de coisas que dela dependam." (SAVATIER *apud* FACCHINI NETO, 2010, p. 19)

a (in)aplicabilidade automática do CDC, para fins de responsabilização civil. Ao final, apresentam-se as considerações conclusivas, a partir da sistematização dos argumentos desenvolvidos ao longo da abordagem do tema.

2 O VAZAMENTO DE DADOS COMO FENÔMENO DA SOCIEDADE INFORMACIONAL

A internet proporcionou grande revolução na sociedade moderna, se tornando um dos principais meios de comunicação instantânea do mundo. Além de potencializar a socialização, a democratização do conhecimento e a comercialização de produtos e serviços, a rede mundial de computadores permitiu, ainda, a criação de espaços para fomentar debates políticos e a expansão da mobilização social, rompendo com as barreiras geográficas outrora existentes. Nas palavras de Diego Ferreira dos Santos,

> As últimas décadas foram marcadas por um espetacular avanço científico-tecnológico. Em adição, o processo de globalização potencializou o fluxo de relações sociais e econômicas entre os países, sobretudo após o advento da internet. É nesse ambiente impulsionado pela evolução tecnológica que nasce a chamada sociedade da informação. (SANTOS, 2021, p. 129)

O usuário, dentro dessa nova realidade tecnológica, especialmente, através das redes sociais, passou a atuar ativamente do processo de criação e difusão de conteúdos. Como ensina o professor Fábio Queiroz Pereira,

> As redes sociais difundiram-se como formas de comunicação e interação entre os indivíduos afetivos e comunitários no ambiente digital. Com o uso da internet por meio de novos aparatos tecnológicos – notadamente os aparelhos de telefonia celular -, o acesso e as trocas tornaram-se frequentes e demasiadamente céleres, o que contribuiu para a expansão do fenômeno na realidade contemporânea. Para além de interesses meramente pessoais, o uso das redes sociais apresenta novas dimensões, como aquelas ligadas ao comércio eletrônico, tendo em consideração que esses espaços virtuais também passam a ser utilizados com o intuito de lucro, não raramente, incentivando o surgimento de pequenos empreendedores virtuais. (PEREIRA, 2025, p. 3)

Consequência direta dessa intensa participação digital é o compartilhamento de dados pessoais pelos usuários - até mesmo em virtude da forma como as redes são arquitetadas[2] - os quais, quando sistematizados, são convertidos em informações sobre o indivíduo[3], permitindo a identificação de

[2] Para o professor Fábio Queiroz Pereira, "a arquitetura de rede traz consigo a ideia de que é possível moldar comportamentos por meio do estabelecimento de protocolos específicos, que conduzam a um salutar ambiente digital. A título de exemplo, a forma como as plataformas são desenhadas pode conduzir a um maior ou a um menor compartilhamento de dados dos usuários. Assim, uma boa arquitetura seria aquela que faz a contenção dos riscos afetos ao ambiente digital e que permite uma utilização dos aparatos de maneira profícua" (PEREIRA, 2025, p. 2).

[3] Danilo Doneda faz uma importante diferenciação entre os conceitos de dado e informação. "Assim, o "dado" apresenta conotação um pouco mais primitiva e fragmentada, como se observa em um autor que o entende como uma informação em estado potencial, antes de ser transmitida. O dado, assim, estaria associado a uma espécie de "pré-informação", anterior à interpretação e a um processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Mesmo sem aludir ao seu significado, na informação, já se pressupõe a depuração

perfis, hábitos e preferências, por exemplo. Trata-se, portanto, de situação sensível e de alta complexidade, pois, conforme explicam Bruno Bioni e Daniel Dias,

> atualmente, as pessoas são julgadas e avaliadas com base no que seus dados pessoais dizem em todos os âmbitos da sua vida. Do acesso a programa de transferência de renda ao de linha de crédito, essas oportunidades sociais são filtradas pelo processamento de seus dados (BIONI; DIAS, 2020, p. 2)

A obtenção e a coleta de dados pessoais, todavia, não se restringem às redes sociais autobiográficas acima citadas, alcançando um vasto número de plataformas, sites e aplicativos[4]. Como explica Heideivirlandia Leite Galvão *et. al.*, muitos sistemas exigem que os usuários se cadastrem ou ingressem no sítio eletrônico de maneira prévia para, só então, ter acesso ao conteúdo ofertado na página virtual.

> Ao acessar plataformas ou redes digitais, é comum que dados pessoais como nome completo, email, data de nascimento, CPF, endereço, entre outros, sejam solicitados para ingresso ou cadastro. Portanto, é essencial que haja um tratamento adequado dessas informações pessoais, garantindo sua proteção e segurança. Qualquer atividade realizada com esses dados é considerada tratamento, englobando coleta, uso, transmissão e armazenamento, seja em operações online ou offline. (GALVÃO *et. al*., 2024, p. 183)

Outra estratégia adotada pelas plataformas digitais, que visam compelir os internautas a disponibilizar dados pessoais, é o condicionamento do acesso ao ambiente virtual à aceitação dos "cookies", que são definidos pela Agência Nacional de Proteção de Dados Pessoais (ANPD) como sendo "arquivos instalados no dispositivo de um usuário que permitem a coleta de determinadas informações, inclusive de dados pessoais em algumas situações, visando ao atendimento de finalidades diversas"[5] (BRASIL, 2022, p. 8).

Dentro desse cenário, a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei 13.709/2018) ganhou especial relevância no Brasil, pois foi instituída com o objetivo de regular o tratamento de dados pessoais[6], tornando-o mais transparente e seguro. A existência da referida legislação, entretanto,

---

de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido da redução de um estado de incerteza (DONEDA, 2019).

[4] Pode-se dizer que, na atualidade, raros são os sistemas eletrônicos que não captam dados pessoais. A maioria absoluta das páginas eletrônicas solicita a disponibilização de informações, através dos cookies.

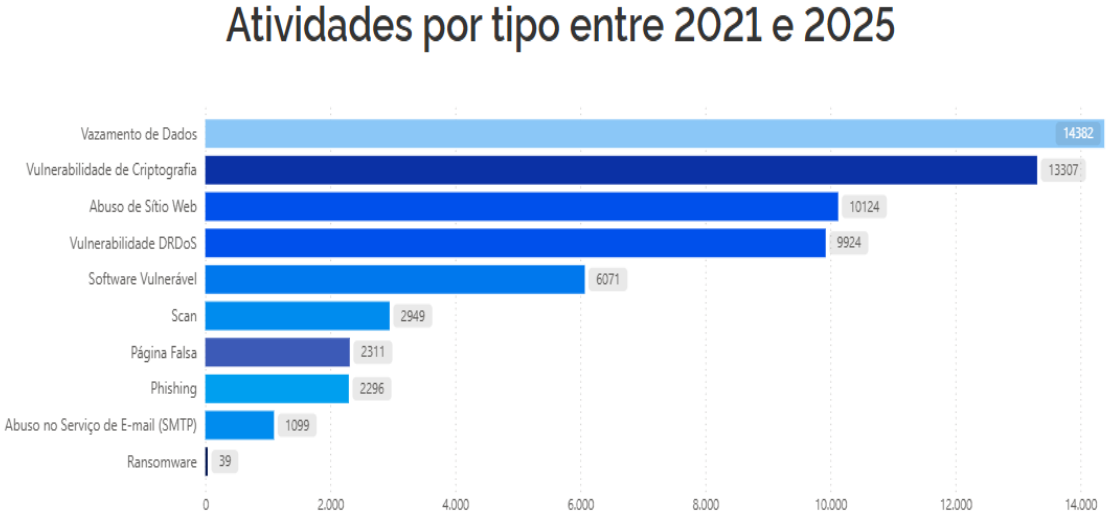
[5] A referida definição encontra-se no Guia Orientativo Cookies e proteção de dados pessoais. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf. Acesso em 11 nov. 2025.

[6] Segundo o artigo 5°, x, da Lei 13.709/2018, considera-se "tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (BRASIL, 2018);

não impede a ocorrência de incidentes de segurança, que poderão ensejar a responsabilização civil dos agentes de tratamento[7].

O gráfico a seguir, retirado do site do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov - "Em Números",[8] demonstra que, entre os anos de 2021 e 2025[9], momento em que já vigorava a referida legislação, somente nas plataformas governamentais, foram registrados cerca de 59.840 incidentes cibernéticos[10]. Dentre eles, 9.572 registros foram de vazamentos de dados. Confira-se:

Gráfico 1 – Incidentes Cibernéticos



Fonte: CTIR Gov

A partir do gráfico acima é possível constatar que os vazamentos de dados pessoais figuraram entre os incidentes cibernéticos mais recorrentes no período compreendido entre 2021 e 2025, ao lado de outras ocorrências relevantes, como vulnerabilidades de criptografia, abusos de sites e falhas de

[7] Compreende-se como agentes de tratamento de dados pessoais, nos termos da Lei 13.709/2018, o controlador e o operador de dados pessoais.

[8] "O CTIR Gov "Em Números" é uma iniciativa criada com o objetivo de disponibilizar estatísticas gerais de interesse público relacionadas aos incidentes cibernéticos de governo, em um ambiente que simplifica o acesso e compreensão dos dados, utilizando-se de relatórios interativos e uma interface visual mais amigável" (BRASIL, 2025). Disponível em https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros. Acesso em 15 de setembro. de 2025.

[9] Atualizado até 15 de setembro de 2025.

[10] O artigo adotará como conceito de "incidente cibernético" o previsto no art. 4°, V, do Decreto n° 10.748/21, que instituiu a Rede Federal de Gestão de Incidentes Cibernéticos, qual seja: "ocorrência que comprometa, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema, que poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que constitua violação de norma, política de segurança, procedimento de segurança ou política de uso" (BRASIL, 2021).

software. Nesse contexto, a elevada incidência de vazamentos de dados pessoais intensificou o debate sobre o regime jurídico aplicável à responsabilização civil dos agentes de tratamento[11].

Observa-se, ainda, que os vazamentos de dados frequentemente se relacionam a múltiplas categorias de incidentes, indicando que tais eventos podem decorrer tanto de ataques externos quanto de fragilidades internas nos mecanismos de proteção adotados pelos agentes de tratamento.

A procura ilegal por acesso aos dados pessoais pode ter diversas motivações, mas, geralmente, as informações obtidas são utilizadas para o cometimento de fraudes no sistema financeiro, como: abertura de contas correntes em instituições financeiras para movimentação de dinheiro cuja origem é ilícita; a solicitação de empréstimos bancários e/ou clonagem de cartão de crédito, entre vários outros tipos de golpes.

Além disso, sabe-se que os invasores também comercializam os dados pessoais obtidos ilegalmente no mercado digital, pois algumas empresas têm interesse nesse tipo de informação, visando oferecer os seus produtos diretamente aos consumidores, cujos dados armazenados demonstrem qualquer disposição destes em adquirir bens ou serviços oferecidos pela empresa adquirente dos dados. As comunicações da empresa, ofertando seus serviços ou produtos poderão ocorrer seja por e-mails, WhatsApp ou, até mesmo, contatos telefônicos.

Assim, o usuário/consumidor, independente da sua autorização e vontade, perde a faculdade de obstar a ingerência alheia sobre a sua vida privada e de definir quais informações poderão ser compartilhadas, fato que afeta diretamente a sua autodeterminação informativa, compreendida como a capacidade de o sujeito poder "manter o controle das suas próprias informações e de determinar a maneira de construir sua própria esfera particular" (RODOTÀ, 2008, p. 15).

O vazamento de dados pessoais, portanto, apresenta-se como um grave problema da sociedade informacional pois, por ele, poderá ocorrer o acesso a informações dos titulares dos dados por indivíduos não autorizados que, muitas vezes, sequer poderão ser identificados. Assim, as informações de caráter pessoal poderão ser utilizadas de maneira indevida, para finalidades completamente diferentes daquelas para as quais foram originalmente coletadas, incluindo o cometimento de fraudes de toda natureza.

3 DISPOSIÇÕES DA LGPD NO TOCANTE AO VAZAMENTO DE DADOS PESSOAIS

Em primeiro lugar, importante esclarecer conceitos relevantes para a compreensão das nuances do tema, constantes da Lei Geral de Proteção de Dados.

O titular de dados caracteriza-se apenas pela pessoa natural que tem seus dados utilizados, independente da finalidade. Por outro lado, os agentes de tratamento são os responsáveis pela manipulação dos dados pessoais, estando sujeitos às regras da LGPD e à fiscalização da Autoridade

[11] Lei 13.709/18: "Art. 5º [...] IX - agentes de tratamento: o controlador e o operador" (BRASIL, 2018).

Nacional de Proteção de Dados (ANPD)[12]. O controlador é quem toma as decisões referentes ao tratamento de dados pessoais, enquanto o operador realiza o tratamento de dados pessoais em nome do controlador. Nesse sentido, prevê a LGPD:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados – ANPD;
> IX - agentes de tratamento: o controlador e o operador;
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
> XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
> XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
> XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
> XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
> XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e
> XIX - autoridade nacional: entidade da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (BRASIL, 2018)

[12] BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). *Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*. Brasília, DF: ANPD, 2021. Disponível em: https://www.gov.br/anpd/. Acesso em: 18/12/2025.

No âmbito das pessoas jurídicas, é a própria companhia que assume a condição de agente de tratamento para fins da LGPD, uma vez que cabe a ela definir as diretrizes, objetivos e parâmetros do tratamento de dados pessoais, os quais serão executados por seus representantes, colaboradores ou prestadores de serviços.

Destaca-se, ainda, que a qualificação como controlador ou operador não é atribuída de forma permanente, mas deve ser analisada em relação a cada operação específica de tratamento, de modo que uma mesma entidade pode ocupar posições distintas, conforme o papel que desempenha em diferentes atividades envolvendo dados pessoais.

Além disso, pessoas naturais também podem ser enquadradas como agentes de tratamento e serão consideradas controladoras quando atuarem com autonomia decisória, orientadas por interesses próprios e com poder para definir as finalidades e os elementos essenciais do tratamento de dados. Por outro lado, serão qualificadas como operadoras quando realizarem o tratamento em nome e de acordo com as diretrizes estabelecidas pelo controlador, limitando-se à execução técnica e operacional, com liberdade apenas quanto a aspectos não essenciais da atividade. Ressalte-se que o operador deve possuir autonomia organizacional em relação ao controlador, não se confundindo com profissionais subordinados ou integrantes de seus órgãos internos.

Nesse sentido, os empregados ou colaboradores da organização não se caracterizam como operadores, uma vez que atuam sob o poder diretivo do controlador, executando tarefas em seu nome e por sua determinação, sem autonomia decisória quanto ao tratamento de dados.

A fim de melhor compreensão, pode-se imaginar uma empresa do setor de comércio eletrônico que decide realizar uma campanha promocional direcionada a determinados clientes. Para tanto, contrata uma empresa especializada em marketing digital, responsável por analisar dados cadastrais, segmentar o público e desenvolver o conteúdo da campanha.

A empresa contratante define os objetivos da ação, o público-alvo e os critérios gerais do tratamento dos dados, enquanto a empresa de marketing executa essas diretrizes técnicas, tratando os dados conforme as instruções recebidas. Nesse caso, a empresa de comércio eletrônico atua como controladora, a agência de marketing como operadora, e os funcionários da empresa contratante, ao dispararem os e-mails promocionais, agem apenas como representantes do controlador, não sendo considerados agentes autônomos de tratamento.

Apresentados os conceitos relevantes relacionados ao sistema de proteção de dados pessoais, passa-se à conceituação da responsabilidade civil. Nas palavras de José Carlos Van Cleef de Almeida Santos e Luís de Carvalho Cascaldi, "a noção de responsabilidade carrega essencialmente a ideia de identificação do sujeito (pessoa física ou jurídica) que deverá suportar o encargo de um determinado dano" (SANTOS; CASCALDI, 2014, p. 589).

Ainda, os doutrinadores Pablo Stolze Gagliano e Rodolfo Pamplona Filho assim conceituam o fenômeno da responsabilidade civil:

> De tudo o que se disse até aqui, conclui-se que a noção jurídica de responsabilidade pressupõe a atividade danosa de alguém que, atuando a priori ilicitamente, viola uma norma jurídica preexistente (legal ou contratual), subordinando-se, dessa forma, às consequências do seu ato (obrigação de reparar). (GAGLIANO; PAMPLONA FILHO, 2008, p. 9)

Diante disso, conclui-se que a responsabilidade civil é uma obrigação derivada, sucessiva[13] e secundária que se origina de dano decorrente de relação obrigacional legal ou contratual. Ou seja, é patente a obrigação de indenizar os danos causados em prejuízo de outrem[14].

Dentro do tema, sabe-se que referido instituto possui três funções principais: a reparatória, que busca recompor o dano e restabelecer a situação anterior ao dano; a punitiva, de caráter pedagógico, que visa sancionar o agente e desencorajar condutas ilícitas; e a promocional, que ultrapassa a compensação e incentiva práticas socialmente responsáveis, permitindo que a reparação integral seja relativizada em prol de ganho coletivo mais amplo, ligado à ética, à governança e à proteção de direitos fundamentais.

Além disso, a responsabilidade civil se subdivide em duas categorias, são elas: a responsabilidade subjetiva – prevista no art. 186 do Código Civil[15] - e a objetiva – prevista no parágrafo único do art. 927 do Código Civil. Fernando Noronha pontua que:

> A responsabilidade civil subjetiva, ou culposa, é a obrigação de reparar danos causados por ações ou omissões intencionais, negligentes ou imprudentes. A responsabilidade civil objetiva, ou pelo risco, é a obrigação de reparar danos que independentemente de qualquer ideia de dolo ou culpa, sejam resultantes de ações ou omissões de alguém, ou estejam simplesmente conexas com a sua atividade. [...] Confrontando as duas espécies de responsabilidade, subjetiva e objetiva, pode-se dizer, em rápida síntese, que verificado um fato danoso para uma pessoa ou para o seu patrimônio, no domínio da responsabilidade subjetiva é preciso averiguar se o seu autor agiu com culpa ou dolo, porque só nestes casos ele estará obrigado a reparar o dano; no domínio da responsabilidade objetiva, prescinde-se de indagações sobre a culpa do agente, bastando que haja nexo causal entre o fato e o dano, para que ele seja forçado à reparação. (NORONHA, 1993, p. 15-16)

Importante ressaltar, ainda, que o regime de responsabilidade civil de natureza subjetiva prevalece nas hipóteses em que não houver previsão legal expressa que imponha a responsabilização objetiva.

---

[13] "Outra característica da obrigação de indenizar é ser sucessiva, porque sempre decorre da violação de uma obrigação anterior (dever originário), estabelecida na lei, no contrato ou na própria ordem jurídica. Autores há que, para distinguirem essas duas obrigações, chamam a primeira de obrigação originária e a segunda de responsabilidade, com o que estamos de pleno acordo." (Cavalieri Filho, p. 35)

[14] "Trata-se, na verdade, de uma situação derivada da violação de uma norma jurídica preexistente (legal ou contratual), desembocando na necessidade de reparação dos danos causados." (Gagliano; Pamplona Filho, 2008, p. 285)

[15] Código Civil/2002: "Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito" (Brasil. 2002).

Volvendo-se ao cerne da questão, aborda-se agora sobre como a LGPD trata a responsabilidade civil, especificamente nos casos de vazamento de dados pessoais. A referida lei não reproduz integralmente o modelo tradicional do Código Civil de 2002, tampouco se limita à logica consumerista, mas cria um regime de tratamento próprio, especificamente nos artigos 42 a 45:

> Seção III
> Da Responsabilidade e do Ressarcimento de Danos
> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.
> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.
> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
> I - o modo pelo qual é realizado;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.
> Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente. (BRASIL, 2018)

Embora a LGPD não utilize expressamente as categorias tradicionais de responsabilidade civil subjetiva e objetiva, sua redação permite diferentes interpretações quanto ao regime aplicável. Isso ocorre porque a lei, ao mesmo tempo em que exige a demonstração de falha no tratamento de dados ou no descumprimento das normas de proteção, também prevê instrumentos que facilitam a prova em favor do titular, reduzindo o seu ônus probatório. Em determinadas situações, essa combinação aproxima a responsabilização de um regime objetivo, ainda que não afastada por completo a análise da conduta do agente de tratamento.

Nesse sentido, o § 1º do art. 42 trata da possibilidade de responsabilização solidária entre os agentes de tratamento, tendo em vista que controlador e operador podem ser responsabilizados de forma conjunta pelos danos decorrentes do tratamento de dados pessoais, sempre que não observarem as normas legais ou quando não comprovarem o cumprimento dos deveres que lhes são atribuídos.

A solidariedade, nesse contexto, tem por finalidade ampliar a tutela do titular dos dados, facilitando a reparação do dano e evitando que a complexidade da cadeia de tratamento inviabilize a identificação do responsável direto pelo evento lesivo. Trata-se, portanto, de mecanismo que reforça a efetividade do sistema de proteção de dados, sem afastar a possibilidade de posterior direito de regresso entre os agentes, conforme o grau de participação de cada um na ocorrência do dano. A princípio, essa é a única hipótese em que o operador é equiparado ao controlador.

No campo jurisprudencial, a interpretação e a aplicação desse regime de responsabilidade civil não são realizadas de maneira uniforme, de modo que os Tribunais ainda não apresentam o mesmo entendimento acerca da natureza jurídica da responsabilidade civil nos casos de vazamento de dados pessoais.

Observa-se, em decisões recentes, tanto a exigência de demonstração de falha concreta na adoção de medidas de segurança, quanto o reconhecimento de que o simples vazamento de dados pode configurar indício suficiente de inadequação do tratamento, ensejando o dever de indenizar.

A título exemplificativo, o Tribunal de Justiça de Minas Gerais, em julgado extremamente recente, ao analisar hipótese de golpe de engenharia social[16], afastou a responsabilização da instituição financeira ao reconhecer a ausência de nexo causal entre a conduta do banco e o dano sofrido pelo consumidor. Confira-se ementa do julgado:

> APELAÇÃO CÍVEL - AÇÃO INDENIZATÓRIA - GOLPE DE ENGENHARIA SOCIAL ("FALSA CENTRAL DE ATENDIMENTO") - TRANSAÇÕES EM CONTA BANCÁRIA POSSIBILITADAS PELO PRÓPRIO AUTOR AO ATENDER ÀS SOLICITAÇÕES DOS ESTELIONATÁRIOS - MÁXIMAS DA EXPERIÊNCIA, INDÍCIOS E PRESUNÇÃO JUDICIAL - ÔNUS DO CONSUMIDOR DE PROVAR O NEXO DE CAUSALIDADE E O DEFEITO DOS SERVIÇOS BANCÁRIOS - NÃO COMPROVAÇÃO - CULPA EXCLUSIVA DO TERCEIRO E DA VÍTIMA - FORTUITO EXTERNO - IMPROCEDÊNCIA DOS PEDIDOS - Tratando-se de golpe em que o próprio consumidor, seguindo as orientações do golpista transmitidas por telefone, realiza procedimentos que resultam em desfalque de valores em sua conta bancária, pode-se afirmar, com base na "observação do que ordinariamente acontece" (art. 375, CPC), que a causa do evento danoso, do ponto de vista jurídico, provavelmente não reside em conduta do banco, mas no comportamento ilícito dos estelionatários associado à desídia ou ignorância da vítima. - Não cabendo, à luz das regras de experiência comum, presumir o nexo de causalidade e o defeito nos serviços do fornecedor, incumbe ao consumidor provar tais elementos, que, ao lado do dano - incontroverso no caso -, compõem a tríade de requisitos da responsabilidade civil regulada pelo art. 14 do CDC. - **Mostrando-se plausível a hipótese de que os fraudadores**

[16] *"Golpes de engenharia social são classificados na literatura de cibersegurança como aqueles oriundos da exploração de fraquezas humanas para obtenção de acesso a sistemas ou arquivos. As duas principais táticas envolvem o hunting mais direto e frequente e com o mínimo grau de interação com a vítima, e o farming, menos frequente, seguido de um relacionamento mais engajado com a vítima para obtenção do maior número de informações possíveis."* (Breda; Barbosa; Morais, 2017. p. 3).

> **tenham obtido pela internet ou por outra fonte estranha ao banco os dados do autor informados na ligação telefônica, descabe supor a ocorrência de vazamento indevido de dados imputável à instituição financeira**. - Verificado, pela análise do extrato bancário do autor, que as transações questionadas não destoam de seu perfil de movimentações, não se pode dizer que a instituição financeira tinha o dever de impedir ou frustrar tais transações, realizadas mediante digitação de senha pessoal e intransferível. - Se o "golpe de engenharia social" resulta em transações bancárias, com uso de senha, para as quais concorreu o próprio correntista, atendendo às solicitações do fraudador, não cabe responsabilizar a instituição financeira pelos prejuízos, se não evidenciadas falhas nos serviços bancários, hipótese em que nem sequer há falar em nexo de causalidade entre conduta sua e os danos sofridos pelo consumidor, dos quais a causa é a culpa de terceiro, associada à desídia da vítima, fortuito externo que exclui a incidência da súmula 479 do STJ. (20ª Câmara Cível do Tribunal de Justiça do Estado de Minas Gerais. Apelação Cível n° 1.0000.25.378065-4/001. Apelante(s): Banco Santander (Brasil) S.A.; Mercado Pago Instituição de Pagamento Ltda. Apelado(a)(s): Banco Santander (Brasil) S.A.; Mercado Pago Instituição de Pagamento Ltda.; Patrícia Ferreira Zago. Relator: Desembargador Fernando Lins. Belo Horizonte, 18 de dezembro de 2025. Data de publicação da súmula: 19 de dezembro de 2025. Grifo nosso.)

Assim, o Exmo. Des. Fernando Lins reconheceu a incidência de culpa exclusiva de terceiro e da própria vítima, caracterizando fortuito externo.

Em sentido diverso, o Tribunal de Justiça de São Paulo tem adotado orientação mais rigorosa em relação aos agentes de tratamento, reconhecendo a responsabilidade civil objetiva nos casos em que comprovado o vazamento de dados pessoais. Verifique-se o acórdão sobre o tema:

> DIREITO CIVIL E DO CONSUMIDOR. APELAÇÃO CÍVEL. VAZAMENTO DE DADOS PESSOAIS. DANO MORAL. LEI GERAL DE PROTEÇÂO DE DADOS PESSOAIS. I. Caso em exame Trata-se de recurso de apelação interposto contra sentença que reconheceu a responsabilidade civil objetiva da ré pelo vazamento de dados pessoais do autor, condenando-a ao pagamento de indenização por danos morais no valor de R$ 10.000,00, devidamente corrigidos e acrescidos de juros moratórios. II. Questão em discussão. Há três questões em discussão: (i) saber se restou comprovado o vazamento de dados pessoais; (ii) saber se era cabível a inversão do ônus da prova à luz do Código de Defesa do Consumidor; (iii) saber se o valor da indenização fixado se mostra adequado aos princípios da proporcionalidade e da razoabilidade. III. Razões de decidir A relação contratual entre as partes enquadra-se no microssistema consumerista, legitimando a inversão do ônus probatório em razão da hipossuficiência técnica do consumidor e da verossimilhança das alegações, nos termos do artigo 6º, inciso VIII, do Código de Defesa do Consumidor. O conjunto probatório é suficiente para comprovar o ilícito, consistente no repasse indevido de dados a terceiro, em afronta aos princípios e deveres estabelecidos na Lei nº 13.709/2018. **A responsabilidade do controlador de dados é objetiva, ex vi do artigo 42 da referida lei.** O valor arbitrado a título de danos morais mostra-se proporcional e razoável, alinhado à gravidade da conduta e ao caráter pedagógico da medida. Precedentes do Tribunal de Justiça do Estado de São Paulo corroboram a fixação da indenização em R$ 10.000,00. A majoração pretendida em contrarrazões não pode ser conhecida, por ausência de recurso próprio, em atenção ao princípio da *vedatio reformatio in pejus*. IV. Dispositivo e tese RECURSO NÃO PROVIDO. SENTENÇA MANTIDA. Tese de julgamento: "1. **A responsabilidade civil por vazamento de dados pessoais é objetiva, à luz da Lei nº 13 .709/2018**. 2. O dano moral é presumido diante da violação à privacidade e intimidade, independentemente de prova de prejuízo material. 3. O valor da indenização de R$ 10.000,00 é adequado às circunstâncias do caso concreto." Dispositivos relevantes citados: CF, art. 5º, caput e XXXV; CDC, arts. 2º, 3º e 6º, VIII; Lei nº 13.709/2018, arts. 6º, 42 e 46; CC, art. 927, parágrafo único. Jurisprudência relevante citada: TJSP, Apelação Cível nº 1000144-71.2021.8.26 .0405, Rel. Maria Lúcia Pizzotti, 30ª Câmara de Direito Privado, j. 25/08/2021; TJSP, Apelação Cível nº 1054460-85.2022.8.26.0506, Rel. Olavo Sá, Núcleo de Justiça 4 .0 – Turma I, j. 29/11/2024. (**5ª Câmara de Direito Privado do Tribunal de Justiça do Estado de São Paulo.** Apelação Cível n° 1001438-40.2025.8.26.0011. **Apelante/Apelado:** Rodrigo Basso Dias. **Apelados/Apelantes:** Mercadolivre.com Atividades de Internet Ltda.; Mercado Pago Instituição de Pagamento Ltda. **Relator:** Desembargador Olavo Paula Leite Rocha. São Paulo, 29 de setembro de 2025. Data de Publicação: 29 de setembro de 2025. **Grifo nosso)**

A partir da ementa acima, verifica-se que o TJSP adota entendimento no sentido de que o vazamento de dados pessoais, uma vez comprovado, configura falha no tratamento e enseja a responsabilização objetiva do controlador, nos termos do art. 42 da LGPD, dispensando-se a investigação acerca da culpa.

O acórdão também reconhece a incidência do microssistema consumerista, especialmente quanto à inversão do ônus da prova, em razão da hipossuficiência técnica do consumidor, bem como admite a caracterização do dano moral de forma presumida, decorrente da violação à privacidade e à intimidade do titular, reforçando uma orientação jurisprudencial mais protetiva e alinhada à teoria do risco do empreendimento.

Em relação ao Superior Tribunal de Justiça, a matéria vem sendo enfrentada de forma mais criteriosa. No julgamento do REsp nº 2.147.374/SP, a Terceira Turma assentou que o agente de tratamento permanece sujeito às obrigações previstas na LGPD mesmo em hipóteses de vazamento decorrente de ataque hacker, desde que não demonstrada a adoção de medidas de segurança adequadas. É ver:

> RECURSO ESPECIAL. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. DIREITO À PRIVACIDADE, À LIBERDADE E À AUTODETERMINAÇÃO INFORMATIVA. AGENTE DE TRATAMENTO. VAZAMENTO DE DADOS NÃO SENSÍVEIS DO TITULAR. INCIDENTE DE SEGURANÇA. ATAQUE HACKER. RESPONSABILIDADE EXCLUSIVA DE TERCEIRO. NÃO COMPROVADA. RESPONSABILIDADE CIVIL PROATIVA. EXPECTATIVA DE LEGÍTIMA PROTEÇÃO. COMPLIANCE E REGULAÇÃO DE RISCO DA ATIVIDADE. DIREITOS DO TITULAR. CONCRETIZAÇÃO. APLICABILIDADE. 1. A controvérsia jurídica consiste em definir se o vazamento de dados pessoais não sensíveis do titular, decorrente de atividade alegadamente ilícita, é passível de imputar ao agente de tratamento de dados as obrigações previstas no art. 19, II, da LGPD, ou se o fato de tal vazamento ter decorrido de atividade ilícita seria uma excludente de responsabilidade, prevista no art. 43, III, da LGPD. 2. Ao inscrever a proteção e o tratamento de dados pessoais no rol dos direitos e garantias fundamentais da Constituição (art. 5º, LXXIX), a Emenda Constitucional nº 115/2022 inaugurou um novo capítulo no ordenamento jurídico brasileiro no que tange aos direitos de personalidade, à liberdade e à autodeterminação informativa. 3. **A empresa recorrente, pelo fato de se enquadrar na categoria dos agentes de tratamento, tinha a obrigação legal de tomar todas as medidas de segurança esperadas pelo titular para que suas informações fossem protegidas, e seus sistemas utilizados para o tratamento de dados pessoais deveriam estar estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD e às demais normas regulamentares.** 4. Compliance de dados é o esforço de conformidade e de aplicação da LGPD nas atividades das empresas que lidam com tratamento de dados. Referido instrumento assume importância central ao induzir não apenas à obediência ao direito, mas também à comprovação da efetividade dos programas de conformidade. 5. O tratamento de dados pessoais configurou-se como irregular quando deixou de fornecer a segurança que o titular dele poderia esperar ("expectativa de legítima proteção"), consideradas as circunstâncias relevantes, entre as quais as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado (art. 44, III, da LGPD). 6. Ao não provar, perante as instâncias ordinárias, que o vazamento dos dados da recorrida teria se dado exclusivamente em razão do incidente de segurança, é impossível aplicar em favor da recorrente a excludente de responsabilidade do art. 43, III, da LGPD.
> 7. Assim, correta a conclusão do TJSP de concretizar os direitos do titular ao condenar a recorrente na obrigação de apresentar informação das entidades públicas e privadas com as quais realizou o uso compartilhado dos dados da recorrida (art. 18, VII, da LGPD) e a fornecer declaração completa que indique a origem dos dados, a inexistência de registro, os critérios

> utilizados e a finalidade do tratamento, bem como a cópia exata de todos os dados referentes ao titular constantes em seus bancos de dados (art. 19, II, da LGPD). 8. Recurso especial não provido. **(Terceira Turma do Superior Tribunal de Justiça.** Recurso Especial n° 2.147.374/SP. **Recorrente:** Eletropaulo Metropolitana Eletricidade de São Paulo S.A. **Recorrido:** Thayna Nayara da Silva Queiroz. **Relator:** Ministro Ricardo Villas Bôas Cueva. Brasília, 3 de dezembro de 2024. Data de Publicação no DJEN: 6 de dezembro de 2024. **Grifo nosso)**

Assim, frisou-se a violação da legítima expectativa de proteção dos dados pessoais, prevista no art. 44 da LGPD.

Por outro lado, a Segunda Turma do STJ, no julgamento do AREsp nº 2.130.619/SP, firmou entendimento no sentido de que o vazamento de dados pessoais comuns não enseja, por si só, a configuração de dano moral presumido. Na ocasião, restou assentado o seguinte:

> PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZAMENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO. I - Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais. II - A sentença julgou os pedidos improcedentes, tendo a Corte Estadual reformulada para condenar a concessionária ao pagamento da indenização, ao fundamento de que se trata de dados pessoais de pessoa idosa. III - A tese de culpa exclusiva de terceiro não foi, em nenhum momento, abordada pelo Tribunal Estadual, mesmo após a oposição de embargos de declaração apontando a suposta omissão. Nesse contexto, incide, na hipótese, a Súmula n. 211/STJ. In casu, não há falar em prequestionamento ficto, previsão do art. 1.025 do CPC/2015, isso porque, em conformidade com a jurisprudência do STJ, para sua incidência deve a parte ter alegado devidamente em suas razões recursais ofensa ao art. 1022 do CPC/2015, de modo a permitir sanar eventual omissão através de novo julgamento dos embargos de declaração, ou a análise da matéria tida por omissa diretamente por esta Corte. Tal não se verificou no presente feito. Precedente: AgInt no REsp 1737467/SC, Rel. Ministro Napoleão Nunes Maia Filho, Primeira Turma, julgado em 8/6/2020, DJe 17/6/2020. IV - O art. 5º, II, da LGPD, dispõe de forma expressa quais dados podem ser considerados sensíveis e, devido a essa condição, exigir tratamento diferenciado, previsto em artigos específicos. Os dados de natureza comum, pessoais mas não íntimos, passíveis apenas de identificação da pessoa natural não podem ser classificados como sensíveis. V - **O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações.** VI - Agravo conhecido e recurso especial parcialmente conhecido e, nessa parte, provido**. (Segunda Turma do Superior Tribunal de Justiça.** Agravo em Recurso Especial n° 2.130.619/SP. **Recorrente:** Wagner Fernando da Silva. **Recorrido:** Boa Vista Serviços S.A. **Relator:** Ministro Francisco Falcão. Brasília, 7 de março de 2023. Data de Publicação no DJe: 10 de março de 2023**. Grifo nosso)**

Ou seja, entendeu-se que é indispensável a comprovação de prejuízo concreto pelo titular dos dados. Distinta, contudo, é a orientação da Corte Superior quando se trata de dados pessoais sensíveis. No julgamento do REsp nº 2.121.904/SP, a Terceira Turma reconheceu que, em contratos de seguro de vida, o vazamento de dados sensíveis do segurado implica responsabilização objetiva da seguradora e caracteriza dano moral presumido. Confira-se a ementa do julgado:

> CIVIL. RECURSO ESPECIAL. CONTRATO DE SEGURO DE VIDA. RELAÇÃO DE CONSUMO. CÓDIGO DE DEFESA DO CONSUMIDOR. LEI GERAL DE PROTEÇÃO DE DADOS. VAZAMENTO DE DADOS SENSÍVEIS. RESPONSABILIDADE OBJETIVA. DANO MORAL PRESUMIDO. RECURSO CONHECIDO EM PARTE. DESPROVIMENTO. 1. Ação de obrigação de fazer c/c indenização por danos morais e materiais, da qual foi extraído o presente recurso especial, interposto em 28/6/2023 e concluso ao gabinete em 22/2/2024. 2. O propósito recursal é definir se, em contrato de seguro de vida, o vazamento de dados sensíveis do segurado gera: (a) dano moral presumido e (b) responsabilização objetiva da empresa seguradora. 3. Inexistência de negativa de prestação jurisdicional. Acórdão do Tribunal de origem devidamente fundamentado para solucionar integralmente a controvérsia submetida à sua apreciação. 4. Não há cerceamento de defesa nas hipóteses em que o julgador resolve a questão controvertida, de forma fundamentada, sem a produção da prova requerida pela parte, em virtude de considerar suficientes os elementos que integram os autos. 5. A matéria que não foi objeto de debate no acórdão recorrido, mesmo após a interposição de embargos declaratórios, não pode ser conhecida por meio de recurso especial. Súmula nº 211/STJ. 6. Cabe ao fornecedor o ônus de comprovar que cumpriu com seu dever de proteger dados pessoais do consumidor, sobretudo quando se tratam de dados sensíveis, nos termos do CDC (arts. 6º, VIII e 14, caput e §3º) e da LGPD (arts. 6º, X, 8º, §2º, 42, §2º e 48, §3º). 7. Há especial proteção legal aos chamados dados pessoais sensíveis: aqueles que, quando revelados, podem gerar algum tipo de discriminação, sobretudo os que incidem sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico" (art. 5º, II, da LGPD). 8. O tratamento de dados pessoais sensíveis observa requisitos significativamente mais rigorosos, sobretudo com a exigência, em regra, do consentimento específico e destacado do titular (art. 11 da LGPD). 9. Em contrato de seguro de vida, deve-se empreender um rigoroso esforço para a proteção dos dados pessoais, já que, para sua celebração, a seguradora, para a avaliação dos riscos, recebe dados sensíveis sobre aspectos pessoais, familiares, financeiros e de saúde do segurado. 10. **O vazamento de dados pessoais sensíveis fornecidos para a contratação de seguro de vida, por si só, submete o consumidor a riscos em diversos aspectos de sua vida, como em sua honra, imagem, intimidade, patrimônio, integridade física e segurança pessoal. 11. Por isso, em seguro de vida, na hipótese de vazamento de dados sensíveis do segurado, verifica-se a responsabilização objetiva da seguradora e a caracterização de dano moral presumido.** 12. Conforme entendimento desta Corte, a revisão da compensação por danos morais só é viável em recurso especial quando o valor fixado for exorbitante ou ínfimo, o que não se constata no recurso sob julgamento. 13. Hipótese em que o acórdão recorrido, ao manter a responsabilização da seguradora, reconheceu que: i) houve vazamento de dados pessoais do consumidor; ii) tais dados são classificados como sensíveis, de modo a abranger informações fiscais, bancárias e sobre a saúde do consumidor; iii) há nexo de causalidade entre o vazamento de dados sensíveis do consumidor e falhas na prestação do serviço pela recorrente, que não atendeu a seu dever de garantir a proteção dos dados sensíveis do consumidor. 14. Recurso especial parcialmente conhecido e, nessa extensão, desprovido. **(Terceira Turma do Superior Tribunal de Justiça.** Recurso Especial n° 2.121.904/SP. **Recorrente:** Prudential do Brasil Seguros de Vida S.A. **Recorrido:** Pedro Henrique Camiloti. **Relatora:** Ministra Nancy Andrighi. Brasília, 11 de fevereiro de 2025. Data de Publicação no DJEN: 17 de fevereiro de 2025. **Grifo nosso).**

Conforme registrado no acórdão, “o vazamento de dados pessoais sensíveis, por si só, submete o consumidor a riscos relevantes à sua honra, imagem, intimidade, patrimônio e segurança pessoal” (BRASIL, 2015), razão pela qual se dispensa a comprovação do dano, diante de sua natureza *in re ipsa*.

Desse modo, a análise das decisões judiciais evidencia a existência de entendimentos distintos acerca da natureza da responsabilidade civil nos casos de vazamento de dados pessoais, variando conforme o contexto fático, a natureza dos dados envolvidos e a forma como os tribunais interpretam os deveres impostos pela LGPD. Enquanto alguns julgados reconhecem a responsabilização objetiva a partir do próprio evento do vazamento, outros condicionam o dever de indenizar à comprovação de

falha concreta na conduta do agente de tratamento. Tal diversidade de posicionamentos demonstra que a aplicação do regime de responsabilidade civil previsto na Lei Geral de Proteção de Dados ainda vem sendo construída no âmbito jurisprudencial.

4 DISPOSIÇÕES DO CDC NO TOCANTE AO VAZAMENTO DE DADOS PESSOAIS

O Código de Defesa do Consumidor adota, como regra geral, um regime de responsabilidade civil objetiva, no qual a reparação dos danos independe da comprovação de culpa do fornecedor (caput dos art. 12 e 14, CDC/90). Para que esse sistema especial de responsabilização seja corretamente aplicado, contudo, é indispensável a prévia identificação da existência de uma relação de consumo. Nesse sentido, o próprio CDC delimita, de forma expressa, os sujeitos que a compõem, ao caracterizar a figura do consumidor e fornecedor.

A definição de consumidor encontra-se previsto no art. 2º do Código de Defesa do Consumidor[17], segundo o qual consumidor é aquele que adquire ou utiliza produto ou serviço como destinatário final, seja pessoa física ou jurídica. Além disso, o diploma amplia essa proteção ao equiparar o consumidor com a coletividade de pessoas que, ainda que indetermináveis, intervenha nas relações de consumo, reforçando o caráter protetivo do sistema consumerista.

Por sua vez, a definição de fornecedor é projetada de forma ampla pelo artigo 3º do CDC[18], e abrange todos aqueles que participam, direta ou indiretamente, da cadeia de produção, circulação ou prestação de produtos e serviços. Assim, considera-se fornecedor qualquer pessoa, de forma extremamente abrangente, que exerça atividades econômicas relacionadas à oferta de produtos ou serviços no mercado de consumo.

A amplitude dessas definições evidencia a intenção legislativa de assegurar a efetiva proteção do consumidor, reconhecido como parte vulnerável da relação, bem como da adoção da teoria do risco do empreendimento, como ensina o doutrinador Sérgio Cavalieri Filho:

> Pela teoria do risco do empreendimento, todo aquele que se disponha a exercer alguma atividade no mercado de consumo tem o dever de responder pelos eventuais vícios ou defeitos dos bens e serviços fornecidos, independentemente de culpa. Este dever é imanente ao dever de obediência a normas técnicas e de segurança, bem como aos critérios de lealdade, quer em relação aos bens e serviços ofertados, quer perante os destinatários dessas ofertas. A responsabilidade decorre do simples fato de dispor-se alguém a realizar atividade de produzir, estocar, distribuir e comercializar produtos ou executar determinados serviços. O fornecedor

[17] CDC: "Art. 2° Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final. Parágrafo único. Equipara-se a consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo". (BRASIL, 1990)

[18] CDC: "Art. 3° Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços. § 1° Produto é qualquer bem, móvel ou imóvel, material ou imaterial. § 2° Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista" (BRASIL, 1990).

> passa a ser o garante dos produtos e serviços que oferece no mercado de consumo, respondendo pela qualidade e segurança dos mesmos. (CAVALIERI FILHO, 2017)

Essa opção normativa é relevante para a conformação do tema de vazamento de dados pessoais, uma vez que permite enquadrar, como fornecedores, empresas que tratam dados no contexto da prestação de serviços digitais, tecnológicos, financeiros ou comerciais. E, o referido enquadramento viabiliza a incidência do regime de responsabilidade civil previsto no Código de Defesa do Consumidor, reforçando a proteção do titular-consumidor diante de falhas relacionadas à segurança da informação.

Nesse cenário, a responsabilização do fornecedor decorre da simples comprovação do dano sofrido pelo consumidor e de sua vinculação a um defeito do produto ou do serviço prestado, não se exige, portanto, a demonstração de culpa. Incumbe ao fornecedor, por sua vez, afastar o dever de indenizar mediante a prova de alguma das excludentes legalmente previstas, capazes de romper o nexo causal entre sua conduta e o prejuízo experimentado.

No que se refere aos produtos, o art. 12 do CDC/90 consagra expressamente a responsabilidade objetiva do fabricante, produtor, construtor ou importador, ao dispor que tais agentes respondem independentemente da existência de culpa pelos danos causados aos consumidores em razão de defeitos que comprometam a segurança legitimamente esperada. A norma evidencia que o conceito de defeito não se limita a vícios materiais, mas abrange também falhas informacionais e riscos inadequadamente geridos, o que amplia significativamente o espectro de incidência da responsabilidade civil no âmbito consumerista. Confira-se referido dispositivo:

> Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos.
> § 1° O produto é defeituoso quando não oferece a segurança que dele legitimamente se espera, levando-se em consideração as circunstâncias relevantes, entre as quais:
> I - sua apresentação; II - o uso e os riscos que razoavelmente dele se esperam;
> III - a época em que foi colocado em circulação.
> §2º O produto não é considerado defeituoso pelo fato de outro de melhor qualidade ter sido colocado no mercado.
> § 3° O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar:
> I - que não colocou o produto no mercado;
> II - que, embora haja colocado o produto no mercado, o defeito inexiste;
> III - a culpa exclusiva do consumidor ou de terceiro. (BRASIL, 1990)

Todavia, para a análise dos vazamentos de dados pessoais, revela-se ainda mais relevante a redação constante do art. 14 do CDC/14, que disciplina a responsabilidade decorrente da prestação de serviços. Isso porque grande parte das atividades que envolvem o tratamento de dados pessoais, como

plataformas digitais, serviços de armazenamento em nuvem, redes sociais, aplicativos e serviços financeiros digitais, caracterizam-se como prestação de serviços ao consumidor.

Nesses casos, o vazamento de dados pode ser compreendido como falha na segurança do serviço prestado, ao frustrar a legítima expectativa do consumidor quanto à proteção de seus dados pessoais. Veja-se:

> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.
> § 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:
> I - o modo de seu fornecimento;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - a época em que foi fornecido.
> § 2º O serviço não é considerado defeituoso pela adoção de novas técnicas.
> § 3° O fornecedor de serviços só não será responsabilizado quando provar:
> I - que, tendo prestado o serviço, o defeito inexiste;
> II - a culpa exclusiva do consumidor ou de terceiro.
> § 4° A responsabilidade pessoal dos profissionais liberais será apurada mediante a verificação de culpa. (BRASIL, 1990)

A sistemática consumerista parte da premissa de que o fornecedor responde pelos danos causados por defeitos do produto ou do serviço, cabendo-lhe o ônus de demonstrar a ocorrência de excludentes legais para afastar o dever de indenizar, o que reforça a proteção do consumidor enquanto parte vulnerável da relação jurídica.

Não obstante a adoção do regime de responsabilidade objetiva, o CDC/90 também prevê hipóteses de exclusão do dever de indenizar, constantes do referido art. 14, § 3º, circunstâncias capazes de romper o nexo causal entre a atividade do fornecedor e o dano experimentado pelo consumidor.

No contexto dos vazamentos de dados pessoais, tais excludentes assumem especial relevância, sobretudo nas hipóteses em que o evento danoso decorre de ataques cibernéticos[19] sofisticados ou de práticas de engenharia social. Referidos eventos podem decorrer da atuação de terceiros estranhos à relação de consumo, o que suscita a discussão acerca de sua aptidão para afastar a responsabilidade do fornecedor. A análise dessas situações demanda a distinção entre fortuito interno e fortuito externo, construção clássica da doutrina civilista.

Em primeiro lugar, Judith Martins Costa assim caracteriza o fortuito interno:

> De todo modo, nas relações de consumo, convêm registrar, há casos excepcionais que se inserem no risco assumido pelo fornecedor para obtenção do resultado prometido ao consumidor. Trata-se do chamado fortuito interno, compreendido na própria atividade empresarial -riscos de delitos para uma empresa de segurança são previsíveis e assumidos pelo

[19] *"[...] ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente"* BRASIL. Ministério da Defesa. MD31-M-07 Doutrina Militar de Defesa Cibernética. Brasília, DF, 2014.

> fornecedor-, de modo que sua ocorrência não será capaz de eliminar o nexo de causalidade, obrigando o fornecedor a indenizar. (MARTINS COSTA, 2003, P. 201)

Em segundo lugar, quanto ao fortuito externo, leciona Agostinho Alvim:

> O fortuito externo é também fato imprevisível e inevitável, mas estranho à organização do negócio. É o fato que não guarda nenhuma ligação com a empresa como fenômenos da natureza -tempestades, enchentes etc. Duas são, portanto, as características do fortuito externo: autonomia em relação aos riscos da empresa e inevitabilidade, razão pela qual alguns autores o denominam de força maior. (ALVIM, 1972, p. 314)

Aplicando-se referidos conceitos no âmbito do vazamento dos dados pessoais, verifica-se que nem todo ataque cibernético pode ser, automaticamente, qualificado como fortuito externo. Isso porque a segurança da informação constitui elemento indissociável das atividades que envolvem o tratamento de dados pessoais, especialmente quando tais dados são coletados, armazenados e processados em larga escala no ambiente digital. A adoção de medidas técnicas e organizacionais adequadas à proteção dos dados, portanto, integra o próprio risco do empreendimento, sendo legítima a expectativa do consumidor quanto à segurança do serviço prestado.

Por outro lado, há hipóteses em que a atuação do próprio consumidor ou de terceiros pode assumir papel determinante na produção do dano, como nos casos de engenharia social, em que o titular dos dados, induzido em erro, fornece voluntariamente informações sensíveis ou credenciais de acesso. Nessas situações, a depender das circunstâncias concretas e do grau de diligência adotado pelo fornecedor, pode-se cogitar a incidência da culpa exclusiva da vítima ou de terceiro, apta a afastar a responsabilidade civil.

Desse modo, embora o regime consumerista imponha ao fornecedor a responsabilidade objetiva pelos danos decorrentes de defeitos do produto ou do serviço, o Código de Defesa do Consumidor admite expressamente hipóteses de exclusão do dever de indenizar, notadamente quando demonstrada a inexistência do defeito ou a ocorrência de culpa exclusiva do consumidor ou de terceiro.

No contexto dos vazamentos de dados pessoais, a análise dessas excludentes exige especial atenção à natureza do evento danoso, à previsibilidade dos riscos envolvidos na atividade desenvolvida e ao grau de segurança legitimamente esperado pelo consumidor, aspectos que devem ser aferidos à luz das circunstâncias concretas de cada caso.

5 A (IN)APLICABILIDADE AUTOMÁTICA DO CDC/90 PARA RESPONSABILIZAÇÃO CIVIL DOS ENVOLVIDOS

A análise conjunta do Código de Defesa do Consumidor e da Lei Geral de Proteção de Dados Pessoais evidencia que a responsabilização civil decorrente de vazamento de dados não pode ser tratada de forma automática e indistinta sob o regime consumerista. Embora o CDC/90 desempenhe

papel central na tutela do consumidor em diversas hipóteses envolvendo tratamento de dados pessoais, sua incidência depende, necessariamente, da configuração de uma relação de consumo, não sendo suficiente, por si só, a mera ocorrência de um incidente de segurança[20].

A LGPD instituiu um microssistema jurídico próprio, voltado à proteção de dados pessoais, aplicável a múltiplas relações jurídicas, inclusive aquelas de natureza não consumerista, como relações trabalhistas, administrativas, contratuais empresariais e relações entre particulares sem finalidade de consumo.

Nesse contexto, o art. 45 do referido diploma estabelece que, nas relações de consumo, continuam a ser aplicadas as normas específicas do CDC/90, o que pressupõe, logicamente, a verificação prévia dos requisitos caracterizadores da relação consumerista.

A adoção automática do Código de Defesa do Consumidor em todo e qualquer caso de vazamento de dados pessoais implica esvaziar a autonomia normativa da LGPD e desconsiderar as particularidades do regime por ela instituído, especialmente no que se refere à definição dos agentes de tratamento, aos deveres de segurança, às bases legais do tratamento e às hipóteses específicas de responsabilização previstas nos arts. 42 a 45, da LGPD previamente demonstradas neste estudo.

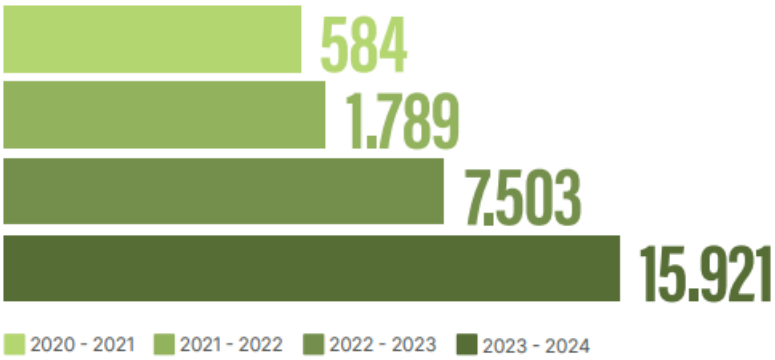
Observa-se que a responsabilidade civil no âmbito da LGPD, embora dialogando com categorias tradicionais do direito civil e do direito do consumidor, apresenta contornos próprios, que exigem análise casuística da conduta do agente, da natureza dos dados envolvidos e das circunstâncias do incidente. Esse debate ganha especial relevo diante do expressivo aumento da judicialização de demandas envolvendo proteção de dados pessoais no Brasil.

A crescente judicialização das controvérsias relacionadas à matéria revela o impacto concreto da LGPD no âmbito do Poder Judiciário. Conforme aponta o Relatório Painel LGPD nos Tribunais – 2025[21], elaborado pelo CEDIS-IDP em parceria com o Jusbrasil, o número de decisões judiciais com menção à Lei nº 13.709/2018 apresentou crescimento exponencial desde sua entrada em vigor, passando de 584 decisões no período de 2020–2021 para 15.921 decisões coletadas no ciclo 2023–2024, das quais mais de 7 mil foram classificadas como de alta relevância. Veja-se:

[20] *"Qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais."* COMUNICAÇÃO de Incidentes de Segurança. In: ANPD, Brasília, 22 fev. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: 24 dez. 2025.

[21] CEDIS-IDP; JUSBRASIL. *Relatório Painel LGPD nos Tribunais 2025*. 2. ed. São Paulo: CEDIS-IDP; Jusbrasil, 2025. Disponível em: Painel LGPD nos Tribunais. Acesso em: 24 dez. 2025.

Gráfico 2 – Número de documentos por ano



Fonte: CEDIS-IDP; Jusbrasil (2025)

Tal cenário evidencia não apenas o aumento quantitativo das demandas, mas também a progressiva incorporação da LGPD como fundamento jurídico central em litígios que envolvem vazamento de dados pessoais e responsabilidade civil dos agentes de tratamento.

A pluralidade de contextos em que surgem essas demandas explica, em grande medida, a ausência de uniformidade na aplicação automática do CDC/90. Em diversos casos, os tribunais têm afastado o regime consumerista justamente por inexistir relação de consumo, ainda que configurada a violação à legislação de proteção de dados. Em outros, reconhece-se a incidência conjunta do CDC e da LGPD, sobretudo quando o tratamento de dados ocorre no âmbito da prestação de serviços ou fornecimento de produtos ao consumidor final.

Dessa forma, a (in)aplicabilidade do Código de Defesa do Consumidor aos casos de vazamento de dados pessoais deve ser analisada à luz das circunstâncias concretas de cada situação, observando-se a natureza da relação jurídica estabelecida entre as partes.

A LGPD não substitui o CDC, tampouco é por ele absorvida, mas atua de forma complementar, exigindo do intérprete uma leitura sistemática que evite tanto a banalização da responsabilidade objetiva quanto a indevida restrição da tutela dos direitos fundamentais do titular dos dados.

6 CONCLUSÃO

Visando analisar a apuração da responsabilidade civil nos casos de vazamento de dados pessoais no ordenamento jurídico brasileiro, importa dar especial atenção ao debate sobre a aplicação automática das normas atinentes ao tema no Código de Defesa do Consumidor em consonância às disposições da Lei Geral de Proteção de Dados Pessoais. Partindo-se do reconhecimento de que o uso intensivo de dados no ambiente digital ampliou de forma significativa os riscos à privacidade e à autodeterminação informativa, verifica-se que os incidentes de segurança têm se tornado cada vez mais frequentes, o que impulsionou a judicialização de conflitos relacionados à proteção de dados.

A análise da LGPD demonstra que o legislador brasileiro optou por instituir um regime próprio de responsabilização civil, estruturado a partir da atuação dos agentes de tratamento e orientado por

deveres específicos de segurança, governança e transparência. Ainda que a LGPD não adote expressamente as categorias tradicionais de responsabilidade subjetiva ou objetiva, seus dispositivos permitem identificar um modelo híbrido, que combina elementos de ambos os regimes e admite, inclusive, a responsabilização solidária entre controlador e operador, com o objetivo de garantir a efetiva reparação dos danos sofridos pelos titulares dos dados.

No que se refere ao Código de Defesa do Consumidor, constata-se que o microssistema consumerista oferece importantes instrumentos de tutela, especialmente diante da vulnerabilidade técnica do consumidor e da adoção da teoria do risco do empreendimento. Contudo, sua aplicação não pode ser presumida em todo e qualquer caso de vazamento de dados pessoais, uma vez que depende da verificação concreta da existência de relação de consumo. E, mesmo que a responsabilidade do fornecedor seja objetiva, o próprio CDC prevê excludentes capazes de afastar o dever de indenizar, cuja análise exige atenção às circunstâncias específicas de cada situação.

A pesquisa jurisprudencial evidencia a ausência de uniformidade nos entendimentos dos tribunais, quanto à natureza da responsabilidade civil nos casos de vazamento de dados pessoais. Enquanto alguns julgados reconhecem a responsabilização objetiva e o dano moral presumido a partir do simples evento do vazamento, outros condicionam o dever de indenizar à comprovação de falha concreta na adoção de medidas de segurança ou à demonstração de prejuízo efetivo pelo titular dos dados. Tal diversidade revela que o regime de responsabilização em matéria de proteção de dados ainda se encontra em fase de consolidação no âmbito jurisprudencial.

Diante desse cenário, conclui-se que a aplicação do Código de Defesa do Consumidor aos casos de vazamento de dados pessoais não deve ocorrer de forma automática ou indistinta. A LGPD e o CDC coexistem de maneira complementar no ordenamento jurídico brasileiro, exigindo uma interpretação sistemática e contextualizada, capaz de considerar a natureza da relação jurídica estabelecida, o papel desempenhado pelos agentes de tratamento, a espécie de dados envolvidos e as circunstâncias do incidente de segurança. Essa leitura equilibrada contribui para a proteção efetiva dos direitos fundamentais dos titulares de dados, sem comprometer a autonomia normativa da LGPD, promovendo ao mesmo tempo a maior coerência e segurança jurídica na adequada determinação da incidência da responsabilização civil.

REFERÊNCIAS

ALVIM, Agostinho. *Da inexecução das obrigações e suas consequências.* 4. ed. São Paulo: Saraiva, 1972.

BIONI, Bruno Ricardo; DIAS, Daniel de Brito. *Proteção de dados pessoais: a função e os limites do consentimento.* São Paulo: Thomson Reuters Brasil, 2020.

BRASIL. Autoridade Nacional de Proteção de Dados. *Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado.* Brasília, DF: ANPD, 2021.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil.* Brasília, DF: Presidência da República, 1988.

BRASIL. Conselho Nacional de Justiça. *Relatório do Painel LGPD nos Tribunais – 2025.* Brasília, DF: CNJ, 2025.

BRASIL. Ministério da Defesa. MD31-M-07 Doutrina Militar de Defesa Cibernética. Brasília, DF, 2014.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. *Altera a Constituição Federal para incluir a proteção de dados pessoais no rol de direitos e garantias fundamentais.* Diário Oficial da União: Brasília, DF, 11 fev. 2022.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. *Dispõe sobre a proteção do consumidor e dá outras providências.* Diário Oficial da União: Brasília, DF, 12 set. 1990.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. *Institui o Código Civil.* Diário Oficial da União: Brasília, DF, 11 jan. 2002.

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

BRASIL. Ministério da Defesa. *MD31-M-07: Doutrina Militar de Defesa Cibernética.* Brasília, DF: Ministério da Defesa, 2014.

BRASIL. Superior Tribunal de Justiça (Segunda Turma). Agravo em Recurso Especial n° 2.130.619/SP. Recorrente: Wagner Fernando da Silva. Recorrido: Boa Vista Serviços S.A. Relator: Ministro Francisco Falcão. Brasília, 7 de março de 2023. Data de Publicação no DJe: 10 de março de 2023.

BRASIL. Superior Tribunal de Justiça (Terceira Turma). Recurso Especial n° 2.121.904/SP. **Recorrente:** Prudential do Brasil Seguros de Vida S.A. **Recorrido:** Pedro Henrique Camiloti. **Relatora:** Ministra Nancy Andrighi. Brasília, 11 de fevereiro de 2025. Data de Publicação no DJEN: 17 de fevereiro de 2025.

BRASIL. Superior Tribunal de Justiça (Terceira Turma). Recurso Especial n° 2.147.374/SP. Recorrente: Eletropaulo Metropolitana Eletricidade de São Paulo S.A. Recorrido: Thayna Nayara da Silva Queiroz. Relator: Ministro Ricardo Villas Bôas Cueva. Brasília, 3 de dezembro de 2024. Data de Publicação no DJEN: 6 de dezembro de 2024.

BRASIL. Tribunal de Justiça do Estado de São Paulo (5ª Câmara de Direito Privado). Apelação Cível n° 1001438-40.2025.8.26.0011. Apelante/Apelado: Rodrigo Basso

Dias. Apelados/Apelantes: Mercadolivre.com Atividades de Internet Ltda.; Mercado Pago Instituição de Pagamento Ltda. Relator: Desembargador Olavo Paula Leite Rocha. São Paulo, 29 de setembro de 2025. Data de Publicação: 29 de setembro de 2025.

BRASIL. Tribunal de Justiça de Minas Gerais (20ª Câmara Cível). Apelação Cível n° 1.0000.25.378065-4/001. Apelante(s): Banco Santander (Brasil) S.A.; Mercado Pago Instituição de Pagamento Ltda. Apelado(a)(s): Banco Santander (Brasil) S.A.; Mercado Pago Instituição de Pagamento Ltda.; Patrícia Ferreira Zago. Relator: Desembargador Fernando Lins. Belo Horizonte, 18 de dezembro de 2025. Data de Publicação no DJE: 19 de dezembro de 2025.

BREDA, Filipe; BARBOSA, Hugo; MORAIS, Telmo. *Social engineering and cyber security, International Technology, Education and Development Conference*, 2017. p. 3. DOI: 10.21125/inted.2017.1008.

CAVALIERI FILHO, Sérgio. *A responsabilidade civil nas relações de consumo: tendências do século XXI.* Revista Eletrônica da Faculdade de Direito da Universidade Federal de Pelotas, Pelotas, v. 3, n. 1, p. 1–20, jan./jun. 2017.

CAVALIERI FILHO, Sérgio. *Programa de responsabilidade civil.* 15. ed. São Paulo: Atlas, 2022.

CAVALIERI FILHO, Sergio. *Responsabilidade civil no novo Código Civil.* Revista EMERJ, n. 24, 2003.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

FACCHINI NETO, Eugêncio. *Da Responsabilidade Civil no novo Código*. Revista do TST, vol. 76, 2010, p. 19.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. *Novo curso de direito civil: responsabilidade civil.* 6. ed. São Paulo: Saraiva, 2008.

GALVÃO, Heideivirlandia Leite; OLIVEIRA, Alyne Leite de; GINO, Bethsaida de Sá Barreto Diaz; VIANA, Hudson Josino; ARAÚJO, Francisco Gledison Lima; BENEVINUTO, Noélia Marques Silva; SILVA, Denis Leonardo Ferraz da. *Incidentes de Segurança: Regulação e Prática de Vazamento de Dados Pessoais Frente à LGPD. Id on Line: Revista de Psicologia*, Maringá, v. 18, n. 72, p. 179–197, jul. 2024. ISSN 1981-1179. Disponível em: https://idonline.emnuvens.com.br/id/article/view/4042/6035. Acesso em: 21 dez. 2025

MARTINS-COSTA, Judith. *Comentários ao novo Código Civil.* Rio de Janeiro: Forense, 2003. v. V, t. II.

NORONHA, Fernando. *Responsabilidade civil: uma tentativa de ressistematização.* São Paulo: Saraiva, 1993.

PEREIRA, Fábio Queiroz. *Os perfis de redes sociais e a morte do usuário: privacy by design e o estabelecimento de uma regra padrão.* Civilistica.com. Rio de Janeiro, a.14, n.1, 2025. Disponível em: https://civilistica.emnuvens.com.br/redc. Acesso em: 08 dez. 2025.

RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje.* Organização, seleção e apresentação de Maria Celina Bondin de Moraes. Tradução: Danilo Doneda; Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SANTOS, José Carlos Van Cleef de Almeida e CASCALDI, Luís de Carvalho. *Manual de Direito Civil*. Revista dos Tribunais, 2014, p. 589

SANTOS, Diego Ferreira dos. *A PROTEÇÃO DOS DADOS PESSOAIS COMO NOVA ESPÉCIE DE DIREITO DA PERSONALIDADE*. Revista de Direito Civil Contemporâneo, São Paulo, v. 28, p. 127–146, 2021. Revista Esmat. Disponível em: https://www.academia.edu/75934831/A_PROTEÇÃO_DOS_DADOS_PESSOAIS_COMO_NOVA_ESPÉCIE_DE_DIREITO_DA_PERSONALIDADE. Acesso em: 08 dez. 2025.
SANTOS, Diego Ferreira dos. *Sociedade da informação e proteção de dados pessoais.* Revista de Direito Civil Contemporâneo, São Paulo, v. 28, p. 127–146, 2021.