REVISTA DIREITO MACKENZIE

ISSN 2317-2622 | RDM | Revista Direito Mackenzie | São Paulo | SP | 19(3) | e18056 | 2025
http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056

INCIDENTES DE SEGURANÇA, VAZAMENTO DE DADOS E ATAQUES CIBERNÉTICOS: POSSÍVEIS RESPOSTAS PARA APLICAÇÃO DO DIREITO A PARTIR DAS DECISÕES DO STJ NO RESP 2.147.374/SP E ARESP 2.130.619/SP

RECEBIDO EM:	9.6.2025
APROVADO EM:	23.10.2025

Gabriel Cemin Petry

https://orcid.org/0000-0002-2357-1573
Universidade do Vale do Rio dos Sinos (Unisinos)
Novo Hamburgo, RS, Brasil
E-mail: Gabrielcpetry96@gmail.com

Karin Regina Rick Rosa

https://orcid.org/0009-0001-2530-951X.
Universidade do Vale do Rio dos Sinos (Unisinos)
Novo Hamburgo, RS, Brasil
E-mail: karinrick.rosa@gmail.com

Wilson Engelmann

https://orcid.org//0000-0002-0012-3559
Universidade do Vale do Rio dos Sinos (Unisinos)
Novo Hamburgo, RS, Brasil
E-mail: wengelmann@unisinos.br

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056
2025 | v. 19 | n. 3 | p. 1-25 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056

· GABRIEL CEMIN PETRY
· KARIN REGINA RICK ROSA
· WILSON ENGELMANN

Para citar este artigo: PETRY, G. C.; ROSA, K. R. R.; ENGELMANN, W. Incidentes de segurança, vazamento de dados e ataques cibernéticos: possíveis respostas para aplicação do Direito a partir das decisões do STJ no REsp 2.147.374/SP e AREsp 2.130.619/SP. *Revista Direito Mackenzie*, São Paulo, SP, v. 19, n. 3, e18056, 2025. http://dx.doi.org/10.5935/2317-2622/direito-mackenzie.v19n318056

RESUMO: O problema central do estudo é verificar como o STJ tem aplicado o Direito diante de casos envolvendo incidentes de segurança, como vazamento de dados e ataques cibernéticos, considerando a multiplicidade de formas, agentes e diferentes impactos que tais acontecimentos podem alcançar. Busca-se analisar os conceitos de incidentes de segurança, além de investigar como o STJ aplicou o Direito em dois precedentes, o REsp 2.147.374/SP e AREsp 2.130.619/SP. Para tanto, adota-se o método de investigação dedutivo, pautado em pesquisa bibliográfica, documental e jurisprudencial. A partir dos casos estudados, conclui-se que existem inconsistências conceituais, que decorrem de uma possível generalização do termo incidentes de segurança, circunstância que pode prejudicar a aplicação do Direito. É necessário aprimorar a compreensão técnica dos incidentes de segurança, sua diferenciação, além de reconhecer o risco como elemento relevante à responsabilização civil, corroborando para consolidação práticas coerentes com a LGPD.

PALAVRAS-CHAVE: Direito Digital; cibersegurança; proteção de dados.

SECURITY INCIDENTS, DATA LEAKS AND CYBER ATTACKS: POSSIBLE ANSWERS FOR THE APPLICATION OF THE LAW BASED ON THE STJ'S DECISIONS IN RESP 2.147.374/SP AND ARESP 2.130.619/SP

ABSTRACT: The central problem of the study is to verify how the STJ has applied the law in cases involving security incidents, such as data leaks and cyber attacks, considering the multiplicity of forms, agents and different impacts that such incidents can have. The aim is to analyze the concepts of security incidents and investigate how the STJ has applied the law in two precedents, REsp 2.147.374/SP and AREsp 2.130.619/SP. To this end, the deductive research method is adopted,

based on bibliographical, documentary and jurisprudential research. Based on the cases studied, it is concluded that there are conceptual inconsistencies arising from a possible generalization of the term security incidents, a circumstance that can hinder the application of the law. It is necessary to improve the technical understanding of security incidents, their differentiation, as well as recognizing risk as a relevant element for civil liability, corroborating the consolidation of practices consistent with the LGPD.

KEYWORDS: Digital Law; cybersecurity; data protection.

1. Introdução

Nas últimas décadas, a transformação digital intensificou de forma exponencial a circulação de dados e a dependência humana de sistemas informacionais em todos os setores da sociedade, ampliando, em contrapartida, os riscos associados à sua segurança. Nesse contexto, incidentes de segurança, em especial os vazamentos de dados e os ataques cibernéticos, tornaram-se eventos recorrentes e de alto impacto, exigindo respostas normativas, técnicas e institucionais que estejam à altura da complexidade do problema posto. Esses eventos não apenas comprometem ativos digitais e operacionais, mas também afetam direitos fundamentais, como a privacidade, a autodeterminação informativa e, notadamente, a proteção de dados pessoais.

É nesse cenário que se insere a presente investigação, cujo problema central reside na verificação sobre como o Superior Tribunal de Justiça (STJ) tem aplicado o Direito diante de casos envolvendo incidentes de segurança, como vazamento de dados e ataques cibernéticos, considerando a multiplicidade de formas, agentes e diferentes impactos que tais acontecimentos podem assumir. A abordagem proposta busca, assim, esclarecer os distintos conceitos jurídicos e técnicos envolvidos – incidentes de segurança, ataques cibernéticos e vazamentos de dados – a fim de contribuir para superação de possíveis confusões terminológicas no discurso jurídico e nas decisões judiciais. A análise se justifica pela urgência de consolidar uma compreensão precisa e tecnicamente fundamentada de tais ocorrências, com vistas à proteção eficaz de direitos no ecossistema digital.

Objetiva-se com o artigo conceituar e distinguir as variações dos denominados incidentes de segurança, incluindo ataques cibernéticos e vazamentos de dados,

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056
2025 | v. 19 | n. 3 | p. 1-25 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056

examinando suas possíveis causas, efeitos e implicações jurídicas - delimitação conceitual que é fundamental para esclarecer os distintos conceitos técnicos e regulatórios, visando a contribuir para superação de possíveis confusões terminológicas no discurso jurídico e decisões judiciais. Em seguida, objetiva-se analisar como o STJ tem aplicado o Direito em casos envolvendo incidentes de segurança, valendo-se do exame de duas decisões: o REsp 2.147.374/SP e o AREsp 2.130.619/SP.

A escolha dos julgados do STJ se justifica pela necessidade de verificar as respostas variadas da Corte Superior diante da multiplicidade de incidentes de segurança e seus impactos. O exame conjunto desses precedentes descortina nuances e divergências quanto à aplicação do Direito, pois, enquanto no REsp 2.147.374/SP fala-se em responsabilidade objetiva e proativa, no AREsp 2.130.619/SP, alinha-se a lógica tradicional subjetiva quanto à comprovação de dano efetivo. A análise crítica dos precedentes propicia examinar inconsistências conceituais e a possível generalização do termo "incidentes de segurança" no discurso jurídico, que podem prejudicar a aplicação do Direito e a proteção eficaz de usuários, consumidores e titulares de dados.

Para tanto, adota-se uma abordagem metodológica dedutiva, de caráter exploratório, subsidiada por pesquisa documental e bibliográfica. Parte-se, portanto, de um conhecimento geral, com a delimitação conceitual e a distinção das variações do termo "incidente de segurança", com base na legislação, doutrina especializada e regulamentos da Autoridade Nacional de Proteção de Dados (ANPD), para, em seguida, chegar-se ao particular, que é analisar e explicar como o Direito foi aplicado em dois casos judiciais específicos (o REsp 2.147.374/SP e o AREsp 2.130.619/SP) pelo STJ. O raciocínio dedutivo possibilita, portanto, *(i)* verificar se as decisões do STJ são logicamente coerentes com as premissas gerais estabelecidas e *(ii)* analisar se existem inconsistências conceituais na aplicação do Direito e/ou a generalização do termo "incidentes de segurança" no discurso jurídico.

A primeira seção propõe uma delimitação conceitual dos incidentes de segurança, apresentando os fundamentos técnicos que os caracterizam e diferenciando-os dos ataques cibernéticos e dos vazamentos de dados. A seção dedica-se, ainda, à análise de dispositivos da Lei Geral de Proteção de Dados (LGPD) e de regulamentos da ANPD que tangenciam a matéria dos incidentes de segurança. A segunda seção, por fim, examina os julgados do STJ, buscando identificar como o tribunal lidou com o conceito de incidentes de segurança e, entre outros, quais foram os critérios utilizados para apurar

a responsabilização dos agentes de tratamento, a fim de verificar quais desafios emergem para a caracterização do dano em contextos de risco digital.

A estrutura proposta permite, portanto, uma compreensão integrada e crítica das múltiplas dimensões envolvidas nos incidentes de segurança, servindo como subsídio para o aprimoramento da atuação jurídica diante das novas dinâmicas tecnológicas. Ao final, pretende-se não apenas oferecer uma breve e incipiente sistematização teórica sobre o tema, mas também fomentar uma reflexão propositiva sobre a necessidade de evolução jurisprudencial e regulatória compatível com a complexidade da era digital.

2. Incidentes de segurança: vazamentos de dados, ataques cibernéticos e outros conceitos para aplicação do Direito

Inicialmente, conforme esclarecem Carvalho e Souza (2019, p. 155), popularmente convencionou-se chamar "vazamento de dados" qualquer tipo de problema atrelado aos denominados "incidentes de segurança", quando, na realidade, os incidentes têm um espectro bem mais amplo do que uma brecha de segurança. Os conceitos, no entanto, diferem na sua definição e podem ter consequências distintas, inclusive para interpretação e aplicação do Direito. Na presente seção, serão abordadas três terminologias relevantes no contexto do Direito Digital: *(i)* incidentes de segurança; *(ii)* vazamentos de dados; e *(iii)* ataques cibernéticos.

2.1 Incidentes de segurança

Incidentes de segurança são aqueles que afetam a segurança da informação, por isso, antes de tratar sobre o seu conceito, é preciso tratar da segurança da informação, que, aliás, é uma preocupação antiga, pois há muito que métodos de segurança são utilizados para evitar o acesso indevido às informações. Vale lembrar que o primeiro computador foi criado para quebrar o mecanismo de segurança utilizado pela Alemanha na 2ª Guerra Mundial. Os modelos matemáticos criados para sigilo de dados, denominados criptografia, evoluíram com a tecnologia, no entanto, a segurança da informação não acompanhou completamente o avanço, de modo que as vulnerabilidades começaram a crescer, circunstância que persiste em virtude da complexificação e intensificação com que sistemas computacionais integram cada vez mais, objetos, redes e ambientes

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056
2025 | v. 19 | n. 3 | p. 1-25 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056

(Schneier, 2019, p. 26-28)[1]. O advento dos crimes cibernéticos, por exemplo, chamou a atenção de reguladores e legisladores, e a combinação de uma legislação mais forte e de ataques cibernéticos mais agressivos mudou o cenário da segurança da informação para as organizações (Freire *et al.*, 2024).

A segurança da informação é uma parte vital dos negócios e é alcançada por meio da implementação de um conjunto adequado de controles, que incluem políticas, processos, procedimentos, estruturas organizacionais, além de funções de *software* e *hardware*. Para proteger de forma eficaz os ativos, é necessário proteger a *confidencialidade*, a *integridade* e a *disponibilidade* dos dados, e isso é feito a partir de controles estabelecidos, implementados, monitorados, revisados e melhorados constantemente[2].

Os princípios fundamentais da segurança da informação são justamente a *confidencialidade*, *integridade* e *disponibilidade*[3] (Hintzbergen *et al.*, 2018, p. 20), auxiliando como uma base inicial para a compreensão dos incidentes de segurança. A *confidencialidade*, também denominada de exclusividade, está relacionada à limitação sobre quem pode obter a informação:

> A confidencialidade assegura que o nível necessário de sigilo seja aplicado em cada elemento de processamento de dados e impede a divulgação não autorizada. Esse nível de confidencialidade deve prevalecer enquanto os dados residirem em sistemas e dispositivos na rede, quando forem transmitidos e quando chegarem ao seu destino (Hintzbergen *et al.*, 2018, p. 21).

A *integridade* diz respeito à consistência e acurácia da informação, significa ela estar completa, perfeita e intacta; qualquer modificação não autorizada dos dados, seja ela intencional ou não, violará o princípio da integridade. A disponibilidade se caracteriza pelo acesso à informação quando necessário, à continuidade do trabalho no caso de uma falha. É possível, a partir desses três princípios basilares, delinear igualmente três tipos de incidentes de segurança:

1 Segundo Schneier (2019, p. 26-28), a complexidade dos sistemas computadorizados significa que é mais fácil atacar do que se defender, uma vez que sistemas complexos implicam, ao menos em princípio, uma área de exploração de vulnerabilidades maior, especialmente considerando a interoperabilidade e interconexão entre os sistemas.

2 A ISO 27002:2013, revogada pela ISO/IEC 27002:2022, aborda o processo para gestão da segurança da informação – Código de prática para a segurança da informação – destacando a importância de compreender os requisitos de segurança da informação, implementar e operar controles para gerenciar risco de segurança da informação, monitorar e revisar o desempenho e a eficiência do Sistema de Gerenciamento de Segurança da Informação, e melhorar a partir de medições objetivas. Disponível em: https://www.iso.org/standard/75652.html. Acesso em: 4 maio 2025.

3 Conhecido como triângulo "CIA" (Hintzbergen *et al.*, 2018, p. 20).

> O primeiro deles, os incidentes de confidencialidade, abrange as ocorrências em que há uma divulgação ou acesso acidental ou não autorizado a dados pessoais. Já os incidentes de integridade ocorrem quando há algum tipo de alteração acidental ou não autorizada dos dados. Por fim, os incidentes de disponibilidade seriam aqueles em que há a perda de acesso ou destruição, acidental ou não autorizada, desses dados (Luciano, 2019, p. 164).

Vale dizer que, além desses três princípios fundamentais, existem outros três que formam o chamado hexagrama parkeriano. São eles: a *posse ou o controle*, a *autenticidade* e a *utilidade*. Tudo aquilo que afeta um ou mais desses atributos fundamentais da informação pode caracterizar uma violação da segurança (Hintzbergen *et al.*, 2018, p. 27).

As ameaças à segurança da informação podem ser humanas ou não. Na categoria de ameaças humanas, temos as que são intencionais, tais como o ataque por um *hacker*, o funcionário que, após ser demitido, destrói dados, ou revela informações à concorrência. A engenharia social é outro exemplo de ameaça humana intencional, que funciona a partir da exploração da falta de consciência sobre segurança. Já as ameaças humanas não intencionais decorrem de acidentes que podem acontecer, como a exclusão de dados ou a instalação de um vírus (*malware*) a partir de uma mensagem de *e-mail* (*v.g.*, ataques de *phishing*). Por outro lado, existem situações que não envolvem ações humanas, como descargas elétricas, incêndios, enchentes, entre outros. Essas ameaças podem resultar em danos diretos ou indiretos e é necessário lidar com os riscos aceitando-os, mitigando-os e evitando-os, o máximo possível.

Assim, incidentes de segurança podem ser definidos como "[...] um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio de uma organização" (Carvalho; Souza, 2019, p. 155)[4]. Sob essa perspectiva, "[...] a perda de um pen drive, o furto de um notebook, a interrupção de acesso a um sistema podem ser considerados do ponto de vista técnico incidentes de segurança, porquanto a informação corporativa estará exposta a uma ameaça" (Jimene, 2019, RL.1.14). O termo "incidente de segurança" (ou somente "incidente") aparece por seis vezes no texto da LGPD, especificamente no Capítulo VII, Secção I e II, sem ser efetivamente definido ou conceituado no rol de 19 incisos do art. 5º da legislação especial (Luciano, 2019, 164).[5]

4 Além do incidente de segurança, outro termo pertinente é "anomalia", que pode ser identificado como uma fase "pré-incidente". Se houver confirmação, da "anomalia" passa para um "incidente" real (Carvalho; Souza, 2019, p. 155).

5 A LGPD faz uso de conceitos jurídicos indeterminados em diversos momentos, quando refere "medidas de segurança adequadas" e fala em "incidentes de segurança", razão pela qual um refinamento dos conceitos por meio de

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056
2025 | v. 19 | n. 3 | p. 1-25 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056

A ANPD, por meio da Resolução CD/ANPD nº 15, de 24 de abril de 2024, que aprovou o "Regulamento de Comunicação de Incidente de Segurança", em seu art. 3º, inc. XII, recepcionou o conceito já consagrado na segurança da informação. Nesse sentido, é incidente de segurança "[...] qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais" (ANPD, 2024). Ou seja, o termo incidente de segurança (no caso, de dados pessoais), concebido como "qualquer evento adverso", parece levar a um conceito abrangente, como um "guarda-chuva" que inclui diversas possibilidades (*v.g.*, tanto a invasão de um dispositivo móvel quanto a subtração de documentos sigilosos podem constituir exemplos de incidentes de segurança).

Outras duas definições importantes surgem no aludido regulamento: *(i)* "incidente que possa acarretar risco ou dano relevante"; e *(ii)* "incidente com dados em larga escala". O primeiro, a rigor do art. 5º e incisos, ocorre quando o incidente afetar interesses e direitos fundamentais dos titulares e, cumulativamente, envolver algum destes tipos de dados: dados pessoais sensíveis, dados de crianças, adolescentes ou idosos; dados financeiros; dados de autenticação de sistemas; dados protegidos por sigilo fiscal, legal ou profissional. O segundo, por sua vez, é conceituado como "[...] aquele que abranger número significativo de titulares, considerando, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica de localização dos titulares" (ANPD, 2024).

Constatada a ocorrência de um incidente relevante (nos parâmetros da LGPD), surge o dever de notificação – elemento indispensável no processo de tratamento de incidentes, conforme o comando do art. 48 da LGPD. Sua importância é multifacetada e abrange desde a detecção e prevenção até a contribuição à segurança coletiva na internet e a geração de conhecimento (ANPD, 2022).[6] Reitera-se: um incidente de segurança de dados pessoais, como definido, é qualquer evento adverso e confirmado relacionado à violação na segurança de dados pessoais, que pode envolver acesso não autorizado, destruição, perda, vazamento ou tratamento inadequado que coloque em risco os direitos dos titulares. O vazamento de dados pessoais, sendo um tipo crítico de incidente,

avaliações de risco, em atenção aos casos específicos (natureza do incidente, tipos de dados envolvidos e gravidade das consequências), parece bem-vindo (Luciano, 2019, p. 164).

6 A própria ANPD reconhece que uma organização deve, frente a um incidente de segurança com dados pessoais, primeiro avaliar a natureza do incidente, quantificando os danos e atingidos e, após isso, iniciar um forte processo de comunicação para (a) o controlador de dados, (b) para a ANPD e (c) para os titulares de dados, em caso de risco ou dano relevante (ANPD, 2022).

caracteriza-se pela obtenção e exposição desses dados, muitas vezes afetando grande número de titulares, por isso aqui está um ponto de suma importância para reflexão quanto ao relevante papel da notificação.

A importância da notificação reside, primeiramente, na melhoria da capacidade de detecção de incidentes. Muitas instituições só descobrem que foram comprometidas quando são notificadas por terceiros; um relatório de 2021 indicou que 41% das vítimas de comprometimento souberam do problema por notificação externa[7]. Notificar, portanto, pode contribuir com a identificação dos problemas e a prevenção de novas ocorrências tanto para quem notifica quanto para quem é notificado.

Além da detecção e prevenção, a notificação contribui para a segurança geral da internet, pois, ao notificar uma tentativa de ataque da qual foi vítima, a entidade deve não apenas mitigar o dano imediato, como também buscar a solução da causa do problema, demonstrando comprometimento com questões de segurança cibernética. Isso é crucial para conter danos e prejuízos, especialmente em casos de fraudes.

Do ponto de vista regulatório, a notificação de incidentes de segurança é também uma obrigação para o controlador em determinados casos. A ANPD recebe comunicados de incidentes de segurança, devendo a comunicação ser detalhada e acompanhada de documentos, além de relatórios de incidentes, obrigatoriamente quando estiverem envolvidos dados relevantes dos titulares – inclusive, boa parte dos processos sancionadores finalizados em âmbito administrativo pela autoridade envolve "Falta de comunicação de incidente de segurança à ANPD e aos titulares" (ANPD, 2025). O relatório e a documentação servem para que a ANPD possa entender a gravidade e avaliar as medidas adotadas para mitigar os riscos. Isso demonstra que a importância da notificação transcende a esfera técnica, alcançando o cumprimento das normativas de proteção de dados, como a LGPD.

Ademais, a consolidação das informações contidas nas notificações possibilita a geração de estatísticas, a correlação entre os dados e a identificação de tendências. Esses dados são valiosos para a elaboração de recomendações e materiais de apoio, a orientação de campanhas pela adoção de boas práticas e o estabelecimento de ações em cooperação entre diferentes entidades e Computer Security Incident Response Teams (CSIRTs).

7 De acordo com o relatório da Mandiant M-Trends® 2021: Special Report, 41% das instituições vítimas de comprometimento souberam do problema por meio de notificação recebida de entidade externa. Disponível: em https://www.cert.br/docs/whitepapers/notificacoes/#1. Acesso em: 12 maio 2025.

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056
2025 | v. 19 | n. 3 | p. 1-25 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056

Para que as organizações monitorem e principalmente os responsáveis saibam como agir no caso de um incidente de segurança é fundamental a elaboração de um Plano de Resposta a Incidentes.

2.2 Vazamentos de dados

Segundo a ANPD, o vazamento de dados é um dos incidentes de segurança mais conhecidos e ocorre, essencialmente, quando dados são indevidamente acessados, coletados, divulgados ou repassados por terceiros. Algumas das consequências de um vazamento incluem a utilização dos dados e informações vazados para perpetrar fraudes, tentativas de golpes, utilização indevida por terceiros e, inclusive, para a venda de dados, situações absolutamente capazes de provocar danos aos titulares dos dados (ANPD, 2022). A despeito disso, vale destacar, até mesmo em razão da imprecisão ao tratar dos diferentes tipos de incidentes de segurança e suas consequências, que alguns tribunais pátrios (como o Tribunal de Justiça do Estado de São Paulo) não têm bases fixas para determinar se um vazamento de dados seria capaz de resultar em uma indenização extrapatrimonial, *in re ipsa*, por exemplo (Oliveira; Gomes; Matteu, 2023, p. 11-25).

Vazamentos de dados é uma realidade presente em sociedades modernas, sendo recorrentes as publicações de manchetes de jornais e sites de notícias neste sentido. A origem dos vazamentos? É absolutamente variada: organizações públicas, privadas e inclusive governamentais, o que comprova que vazamentos não se restringem a determinado setor econômico ou atividade específica (Carvalho; Souza, 2019, p. 156). Todos – pessoas, empresas, organizações e governos – estão propensos a ter seus dados (pessoais ou não) vazados em algum incidente de segurança do gênero. Mais, vazamentos de dados podem implicar violações ao direito à privacidade, à proteção de dados, à propriedade intelectual. Tais incidentes colocam as pessoas (titulares de dados, usuários, consumidores) em situação de risco de diminuição econômica, patrimonial e, inclusive, macular a honra dos atingidos, entre outros. Apenas para citar um exemplo, basta pensar no caso da negativação de um indivíduo, perante os órgãos de proteção ao crédito, em razão de uma contratação fraudulenta, viabilizada por um vazamento de seus dados pessoais.

Ademais, esse tipo de incidente de segurança pode ocorrer em razão do acesso, coleta ou divulgação indevida de dados, situação que, por sua vez, pode ter como origem: a) a invasão de uma conta de um usuário por pessoa não autorizada; b) furto de

aparelhos e equipamentos informáticos; c) erro humano (geralmente atrelado à casos de *phishing*); d) negligência com a segurança da informação e no tratamento de dados; e, nada obstante e) pode ter origem em outro tipo de incidente de segurança: a ação de *hackers* em ataques cibernéticos (CERT.br; NIC.br; CGI.br; ANPD, 2024). Ataques cibernéticos, diferentemente dos vazamentos de dados (como se verá), podem ter consequências mais catastróficas, afinal, como pontua Schneier (2019, p. 9): "[...] agora que tudo é computadorizado, as ameaças dizem respeito à vida e à propriedade"[8].

O vazamento de dados pessoais caracteriza um incidente de segurança que poderá afetar, de forma conjunta ou não, os atributos da confidencialidade, integridade e disponibilidade.

2.3 Os ataques cibernéticos

O termo "ataques cibernéticos", segundo a CISCO, diz respeito a tentativa maliciosa e deliberada de um indivíduo/organização de violar o sistema de informações de outro indivíduo/organização, a fim de obter algum benefício, monetário ou não; por vezes, o objetivo ou motivação do atacante não é financeiro, mas puramente ativista (*hacktivism*) ou militar (*cyber warfare*) (Petry; Hupffer, 2023, p. 89). Entre o ferramental mais comum de um atacante (*hacker*), é possível citar o uso *malwares* (*softwares* maliciosos), *ransomwares*, *spywares*, ataques *Man-in-the-middle* (intromissão no tráfego para filtrar e roubar dados), *DoS* ou *DDoS* (ataques para interrupção de serviços) (CISCO, [*s. d.*]); e, entre outros exemplos, técnicas de engenharia social, como o *phishing* e o *vishing* (comunicações fraudulentas que exploram o elo mais fraco da cadeia de segurança da informação: o humano) (Silva, 2023, p. 25-31; Petry; Hupffer, 2023, p. 89; Branquinho; Branquinho, 2021, p. 88-99).

Os impactos de um ataque cibernético podem ser muito graves e, sob a perspectiva do Direito, transcendem a seara penal – relativamente à penalização de cibercriminosos pela invasão de dispositivos informáticos, por exemplo. O fenômeno tem implicações em diversas áreas do Direito, uma vez que tem o condão de abalar relações contratuais

8 No original: "Now that everything is a computer, the threats are about life and property". Schneier faz esse alerta porque cada vez mais dispositivos tem se tornado *smart things*, feitos "inteligentes" por meio da adoção de dispositivos computacionais conectados à rede e que se relacionam com outros dispositivos. Cita, como exemplo, o caso de máquinas de lavar, carros e, inclusive, aviões, o que demonstra como ataques cibernéticos podem ter contornos catastróficos (Schneier, 2019, p. 9).

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056
2025 | v. 19 | n. 3 | p. 1-25 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056

entre pessoas, organizações, públicas e privadas e interromper a prestação de serviços públicos. Trata-se, pois, de uma problemática global e de irrefutável interesse público, conforme já constatado pelo Parlamento Europeu, por meio da Cyber Resilence Act, aprovada em 23 de outubro de 2024: "Os ciberataques constituem um assunto de interesse público, pois têm um impacto crítico não só na economia da União, mas também na democracia, bem como na saúde e segurança dos consumidores" (Parlamento Europeu, 2024).

Segundo a Estratégia Nacional de Segurança Cibernética (E-Ciber), a digitalização quase total dos modelos de negócios – e do próprio governo digital – teve efeitos benéficos à sociedade, uma vez que fomentou a economia global. No entanto, esse mesmo processo de digitalização teve o efeito colateral de tornar a sociedade mais vulnerável a ataques cibernéticos (Brasil, 2020a). Relativamente aos possíveis impactos de um ataque cibernético, constou da Estratégia Nacional:

> Em ataques cibernéticos recentes, grupos de hackers têm considerado sistemas de governo como alvos compensadores, no intuito de provocar diferentes impactos, como: o potencial dano à imagem do Governo perante seu público interno e perante a comunidade internacional, o descrédito da população nos serviços públicos, a desconfiança de investidores internacionais na capacidade da administração pública em proteger seus próprios sistemas, a desconfiança nos processos eleitorais, e o descontentamento da população com relação à administração pública.
> Além da proteção do próprio Governo, outro ponto crítico refere-se à proteção cibernética das empresas representantes das infraestruturas críticas. A título de compreensão, podemos conceituá-las como as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional. Essas empresas precisam ter uma abordagem consistente e evolutiva em segurança cibernética para identificar e avaliar vulnerabilidades, e gerenciar o risco de ameaças, ao observar, por exemplo, as cinco funções previstas na estrutura de segurança cibernética do National Institute of Standards and Technology – NIST, que são: Identificar, Proteger, Detectar, Responder e Restaurar (Brasil, 2020a).

A depender do tipo de ataque e do alvo, um ataque cibernético naturalmente pode ser considerado um "incidente de segurança de proteção de dados capaz de causar risco ou dano relevante aos titulares de dados", nos termos do art. 5º, §1º, da

Resolução CD/ANPD nº 15, de 24 de abril de 2024, o que ocorre quando a atividade de tratamento puder

> [...] impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade (ANPD, 2024).

A priori se pode relacionar essa classificação a ataques contra infraestruturas críticas, por exemplo, uma vez que dizem respeito a serviços e atividades essenciais da sociedade (como abastecimento de água, combustível, energia elétrica, serviços de saúde, telecomunicações etc.).

Por fim, não à toa que um dos princípios norteadores da Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança (PNCiber), instituída pelo Decreto nº 11.856/2023, é "[...] a prevenção de incidentes e de ataques cibernéticos, em particular aqueles dirigidos a infraestruturas críticas nacionais e a serviços essenciais prestados à sociedade", ao lado da proteção de direitos fundamentais e da resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos (Brasil, 2023a). Todos devem estar preparados, mas, em especial, as infraestruturas críticas, uma vez que, segundo a Estratégia Nacional de Segurança de Infraestruturas Críticas, "[...] possuem dimensão estratégica, uma vez que desempenham papel essencial tanto para a segurança e soberania nacionais, como para a integração e o desenvolvimento econômico sustentável do País" (Brasil, 2020b).

3. Aplicação do Direito frente aos incidentes de segurança: o caso do REsp 2.147.374/SP e do AREsp 2.130.619/SP julgados pelo STJ

Na presente seção, serão estudados dois precedentes do Superior Tribunal de Justiça que, ao seu modo, trataram de incidentes de segurança: *(i)* o Agravo em Recurso Especial nº 2.147.374/SP, envolvendo um ataque *hacker* e vazamento de dados, conforme mencionado na ementa do *decisum*; e *(ii)* o Agravo em Recurso Especial nº 2.130.619/SP, interposto pela Eletropaulo Metropolitana Eletricidade de São Paulo S. A. (atual Enel), envolvendo um vazamento de dados.

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056
2025 | v. 19 | n. 3 | p. 1-25 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056

3.1 O caso do Recurso Especial n. 2.147.374/SP

Na origem, a autora, titular dos dados, ajuizou ação de obrigação de fazer cumulada com indenização por danos morais em face de Eletropaulo Metropolitana Eletricidade de São Paulo S. A. Alegou que recebeu um comunicado do Instituto de Proteção de Dados Pessoais (Iprodape), com notícia sobre a ocorrência de um incidente de segurança envolvendo o vazamento dos seguintes dados pessoais: nome completo, número de CPF e RG, endereço de *e-mail* e telefones. Sustentou que teve sua intimidade violada e que, por essa razão, seria devida a indenização por danos morais, nos termos do art. 42 da LGPD[9]. No caso, a Eletropaulo não informou as circunstâncias em que o fato ocorreu nem a identidade dos terceiros que tiveram acesso a tais dados.

O pedido foi julgado improcedente na origem e, posteriormente, o Tribunal de Justiça do Estado de São Paulo (TJSP) reformou a decisão para dar parcial provimento à apelação, reconhecendo a ocorrência de vazamento de dados pessoais não sensíveis, sem, contudo, fixar indenização por dano moral. No entanto, em virtude desse vazamento, condenou a Eletropaulo a apresentar informação das entidades públicas e privadas com as quais realizou o uso compartilhado dos dados, além de fornecer declaração completa com a origem, a inexistência de registro, os critérios utilizados e a finalidade do tratamento de dados, assim como a cópia exata de todos os dados referentes à titular constantes em seus arquivos (Brasil, 2024).

As premissas constituídas no acórdão do TJSP foram as seguintes: *(i)* a recorrente Eletropaulo foi vítima de um ataque *hacker*; *(ii)* por decorrência do ataque, houve um vazamento de dados, sendo expostos dados pessoais não sensíveis da autora; *(iii)* houve falha na prestação de serviços, o que impõe aos agentes de tratamento a adoção de medidas de segurança; *(iv)* a recorrente Eletropaulo foi condenada a apresentar as informações solicitadas pelo titular, nos termos do art. 19, inc. II, da LGPD[10]; *(v)* não houve condenação em indenizar danos morais, eis que não comprovados (Brasil, 2024).

O Recurso Especial foi interposto pela Eletropaulo, nos termos do art. 103, inc. I, alínea "a", da Constituição Federal de 1988, suscitando violação dos artigos 18, inc. VII,

9 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.

10 Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

19, inc. II, 42, *caput*, 43, inc. III, e 46, *caput*, da Lei 13.709/2018 (LGPD)[11]. Argumentou-se que as obrigações constantes do art. 18, inc. VII, e 19, inc. II, dizem respeito à declaração completa nas hipóteses de compartilhamento *lícito* de dados pessoais. Contudo, no caso, entendia que o compartilhamento seria *ilícito*, uma vez que teria sido decorrente de um ataque cibernético. Eis a controvérsia do recurso: o vazamento de dados pessoais não sensíveis do titular, decorrente de atividade ilícita (ataque cibernético), seria passível de gerar ao agente de tratamento as obrigações suscitadas na LGPD? Ou, por outro lado, o fato de o vazamento ter ocorrido por decorrência de uma atividade ilícita (ataque cibernético) seria uma excludente de responsabilidade, prevista no art. 43, inc. III, da LGPD (*v.g.*, culpa de terceiro)? (Brasil, 2024). Aliás, é de questionar que culpa exclusiva de terceiro isentaria o agente de tratamento de apresentar as informações do art. 19 da LGPD?

Ao enfrentar a questão, o Superior Tribunal de Justiça invocou o direito fundamental à proteção de dados pessoais, inserido no inc. LXXIX, do art. 5º, da Constituição Federal de 1988, por meio da Emenda Constitucional nº 115/2022, referindo, inclusive, que o Supremo Tribunal Federal reconheceu a proteção de dados como direito fundamental antes mesmo de ser positivado, conforme as ADIs 6387, 6388, 6389, 6390 e 6393 MC-REF/DF (DJe 12/11/2020). Houve ainda menção ao Agravo em Recurso Especial nº 2.130.619-SP, também versando caso de ação indenizatória proposta contra Enel em razão de vazamento e acesso de dados pessoais por terceiros - que será explorado adiante (Brasil, 2024).

A Corte Superior consignou que o microssistema introduzido pela LGPD criou, ampliou e consolidou balizas para tratar do assunto, sob o prisma da proteção aos direitos fundamentais, além de sinalizar para um novo sistema de responsabilização, denominado de *responsabilidade civil proativa*, conforme consignado pelo TJSP e parte da doutrina. Reiterou ainda alguns conceitos-chave para a aplicação da LGPD (art. 5º),

11 Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.
Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056
2025 | v. 19 | n. 3 | p. 1-25 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056

como titular, controlador, operador e agentes de tratamento, delineando contornos jurídicos dos envolvidos no "ecossistema de proteção de dados".[12]

Ao verificar que a Eletropaulo se enquadraria na categoria de agente de tratamento, a Corte Superior entendeu que caberia a ela, na condição de agente de tratamento, tomar todas as medidas de segurança esperadas pelo titular, consignando, também, que os sistemas utilizados para o tratamento devem estar estruturados de forma a atender os requisitos de segurança, padrões de boas práticas, governança e princípios esculpidos no texto da LGPD. Ou seja: "[...] a legislação sugere uma série de procedimentos, de ferramentas e de condutas a serem atendidas pelos agentes de tratamento com a finalidade de evitar incidentes de segurança" (Brasil, 2024). Sobre os ataques cibernéticos e ao vazamento de dados, restou consignado:

> No que se refere ao alegado incidente de segurança (ataque hacker), é de se registrar que ataques cibernéticos *destinados a identificar vulnerabilidades de segurança* em diversos sistemas *e a obter o maior número possível de dados* tornam-se cada vez mais frequentes. Os incidentes de *data breaches* ou vazamentos de dados consistem em situações nas quais um grande volume de informações pessoais (tais como nome, endereço, números de documentos, dados bancários, credenciais de acesso, entre outros) é extraído, *resultando em consequências aos seus titulares*, dependendo da extensão do ataque. No longo prazo, a falta de elementos capazes de garantir a segurança da informação podem levar a uma verdadeira corrosão da privacidade, na qual dados sensíveis relacionados à identidade dos indivíduos podem ser indevidamente apropriados por terceiros de maneira contínua e indeterminada (Brasil, 2024).

Na realidade, ataques cibernéticos não estão essencialmente destinados a "identificar vulnerabilidades", mas, antes, *explorar vulnerabilidades preexistentes ou já identificadas pelos atacantes*, vulnerabilidades que podem decorrer tanto da negligência quanto da omissão voluntária dos agentes de tratamento, por exemplo. No mais, ainda no que tange aos propósitos do ataque, nem sempre estarão voltados a "*obter o maior número possível de dados*", assim como as consequências, como visto anteriormente, podem ser variadas, a depender do tipo de ataque, alvo e objetivo do atacante. Tais afirmações apenas demonstram a necessidade de difusão e ampliação dos conhecimentos relativos

12 Para tratar da responsabilidade civil proativa, fundada no conceito de prestação de contas, o *decisum* (Brasil, 2024) remete a Queiroz, Quinelato e Moraes (2019, p. 113).

às complexas matérias de cibersegurança e segurança da informação (isto é, especialmente diante do potencial nocivo que incidentes de segurança podem causar a relações jurídicas). Tangenciar com imprecisão o tema de incidentes de segurança (sejam vazamentos de dados ou ataques cibernéticos) pode levar a generalizações que não favorecem a aplicação do Direito, ao contrário.

Relativamente ao debate quanto à aplicação do art. 43 da LGPD, o voto prossegue, estabelecendo que "[...] um vazamento de dados nem sempre será reconhecido como fortuito externo, portanto, apto a elidir a responsabilidade civil do agente", podendo-se falar em fortuito interno, que inclusive é comparado com a previsão do enunciado nº 479 da Súmula do STJ, que prevê que as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias (Brasil, 2024). Para configuração do fortuito interno, seria necessário que *(i)* o vazamento de dados fosse um risco inerente à atividade ou *(ii)* que a falta de preparação da organização tenha sido determinante para a ocorrência do incidente.

O ponto, e inclusive a analogia ao enunciado sumular do STJ, é promissor e bem poderia ser empregado em outros casos, como os que envolvem danos decorrentes de ataques cibernéticos. No entanto, faz-se a ressalva óbvia: além de um aprofundamento teórico sobre essa possibilidade, o enquadramento do caso fortuito interno envolvendo um ataque cibernético pode depender muito das circunstâncias em que o ataque ocorreu, assim como o método de ataque utilizado, as medidas de segurança adotadas (ou não), a conduta da vítima, entre outros aspectos do caso concreto.

Ademais, o *decisum* refere que o tratamento de dados passou a se configurar como irregular quando deixou de fornecer segurança ao titular ("expectativa de legítima proteção"), nos termos do art. 44, inc. III, da LGPD.[13] Ao não provar, perante as instâncias de origem, que o vazamento dos dados da recorrida teria se dado exclusivamente em razão do incidente de segurança, seria impossível aplicar em favor da recorrente Eletropaulo a excludente de responsabilidade do art. 43, inc. III, da LGPD – até mesmo em razão da técnica legislativa, que impõe ao agente de tratamento o ônus de comprovar a quebra do nexo causal. Por essa razão é certo que o agente de tratamento responderá por violações decorrentes da quebra do dever de segurança, especialmente quando deixar

13 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: [...] III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056
2025 | v. 19 | n. 3 | p. 1-25 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056

de adotar as medidas técnicas e administrativas suscitadas no texto legal, notadamente contra "[...] acessos não autorizados (incidentes de segurança e ataques hacker), e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (Brasil, 2024).

Portanto, a Corte Superior entendeu pelo não acolhimento das teses aventadas pela recorrente Eletropaulo, uma vez que, *(a)* ainda que o vazamento tivesse decorrido de um "incidente ilícito de segurança", não existiam nos autos mínima prova de que a recorrente tivesse adotado as medidas de segurança estabelecidas na LGPD, que pudessem ser necessárias e suficientes para proteção de dados do titular, e *(b)* não há como imputar culpa exclusiva de terceiro ante a inexistência de prova de que o vazamento de dados teria ocorrido estritamente em razão do ataque cibernético. O precedente evidencia a necessidade do cumprimento do dever de segurança nas operações e atividades de tratamento de dados pessoais por agentes de tratamento (atendendo a expectativa de segurança dos titulares de dados), além de que a negligência e a insuficiência de proteção (mesmo em contextos de ataques cibernéticos) podem caracterizar um caso fortuito interno, ensejando a responsabilização civil dos envolvidos.

3.2 O caso do AREsp nº 2.130.619-SP

O caso em questão, julgado pelo STJ no Agravo em Recurso Especial nº 2.130.619-SP, refere-se a uma ação de indenização por danos morais ajuizada por uma particular contra a concessionária de energia elétrica Eletropaulo Metropolitana Eletricidade de São Paulo S.A. (atual Enel). A ação tem como causa de pedir um incidente de segurança envolvendo o vazamento e acesso, por terceiros estranhos à relação comercial, de dados pessoais e contratuais da cliente. Os dados vazados incluíam informações como nome completo, RG, gênero, data de nascimento, idade, telefone fixo, telefone celular, endereço, além de dados relativos ao contrato de fornecimento de energia elétrica (carga instalada, consumo estimado, tipo de instalação e leitura de consumo). A autora alegou que a exposição dessas informações a colocou em potencial perigo de fraude e importunações, e diante do ato ilícito pleiteou indenização por danos morais (Brasil, 2023b).

O pedido foi julgado improcedente em primeiro grau, sob o entendimento de que os dados vazados eram comuns, não acobertados por sigilo, e que o conhecimento por terceiros não violaria o direito de personalidade da autora, não havendo prova efetiva do dano, requisito essencial para configurar o dever de indenizar. O Tribunal

de Justiça do Estado de São Paulo reformou a sentença e condenou a concessionária ao pagamento de indenização, fundamentando a decisão, entre outros motivos, no fato de se tratar de dados pessoais de pessoa idosa e considerando que o vazamento de dados reservados configurou falha na prestação de serviços. No caso, o acórdão do TJSP classificou os dados vazados como sensíveis (Brasil, 2023b).

Ao analisar o recurso da concessionária, o STJ abordou pontos processuais, como a ausência de prequestionamento da tese de culpa exclusiva de terceiro, mas focou sua decisão na matéria de Direito relacionada ao vazamento de dados sob a óptica da LGPD. A Corte Superior acolheu o argumento da concessionária no tocante à classificação dos dados, destacando que o art. 5º, inc. II, da LGPD, traz um rol taxativo de dados pessoais sensíveis, que exigem tratamento diferenciado. Os dados vazados no caso concreto abrangeram nome, RG, telefone, endereço, que se caracterizam como dados pessoais, mas sem enquadramento legal como dado sensível (Brasil, 2023b).

O ponto crucial da decisão do STJ, portanto, reside no tratamento jurídico dado ao dano moral decorrente do vazamento de dados pessoais comuns. O tribunal estabeleceu que o vazamento de dados pessoais, por si só, não tem o condão de gerar dano moral indenizável. Para que haja direito à indenização, é necessário que o titular dos dados comprove o dano efetivo decorrente da exposição das informações. O STJ diferenciou essa situação do vazamento de dados sensíveis, que dizem respeito à intimidade da pessoa natural, sugerindo que as consequências jurídicas poderiam ser distintas nesses casos. Dessa forma, com o provimento ao recurso especial da concessionária foi restabelecida a improcedência do pedido de indenização por danos morais (Brasil, 2023b).

Não obstante juridicamente fundamentada nos requisitos da responsabilidade civil e na interpretação de dispositivo da LGPD, a decisão pode ser criticada no tocante à sua apreciação do fato gerador como incidente de segurança e à repercussão dessa abordagem. O STJ, ao analisar o caso, corretamente identificou o evento como um "vazamento e acesso, por terceiros estranhos" aos dados pessoais e contratuais da autora. O tribunal reconheceu que se tratou de uma "[...] falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica" (Brasil, 2023b). Esse reconhecimento alinha-se à definição de incidente de segurança de dados pessoais, entendido como qualquer evento adverso e confirmado relacionado à violação na segurança de dados pessoais, incluindo acesso não autorizado ou vazamento, que coloque em risco os direitos dos titulares. O vazamento, em si, é caracterizado pela obtenção e exposição de dados.

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056
2025 | v. 19 | n. 3 | p. 1-25 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056

No entanto, a crítica surge na consequência jurídica atribuída a esse incidente, por subestimar o risco e o potencial prejuízo inerente ao próprio vazamento de dados comuns, mesmo que o dano não se materialize imediatamente de forma facilmente comprovável pela vítima ou que se trate de dados sensíveis. As fontes que cuidam de incidentes de segurança destacam que o vazamento de dados pessoais, sendo um tipo crítico de incidente, favorece a criminosos a oportunidade de realizar diversos tipos de delitos como fraudes, obtenção de senhas, clonagem de cartões de crédito e permite o uso de engenharia social para enganar e tirar proveito do cidadão. O prejuízo ao cidadão é, portanto, diretamente relacionado à oportunidade que esse vazamento favorece, sem a necessidade de provar o dano efetivo.

Ao exigir a comprovação do dano efetivo para dados comuns, a decisão do STJ parece focar mais na responsabilidade civil tradicional, que tem na comprovação do dano elemento essencial, do que na gravidade do incidente de segurança em si e no risco que ele cria para o titular dos dados. A exposição de informações como nome, RG, telefone e endereço, embora comuns, são precisamente os blocos de construção para muitas atividades fraudulentas – que inclusive podem ser potencializadas com o uso malicioso da tecnologia, como sistemas de inteligência artificial, *deep fakes*, entre outros. A autora, no caso, alegou justamente o potencial perigo de fraude e importunações, o que, na visão do STJ, não foi suficiente sem a prova do dano efetivo (Brasil, 2023b).

A importância da notificação de incidentes de segurança, conforme destacado inicialmente, reside na detecção, prevenção, contenção de danos e prejuízos, e no cumprimento de obrigações regulatórias, que visam, em última instância, a proteger os titulares e permitir que a ANPD avalie a gravidade e as medidas adotadas. A simples ocorrência do vazamento já impõe obrigações ao controlador e gera a necessidade de ações de mitigação. A decisão do STJ, ao exigir a prova do dano para fins de indenização por danos morais em vazamentos de dados comuns, coloca um ônus considerável sobre o titular dos dados, que pode ter dificuldades em rastrear e comprovar que um dano específico, como por exemplo uma tentativa de fraude ou importunação, resultou diretamente daquele vazamento em particular, especialmente se o vazamento for amplo e seus dados forem usados em conjunto com outras fontes (Brasil, 2023b).

Em suma, enquanto a decisão do STJ estiver alinhada com a necessidade de provar o dano moral em casos que não envolvam dados sensíveis, ela poderá ser criticada por potencialmente minimizar as consequências do incidente de segurança em si, focando apenas no dano materializado, e não no risco significativo criado pela exposição não

autorizada de dados pessoais, mesmo que comuns. Essa abordagem pode enviar uma mensagem de que incidentes envolvendo dados comuns têm menor relevância legal para o titular, apesar do potencial de uso malicioso destacado nas fontes sobre segurança digital.

4. Considerações finais

No cenário da era digital, caracterizada pela expansão exponencial da circulação de dados e pela crescente dependência de sistemas informacionais, constata-se uma acentuada vulnerabilidade da sociedade a incidentes de segurança, notadamente ataques cibernéticos e vazamentos de dados, os quais, longe de se restringirem a meros reveses técnicos, configuram ameaças concretas e multifacetadas à tutela jurídica e aos direitos fundamentais, como a privacidade e a proteção de dados pessoais. Assim, a crescente sofisticação das ameaças digitais e a multiplicidade de formas, agentes e impactos que esses incidentes podem assumir impõem desafios significativos para a aplicação do Direito, exigindo respostas normativas e jurisprudenciais que estejam à altura de sua complexidade técnica e dos riscos sistêmicos envolvidos.

A análise dos precedentes do Superior Tribunal de Justiça, em particular o REsp 2.147.374/SP e o AREsp 2.130.619/SP, revela nuances e respostas parcialmente divergentes quanto à responsabilização civil dos agentes de tratamento de dados. O primeiro julgado sinaliza para uma responsabilidade objetiva e proativa, enfatizando o dever de adoção de medidas de segurança adequadas por parte do agente, ainda que o incidente decorra de conduta ilícita de terceiro, e reconhecendo a expectativa de legítima proteção por parte do titular. O segundo, por sua vez, ao tratar de vazamento de dados não sensíveis, alinha-se à lógica tradicional da responsabilidade civil subjetiva, reforçando a necessidade de comprovação de dano efetivo para fins indenizatórios.

A aplicação do Direito pelo STJ em face da complexidade e dos múltiplos matizes dos incidentes de segurança, como vazamentos e ataques cibernéticos, tem se manifestado de forma parcialmente divergente. Observa-se um trânsito entre dois modelos de responsabilização: uma vertente que sinaliza para a responsabilidade objetiva e proativa do agente de tratamento, enfatizando o dever de segurança adequado; e outra que se alinha à lógica subjetiva tradicional, ao exigir a comprovação de dano efetivo para fins indenizatórios em casos de vazamento de dados pessoais não sensíveis. Tal dissenso e a possível generalização conceitual do termo "incidentes de segurança" são críticos, pois

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056
2025 | v. 19 | n. 3 | p. 1-25 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056

tendem a subestimar o risco e o potencial prejuízo inerente à mera exposição indevida de informações, impondo um ônus considerável ao titular e comprometendo a proteção eficaz prevista por normas como a LGPD, o Marco Civil da Internet (MCI) e o Código de Defesa do Consumidor (CDC).

O dissenso interpretativo e a possível generalização do termo "incidentes de segurança" no discurso jurídico evidenciam a premissa de uma maior acuidade conceitual e técnica na qualificação desses eventos. A abordagem indistinta quanto às causas, natureza e efeitos dos incidentes tende a comprometer a eficácia da proteção conferida pela LGPD e a própria segurança jurídica das decisões. Critica-se, neste ponto, a exigência de prova do dano em casos de vazamento de dados considerados "comuns", pois ela subestima o risco e o potencial prejuízo inerente à mera exposição indevida de informações pessoais. Vazamentos de dados pessoais, mesmo aqueles não classificados como sensíveis, favorecem a prática de crimes como fraudes, golpes e uso indevido, colocando os titulares em situação de riscos concretos. Exigir que o titular prove o nexo causal entre o vazamento e um dano específico impõe um ônus considerável, podendo constituir um entrave à concretização do direito fundamental à proteção de dados.

Diante desse panorama, impõe-se a consolidação de um marco interpretativo que, coerente com os ditames da LGPD, reconheça a gravidade inerente aos incidentes de segurança. Uma compreensão aprimorada da natureza e das consequências desses eventos, dissociada de uma generalização simplista, deve levar em consideração a classificação e o risco que eles representam, independentemente da natureza específica dos dados expostos. A eventual responsabilização civil deve, portanto, sopesar de forma mais robusta a falha na adoção de medidas preventivas e a simples exposição dos titulares a riscos concretos, mesmo na ausência de danos imediatamente quantificáveis. Um enfoque nas medidas adotadas para conter, gerir e estabilizar os danos causados pelo incidente, aliado ao reconhecimento do risco como elemento relevante à responsabilização, permitirá assegurar uma proteção mais efetiva aos direitos fundamentais no ambiente digital e fomentar a cultura de segurança da informação preconizada pela legislação.

REFERÊNCIAS

ANPD. *Atividades fiscalizatórias.* Disponível em: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos?_authenticator=b05dbbec15247ce4c8b7065d588ef945f6d4d340. [*s. d.*] Acesso: 16 abr. 2025.

ANPD. *Incidentes de segurança com dados pessoais*. 2022. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/acoes-e-programas/programas-projetos-acoes-obras-e-atividades/semana-da-protecao-de-dados-2022/incidentes-de-seguranca-com-dados-pessoais. Acesso em: 14 mar. 2025.

ANPD. *Resolução CD/ANPD nº 15, de 24 de abril de 2024*. Aprova o Regulamento de Comunicação de Incidente de Segurança. 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 11 set. 2025.

BRANQUINHO, T.; BRANQUINHO, M. *Segurança cibernética industrial*. Rio de Janeiro: Alta Books, 2021.

BRASIL. *Decreto nº 10.222, de 5 de fevereiro de 2020*. Aprova a Estratégia Nacional de Segurança Cibernética. 2020a. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em: 20 set. 2025.

BRASIL. *Decreto Nº 10.569, de 9 de dezembro de 2020*. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. 2020b. Disponível em: https://www.planalto.gov.br/cCivil_03/_Ato2019-2022/2020/Decreto/D10569.htm. Acesso em: 20 set. 2025.

BRASIL. *Decreto nº 11.856, de 26 de dezembro de 2023*. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. 2023a. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-11.856-de-26-de-dezembro-de-2023-533845289. Acesso em: 20 set. 2025.

BRASIL. Superior Tribunal da Justiça. STJ. *AREsp n. 2.130.619/SPb*. 2023b. Relator Ministro Francisco Falcão, Segunda Turma, julgado em 7/3/2023, DJe de 10/3/2023.

BRASIL. Superior Tribunal de Justiça. STJ. *Recurso Especial n. 2.147.374/SP*. 2024. Relator Ministro Ricardo Villas Bôas Cueva, Terceira Turma, julgado em 3/12/2024, DJEN de 6/12/2024.

CARVALHO, A. C.; SOUZA, V. L. e. Segurança da informação e resposta a incidentes de vazamento no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD). *Revista do Advogado*, n. 144, nov. 2019.

CERT.br; NIC.br; CGI.br; ANPD. *Vazamento de dados*. Disponível em: https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf. Acesso em: 13 set. 2025.

CISCO. *What is a cyberattack?* Disponível em: https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-cyberattack.html. [*s. d.*]. Acesso: 15 set. 2025.

FREIRE, A. *et al.* (org.). *Jornada segurança da informação*: unindo visão executiva e técnica para estratégia, comportamento, inovação e tendências. Rio de Janeiro: Brasport, 2024. *E-book*. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 2 set. 2025.

HINTZBERGEN, J. *et al. Fundamentos da segurança da informação*: com base na ISO 27001 e na ISO 27002. Tradução: Alan de Sá. Rio de Janeiro: Brasport, 2018.

JIMENE, C. do V. Capítulo VII: da segurança e boas práticas. *In*: MALDONADO, V. N.; OPICE, B. R. (coord.). *LGPD*: Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019. *E-book*.

LUCIANO, M. Vazamentos de dados na LGPD: em busca do significado de "incidentes de segurança". *Revista do Advogado*, n. 144, nov. 2019.

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 19(3) | e18056
2025 | v. 19 | n. 3 | p. 1-25 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v19n318056

OLIVEIRA, A. G. de; GOMES, T. R. P. de A.; MATTEU, I. F. de. Vazamento de dados e dano moral: uma análise a respeito do entendimento de julgados do Tribunal de Justiça de São Paulo. *Revista de Direito Constitucional e Internacional*, v. 139, p. 11-25, set./out. 2023.

PARLAMENTO EUROPEU. Regulamento (EU) 2024/2847 do Parlamento Europeu de 23 de outubro de 2024, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera os Regulamentos (UE) n.º 168/2013 e (UE) 2019/1020 e a Diretiva (UE) 2020/1828 (Regulamento de Ciber-Resiliência). *Jornal Oficial da União Europeia*, 20 nov. 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L_202402847. Acesso em: 24 ago. 2025.

PETRY, G. C.; HUPFFER, H. M. O princípio da segurança na era dos ciberataques: uma análise a partir do escopo protetivo da LGPD. *Revista do CNJ*, v. 7, n. 1, 2023.

QUEIROZ, J. Q.; MORAES, M. C. B. de. Autodeterminação informativa e responsabilização proativa. *Cadernos Adenauer*, v. XX, n. 3, p. 113, 2019.

SCHNEIER, B. *Click here to kill everybody*: security and survival in a hyper-connected world. New York: W.W. Norton & Company, 2019.

SILVA, M. B. F. da. *Cibersegurança*: [...]. Rio de Janeiro: Freitas Bastos, 2023.

Gabriel Cemin Petry

Mestrando em Direito Público pela Unisinos, com bolsa PROEX/Capes. Graduado em Direito pela Universidade Feevale. Integrante do Grupo de Pesquisa CNPq/Feevale: Direito e Desenvolvimento. Integrante do Projeto de Pesquisa CNPq/Feevale: Inteligência Artificial para um Futuro Sustentável: Desafios Jurídicos e Éticos; integrante do Grupo de Pesquisa Jusnano/CNPq; colaborador na Mediterranea International Centre for Human Rights Research, MICHR, Itália. Advogado. Autor de artigos jurídicos.
Universidade do Vale do Rio dos Sinos, (Unisinos)
Novo Hamburgo, RS, Brasil
E-mail: Gabrielcpetry96@gmail.com

Karin Regina Rick Rosa

Advogada. Mestra em Direito pela Universidade Unisinos. Especialista em Direito Processual Civil. Professora de Direito Civil e Direito Notarial e Registral. Membro da Academia Notarial Brasileira - Cadeira nº 38. Membro da Diretoria Executiva do IBDFAM-RS. Membro do Conselho Consultivo do Ibradim. Possui certificação internacional Exin - Data Protection and Privacy e Security Information System. Coordenadora de livros e autora de artigos jurídicos.
Universidade do Vale do Rio dos Sinos (Unisinos)
Novo Hamburgo, RS, Brasil
E-mail: karinrick.rosa@gmail.com

Wilson Engelmann

Doutor e mestre em Direito Público, Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos (Unisinos). Realizou estágio Pós-doutoral em Direito Público-Direitos Humanos, no Centro de Estudios de Seguridad (Ceseg), da Universidade de Santiago de Compostela, Espanha. Professor e pesquisador do Programa de Pós-Graduação em Direito - Mestrado e Doutorado e do Mestrado

Profissional em Direito da Empresa e dos Negócios, ambos da Unisinos. Bolsista de Produtividade em Pesquisa do CNPq e líder do Grupo de Pesquisa Jusnano, credenciado no CNPq.
Universidade do Vale do Rio dos Sinos (Unisinos)
Novo Hamburgo, RS, Brasil
E-mail: wengelmann@unisinos.br