Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v11i12.23177

A NATUREZA JURÍDICA DA RESPONSABILIDADE CIVIL DAS EMPRESAS POR FALHAS DE SEGURANÇA NA PROTEÇÃO DE DADOS PESSOAIS: ANÁLISE À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Waldir Franco de Camargo Junior[1]
Thyara Gonçalves Novais[2]
Daniel Alves Gomes Silva[3]

RESUMO: Este trabalho de conclusão de curso tem como objetivo analisar a responsabilidade das empresas por falhas de segurança na proteção de dados pessoais, com base na Lei Geral de Proteção de Dados Pessoais (LGPD). A metodologia empregada consistiu em uma pesquisa bibliográfica e documental, explorando a legislação pertinente, estudos de caso de violações de dados e a jurisprudência brasileira. A justificativa para este estudo reside na crescente importância da proteção de dados em um cenário de aumento do cibercrime e na necessidade de compreender as implicações da LGPD para empresas e consumidores. Os resultados da pesquisa indicam que a LGPD estabelece mecanismos claros de responsabilização, exigindo das empresas a implementação de medidas de segurança e transparência no tratamento de dados. A discussão aponta que a LGPD impacta diretamente a confiança do público e o sucesso dos negócios, tornando a proteção de dados um diferencial competitivo. O judiciário brasileiro, embora em fase de consolidação, tem buscado responsabilizar os agentes de tratamento por incidentes de segurança, com a jurisprudência evoluindo para definir os contornos da responsabilidade civil nesse contexto.

Palavras-chaves: LGPD. Responsabilidade. Segurança. Dados Pessoais, Vazamento.

ABSTRACT: This final course project aims to analyze the responsibility of companies for security failures in the protection of personal data, based on the General Data Protection Law (LGPD). The methodology employed consisted of bibliographic and documentary research, exploring the relevant legislation, case studies of data breaches, and Brazilian jurisprudence. The justification for this study lies in the growing importance of data protection in a scenario of increasing cybercrime and the need to understand the implications of the LGPD for companies and consumers. The research results indicate that the LGPD establishes clear accountability mechanisms, requiring companies to implement security and transparency measures in data processing.The discussion points out that the LGPD directly impacts public trust and business success, making data protection a competitive differentiator. The Brazilian judiciary, although in a consolidation phase, has sought to hold data processing agents accountable for security incidents, with jurisprudence evolving to define the contours of civil liability in this context.

Keywords: LGPD. Responsibility. Security. Personal Data. Data Breach.

[1] Orientador. Docente na Faculdade de Ilhéus-CESUPI.
[2] Coorientadora. Mestre em Direito, Docente na Faculdade de Ilhéus-CESUPI.
[3] Graduando em Direito na Faculdade de Ilhéus-CESUPI.

1. INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD) é resultado de um movimento da sociedade e autoridades brasileiras. Desde o início da década, empresas e usuários procuram soluções para a segurança virtual, que se torna mais importante devido ao aumento do cibercrime. Em 2018, um estudo da McAfee publicado na revista Veja indicou que o Brasil registrou perdas progressivas com crimes virtuais, totalizando R$10 bilhões por ano (MACHADO, 2018). O Brasil está em 4° colocado entre os países com os mais altos índices de crimes virtuais, da américa latina (CNN, 2024). A LGPD surge do esforço de várias instâncias para combater as fraudes e crimes online, que crescem rapidamente no Brasil.

A LGPD representou um avanço significativo no ordenamento jurídico brasileiro ao estabelecer um conjunto de regras e princípios para o tratamento de dados pessoais. Inspirada em legislações internacionais, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD busca equilibrar o desenvolvimento tecnológico e econômico com a proteção dos direitos fundamentais à privacidade e à autodeterminação informativa.

Essa lei, tem remodelado a maneira como as empresas gerenciam informações pessoais, estabelecendo responsabilidades claras que variam de advertências e multas. Tais medidas acentuam a importância de um ambiente digital mais seguro e confiável. Conforme a Federação Brasileira de Bancos (Febraban, 2023), tomando como base o ano 2022, oito em cada dez operações bancárias são realizadas virtualmente, o que evidencia a importância de normas rigorosas que possam assegurar maior confiabilidade nos meios virtuais fornecidos por diversas empresas.

O presente artigo tem como objetivo geral demonstrar a relevância da Lei Geral de Proteção de Dados (LGPD) no cenário atual, marcado pela forte migração de negócios e interações interpessoais para o ambiente *online*, impulsionada pelo uso de aparelhos eletrônicos que vem se tornado quase que uma extensão do nosso corpo. Sendo que uma das características fundamentais do Direito é a sua constante evolução para acompanhar o desenvolvimento social, adaptando-se e respondendo às novas necessidades de uma sociedade em contínua transformação. Neste contexto, a LGPD surge como resposta à necessidade de proteção adequada em um domínio que, por vezes, é percebido como uma "terra de ninguém", expressão historicamente utilizada em tempos de guerra para designar uma área perigosa e desprovida de regulamentação.

Ao passo que, o objetivo específico é demonstrar a efetiva atuação da LGPD no cenário

Revista Ibero-Americana de Humanidades, Ciências e Educação. São Paulo, v. 11, n. 12, dez. 2025.
ISSN: 2675-3375

mais comum de utilização das redes: os negócios. Seja de forma direta entre o usuário e uma loja *online* ou de forma indireta com a simples navegação em redes sociais mas que grandes empresas usam para vincular seus serviços e produtos, sendo assim uma forma de comércio mais velada. Seus gostos, necessidades e sua identidade, ficam armazenados em bancos de dados por essas empresas, o cerne deste artigo é apresentar seus direitos quanto a usuário, e as responsabilidades quanto a empresa, seus dados tem valor, e merecem de tratamentos e cuidados adequados.

A metodologia empregada na elaboração deste artigo baseia-se integralmente na análise documental, pesquisas em plataformas de notícias e, principalmente, no texto normativo da Lei Geral de Proteção de Dados Pessoais (LGPD).

Nesse contexto surge o seguinte problema: Qual a natureza jurídica da responsabilidade civil dos agentes de tratamento (controladores e operadores) por danos patrimoniais e morais decorrentes de incidentes de segurança e vazamentos de dados pessoais, à luz da Lei Geral de Proteção de Dados (LGPD) e do atual posicionamento do Superior Tribunal de Justiça (STJ).

2. FUNDAMENTOS E APLICAÇÃO DA RESPONSABILIDADE CIVIL NA LGPD

No cerne da LGPD reside a atribuição de responsabilidade aos agentes de tratamento, especialmente às empresas que atuam como controladoras e operadoras de dados pessoais. Essa responsabilidade abrange a implementação de medidas de segurança adequadas para proteger os dados contra acessos não autorizados, destruição, perda, alteração ou qualquer forma de tratamento ilícito.

As violações dos bancos de dados das grandes empresas por hackers, que vendem essas informações para terceiro interessado com propósito desconhecido, segundo a CNN Brasil (2023), cerca de 25% das empresas no Brasil tiveram perdas por conta da ação de hackers em 2022. Conhecer a LGPD e fazer valer seus direitos é uma forma de forçar empresas que trabalham com dados pessoais a melhorarem o sistema de segurança em seus bancos de dados, como também evitar que os próprios controladores (empresas responsáveis pelos dados), compartilhem esses dados indevidamente sem o conhecimento do titular.

Em 2021 a 18ª Vara de Relações de Consumo de Salvador condenou a Confederação Nacional de Dirigentes Lojistas (CNDL) foi condenada a pagar R$5 mil de indenização a um consumidor por divulgar seus dados pessoais sem consentimento. A juíza Lícia Pinto Fragoso Modesto confirmou que a CNDL estava divulgando as informações do requerente em seus canais digitais, o que resultou em assédio por parte de empresas. Para a magistrada, houve uma

violação dos direitos de personalidade do autor, incluindo sua vida íntima e privada (TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA, 2023).

O presente trabalho de conclusão de curso tem como objetivo analisar a responsabilidade das empresas por falhas de segurança na proteção de dados pessoais com base na LGPD. Para tanto, serão explorados os mecanismos de responsabilização previstos na legislação, as obrigações impostas às empresas em relação à transparência e segurança, o impacto dessas exigências na confiança do público e nos negócios, a análise de casos reais de violações e suas consequências, bem como o atual comportamento do judiciário brasileiro sobre o tema. Ao final, será apresentado um resumo das principais conclusões e das referências bibliográficas utilizadas.

Para maior compreensão dos termos utilizados, vise o artigo 5°.

> Art.5°. (LGPD). I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> 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 Autoridade Nacional de Proteção de Dados (ANPD);
> IX - agentes de tratamento: o controlador e o operador;
> (BRASIL. Lei nº 13.709, de 14 de agosto de 2018)

2.1 RESPONSABILIDADE DAS EMPRESAS

Um dos pilares centrais da Lei Geral de Proteção de Dados Pessoais (LGPD) é a atribuição de responsabilidades claras às empresas, denominadas Controladores e Operadores, em relação ao tratamento de dados pessoais. Essa responsabilização abrange todo o ciclo de vida da informação, desde a coleta até a eliminação dos dados, conforme o princípio da responsabilização e prestação de contas (accountability), previsto no artigo 6º, inciso X, da LGPD, que exige a demonstração de medidas eficazes para o cumprimento da lei (BRASIL, 2018). Se não vejamos:

> **Art. 6º, X -** responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, **inclusive, da eficácia dessas medidas**. (BRASIL. Lei nº 13.709, de 14 de agosto de 2018) **Grifei**

É central nesse contexto, exigindo que os agentes de tratamento demonstrem a adoção de medidas eficazes para garantir a observância e o cumprimento da lei.

Revista Ibero-Americana de Humanidades, Ciências e Educação. São Paulo, v. 11, n. 12, dez. 2025.
ISSN: 2675-3375

A legislação impõe às empresas a necessidade de atuar com transparência em relação ao tratamento de dados, informando de maneira clara e acessível aos titulares sobre a finalidade da coleta, os responsáveis pelo tratamento, os seus direitos e os procedimentos para exercê-los.

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso.
>
> (BRASIL. Lei nº 13.709, de 14 de agosto de 2018)

Essa exigência visa garantir que os titulares tenham conhecimento e controle sobre seus dados pessoais.

No que concerne à segurança, a LGPD em seu artigo 46, determina que as empresas devem implementar medidas técnicas e administrativas aptas a proteger os dados pessoais de incidentes como acessos não autorizados e vazamentos. Vejamos:

> 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.
>
> (BRASIL. Lei nº 13.709, de 14 de agosto de 2018)

Isso inclui a adoção de políticas internas de segurança da informação, a realização de avaliações de risco, a implementação de controles de acesso, a utilização de criptografia, a realização de testes de segurança e a elaboração de planos de resposta a incidentes. Nos casos em que houverem os vazamentos por quaisquer motivos deverão informar aos usuários ou titulares dos dados, como bem descreve o art. 48. "*O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.* " Nesta comunicação deverão estar presentes a descrição dos dados afetados e as medidas adotadas para adotadas para que se reverta ou que seu dano venha a ser mitigado, em se tratando de incidentes mais gravosos poderá a autoridade nacional tornar o caso público, sendo portanto, uma forma de punição pois diminui a confiabilidade do operador. Vejamos:

> Art. 48 § 2º. A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
>
> I - ampla divulgação do fato em meios de comunicação; e
>
> II - medidas para reverter ou mitigar os efeitos do incidente.
>
> (BRASIL. Lei nº 13.709, de 14 de agosto de 2018)

Em caso de descumprimento da LGPD, incluindo falhas de segurança que resultem em incidentes com dados pessoais, as empresas estão sujeitas a diversas penalidades administrativas aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD).

> 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.
>
> (BRASIL. Lei nº 13.709, de 14 de agosto de 2018)

Conforme previsto no artigo 52. Essas sanções podem variar desde advertências até multas de até 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração, além de outras medidas como a publicação da infração, o bloqueio ou a eliminação dos dados.

> Art. 52. [...]em razão das infrações cometidas [...], ficam sujeitos[...]
>
> I- advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III - multa diária, observado o limite total a que se refere o inciso II;
>
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI - eliminação dos dados pessoais a que se refere a infração;
>
> (BRASIL. Lei nº 13.709, de 14 de agosto de 2018)

Operadores e controladores são solidariamente responsáveis por danos resultantes de violações de dados sob sua custódia. O amparo legal para essa questão encontra-se nos artigos 42 a 45, os quais tratam da responsabilidade e dos danos decorrentes da falta de segurança, uso indevido ou compartilhamento de dados sem o consentimento do titular. É fundamental que o titular seja devidamente informado sobre onde e como seus dados serão utilizados.

Além disso, a responsabilidade pelo dano causado por compartilhamento não autorizado também recai sobre eles. Caso a operadora tenha interesse em compartilhar esses dados, os titulares devem ser informados de forma inequívoca, sem margem para dúvidas. O Art. 8º, § 4º, elucida um ponto crucial sobre o consentimento para o tratamento de dados pessoais, estipulando que este deve estar atrelado a finalidades específicas e predeterminadas. Isso implica que o indivíduo deve ser clara e detalhadamente informado sobre o que será feito com seus dados e com qual propósito serão utilizados.

Além disso, as autorizações genéricas ou amplas para o tratamento de dados pessoais, que não especificam exatamente as finalidades, são consideradas nulas. Em outras palavras, um consentimento vago ou sem detalhes não é válido de acordo com a lei. Essa regra é essencial para proteger os direitos dos titulares de dados, garantindo que eles tenham total conhecimento e controle sobre o uso das suas informações pessoais (BRASIL, 2018, Art. 8º, § 4º).

2.2 IMPACTOS NA CONFIABILIDADE DOS NEGÓCIOS

A LGPD tem exercido uma influência significativa na confiança do público em relação às empresas que lidam com seus dados pessoais. A maior conscientização sobre os direitos à privacidade e à proteção de dados leva os consumidores a serem mais seletivos e a exigir maior transparência e segurança das organizações. (Gagno et al. 2022).

A ausência dessa confiança é uma das principais barreiras para o crescimento do comércio online, a confiança é um pilar crucial nas transações digitais, sendo a sua ausência um dos maiores obstáculos ao crescimento do comércio eletrônico. A percepção de segurança, essencial em ambientes onde o cliente não controla diretamente as ações do vendedor, é sustentada por três dimensões principais: competência, benevolência e integridade (Silva, 2021).

Empresas que demonstram um compromisso efetivo com a proteção de dados tendem a fortalecer a confiança de seus clientes, o que pode se traduzir em um aumento de negócios baseados na confiança do cliente na segurança prestada por essa empresa, a exemplo posso mencionar o Mercado Pago, método de pagamento criado pelo Mercado Livre que aumentam a confiança do consumidor, chegando a ser um fator decisivo de compra, se o site oferece esse método ou não. Em suma, a reputação de uma empresa como guardiã confiável das informações pessoais pode se tornar um diferencial competitivo importante (Gagno et al. 2022).

Por outro lado, o contrário também é verdadeiro, haja visto que, falhas de segurança podem resultar em vazamentos ou acessos indevidos e podem gerar uma queda significativa na confiança do público. Essa perda de confiança pode levar à rejeição de produtos e serviços oferecidos por ela, como também, o cancelamento de contratos e a danos à imagem da marca, causando impacto negativo nos resultados financeiros e a sustentabilidade dos negócios (NETCONSULTING, 2025).

A LGPD, portanto, estabelece um novo paradigma em que a proteção de dados não é apenas uma obrigação legal, mas também um fator crucial para a construção de relacionamentos de confiança com os clientes e para o sucesso a longo prazo dos negócios na economia digital (Gagno et al. 2022).

2.3 CASOS REAIS DE VIOLAÇÕES E SUAS CONSEQUÊNCIAS

A ocorrência de incidentes de segurança envolvendo dados pessoais tem se tornado cada vez mais comum, expondo a vulnerabilidade de empresas de diversos setores. No Brasil, o

Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) reportou um recorde de 3.253 vazamentos de dados em 2024, um número que mais do que dobrou em relação ao período de 2020 a 2023, estabelecendo o maior índice já registrado pelo Governo Federal (IT FORUM, 2024).

Essa escalada confirma a crescente ameaça e a fragilidade das medidas de segurança adotadas por muitas instituições (IT FORUM, 2024). A análise de casos reais de violações permite ilustrar as diferentes formas como essas falhas podem ocorrer e as graves consequências para os titulares dos dados e para as empresas responsáveis.

As falhas não se limitam apenas a ataques externos, como o ransomware e o roubo de credenciais (MIGALHAS, 2025). Casos de violação têm levado a graves consequências jurídicas, como a condenação de empresas ao pagamento de indenizações individuais, a exemplo do caso da Cyrela, a primeira a ser condenada na justiça com base na LGPD (Lei Geral de Proteção de Dados) (PORTAL DE PRIVACIDADE, 2025).

As penalidades impostas pela LGPD podem variar desde advertências até multas de até R$50 milhões por infração, aplicadas pela Agencia Nacional de Proteção de Dados (ANPD) em casos de descumprimento, como a ausência de notificação do incidente aos titulares (CNN BRASIL, 2023). Tais fatos demonstram que as consequências dos incidentes de segurança transcendem os danos operacionais, atingindo a reputação e gerando pesados encargos financeiros e legais para os agentes de tratamento. Na sequência, veremos alguns casos relevantes para o tema:

O caso Facebook e WhatsApp (Empresa Meta), ocorrido entre 2018 e 2019, envolveu três grandes ataques que resultaram no vazamento massivo de dados de milhares de usuários, as falhas que envolveram desde o acesso indevido de terceiros a fotos privadas até a instalação de software espião nas chamadas de vídeos dos usuários. A ação foi proposta pelo Instituto Defesa Coletiva, na qual sustentou que houve exposição massiva de dados sensíveis e um desrespeito a LGPD. Em relato o desembargador Newton Teixeira Carvalho, destaca que o serviço prestado pela empresa foi defeituoso e contrapõe a LGPD e o CDC, restante evidente o dever de indenizar, em suas palavras: "*O dano moral coletivo é evidente e se materializa pelo simples fato de o vazamento ter ocorrido, afrontando toda a coletividade, que teve seus dados pessoais expostos sem autorização.*" A Justiça de Minas Gerais condenou a empresa a pagar o valor de R$40 milhões por danos morais coletivos (Migalhas, 2025) .

Caso Netshoes (empresa Netshoes), também em 2018, a Netshoes teve vazamento de dados de 2 milhões de clientes, afirmou que os dados teriam vazado após um incidente de ataque

cibernético. O MP apurou que um incidente expôs dados pessoais como nome, CPF, e-mail, data de nascimento como também o histórico de compras (GLOBO, 2019).

As investigações, constataram que informações mais sensíveis como cartão de crédito ou senhas de clientes não foram reveladas, entretanto, deixaram as pessoas vulneráveis a golpes e fraudes (GLOBO, 2019).

A empresa foi condenada a pagar a quantia de R$500 mil, a título de danos morais, depositados no Fundo de Defesa de Direitos Difusos (FDD) – vinculado ao Ministério da Justiça. Com a assinatura de um documento se compromete a adotar melhores medidas de proteção como também a realizar campanhas de conscientização relacionadas ao tema "melhores práticas para privacidade". Quanto aos indivíduos lesados, não houve menção à indenização individual (GLOBO, 2019).

Novamente, o ocorrido foi em 2018, não houveram aplicações mais severas a empresa, como por exemplo o previsto no art. 52, inciso II – "*multa simples, de até 2% (dois por cento) do faturamento [...] da empresa*", em que pese, no ano apresentado a empresa teve uma redução no faturamento de 3,7%, ainda totalizou um montante de R$ 417 milhões, aplicando o inciso II a multa poderia chegar ao valor de R$ 8.340.000. Para além do dano financeiro o inciso IV – "*publicização da infração após devidamente apurada e confirmada a sua ocorrência;* " Poderia manchar a reputação da empresa (BRASIL. Lei nº 13.709, de 14 de agosto de 2018).

Caso Drogasil (empresa RaiaDrogasil), investigada em fevereiro de 2023, pela suposta venda de dados pessoais de seus consumidores, de acordo ao narrado pelo UOL, Veja Negócios, CNN Brasil e outras revistas (SAKAMOTO, 2023), os consumidores seriam levados a fornecer seus dados pessoais ao banco de dados da empresa sob promessa de descontos nos produtos e serviços, ocultando a real intenção da empresa que era a captação dos dados para utilização posterior não informada aos titulares, indo de encontro ao já mencionado texto legal do art.8 § 3º "*É vedado o tratamento de dados pessoais mediante vício de consentimento.*" (BRASIL. Lei nº 13.709, de 14 de agosto de 2018). Após essa denúncia o Ministério da Justiça notificou a empresa para prestar esclarecimentos. As medidas de regularização requisitadas pela ANPD foram:

- Disponibilizar aos clientes cadastrados no programa de fidelidade Universal um mecanismo de verificação de identidade alternativo à biometria.
- Disponibilizar aos titulares dos dados um canal no Portal de Privacidade do Titular, que permita a obtenção de informações relativas ao tempo de armazenamento dos diferentes dados pessoais coletados e tratados.

- Apresentar à ANPD uma série de informações e documentos, especialmente sobre como os dados pessoais sensíveis são usados para criar perfis comportamentais
- Detalhar á ANPD como esses dados são compartilhados com a Rd Ads, braço de publicidade do grupo e como é feita a oferta de publicidade direcionada para empresas terceiras.

O caso da CNDL, mencionado na introdução deste artigo, refere-se à condenação da Confederação Nacional de Dirigentes Lojistas em 2021, pela 18ª Vara de Relações de Consumo de Salvador. A empresa foi obrigada a indenizar um consumidor em R$ 5 mil por divulgar seus dados pessoais sem consentimento. A magistrada Lícia Pinto Fragoso Modesto confirmou que a CNDL estava divulgando as informações do requerente em seus meios digitais sem autorização, o que resultou no assédio de outras companhias (TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA, 2023). Em suas palavras, "É incontroverso, que a ré vem disponibilizando em suas plataformas digitais, os dados pessoais da parte autora, sem que a mesma tenha emitido autorização para a prática de tais atos." (TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA, 2023). Na sequência, a magistrada concluiu que "[...] resta devidamente comprovado que o autor foi assediado por diversas empresas pelo fato de ter seus dados pessoais vazados pela empresa, ora ré." (TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA, 2023). 3391

Para a juíza, ocorreu transgressão aos direitos da personalidade do autor, como sua vida íntima e sua vida privada.

> Não há dúvida que a relação entre as partes é de natureza consumerista, de sorte que um dos direitos fundamentais do consumidor é de acesso à informação adequada, acerca dos serviços que lhes são postos à disposição. Especificamente sobre o assunto referente ao tratamento de dados, a Lei nº13.709/2018 (Lei Geral de Proteção de Dados LGPD) prescreve que são fundamentos da disciplina da proteção de dados, dentre outros, o respeito à privacidade, à autodeterminação informativa, a inviolabilidade da intimidade, da honra e da imagem, a defesa do consumidor, os direitos humanos, o livre desenvolvimento da personalidade e a dignidade (art. 2º). (MODESTO apud TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA, 2023)

Como veremos na continuidade deste artigo, não se trata de um vazamento de dados comuns, mas a relevância desse caso se deu principalmente pela natura sensível dos dados indevidamente compartilhados.

3. RESPONSABILIDADE CIVIL

Com a implementação da LGPD, observa-se uma crescente judicialização de casos usando esse dispositivo por base. Conforme dados divulgados pelo Consultor Jurídico, "o

número de decisões judiciais em que dispositivos da norma foram usados de forma relevante teve um aumento de 81,4% entre 2022 e 2023" (**CONJUR**, 2023).

Entretanto, o tratamento de casos envolvendo responsabilidade de empresas por falhas de segurança na proteção de dados pessoais no judiciário brasileiro ainda está em fase de consolidação, devido a recente atuação da LGPD frente ao rápido avanço das tecnologias atuais incluindo as IAs, em 09/10/2025, ocorreu o 1° Encontro Nacional de Encarregadas e Encarregados de Dados do Poder Judiciário, de acordo com o Conselho Nacional de Justiça, as reflexões do evento foram "consolidadas na Carta de Brasília, com diretrizes e propostas para garantir a efetiva implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) no âmbito do Judiciário" (CONSELHO NACIONAL DE JUSTIÇA, 2025, Brasília.). Dentre os pontos debatidos, destaca-se a importância da contínua formação e atualização dos magistrados e servidores nos temas de proteção de dados bem como nas atuações das IAs.

Ademais, um fato que tem gerado bastante discussão é sobre a configuração do dano moral em casos de vazamento de dados, mesmo quando não há comprovação de prejuízo financeiro direto.

Segundo Tepedino (2022, n.p), a reparação do dano moral na LGPD assume características particulares, o que reforça a crítica à presunção do dano (técnica *in re ipsa*). Para o autor, não se deve exigir a comprovação da dor ou do sofrimento da vítima, mas sim a prova da lesão sofrida, tal como ocorre com a lesão patrimonial no dano material. A aplicação irrestrita de presunções no âmbito da LGPD, para ele, apenas incentiva a tarifação de indenizações.

Nesse sentido, a jurisprudência tem avançado no caminho de não reconhecer automaticamente o dano moral *in re ipsa*, que é o dano presumido decorrente do próprio fato da violação, em situações que envolvam dados comuns, entretanto, reconhecendo de logo quando se trata de dados sensíveis.

É importante ressaltar que o entendimento do judiciário sobre a responsabilidade das empresas por falhas de segurança na proteção de dados ainda está em construção. Este processo deve ser acompanhado de perto pela comunidade jurídica e pelas empresas, à medida que novos casos são julgados e a jurisprudência se consolida (CNJ, 2025).

3.1. DECISÕES JUDICIAIS RELEVANTES (STJ)

O Superior Tribunal de Justiça (STJ) continuou a emitir decisões importantes que impactam a responsabilidade civil das empresas por violação de dados, muitas vezes em conjunto com o Código de Defesa do Consumidor (CDC). Em Outubro de 2025, o STJ decidiu

que bancos e instituições de pagamento devem indenizar clientes que foram vítimas do "golpe da falsa central de atendimento" por falha na prestação de serviço, indicando que a falta de medidas de segurança adequadas para proteger informações pessoais configura um serviço defeituoso (Art. 14, §1º, CDC), o que tem forte conexão com os deveres de segurança da LGPD Art. 46 (SUPERIOR TRIBUNAL DE JUSTIÇA, 2025).

> "AÇÃO DECLARATÓRIA DE INEXIGIBILIDADE DE DÉBITO C.C. INDENIZAÇÃO POR DANOS MORAIS - Golpe da falsa central de atendimento - Autor que, após receber ligação supostamente do banco, realizou transações bancárias seguindo orientações de estelionatários - Sentença que julgou parcialmente procedentes os pedidos - Pretensão do réu de reforma - ADMISSIBILIDADE: Autor entrou em contato com os estelionatários, seguiu as instruções deles e realizou as transações bancárias mediante utilização de senha pessoal e intransferível. Ausência de falha na prestação de serviço do Banco em decorrência de fortuito externo. Colaboração involuntária da vítima. Culpa de terceiro fraudador. Nexo causal rompido. Aplicabilidade do art. 14, § 3º, II, do CDC. Sentença reformada. RECURSO PROVIDO" (e-STJ fl. 538).

O STJ tem reconhecido a responsabilidade de empresas pelo vazamento de dados pessoais sensíveis, mesmo em casos de invasão por hackers, um bom exemplo é o REsp 2.147.374-SP, que determinou a culpa da empresa Eletropaulo, por vazamento de dados de usuários em uma invasão hacker (STJ, 2024).

> RECURSO ESPECIAL. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. DIREITO À PRIVACIDADE, À LIBERDADE E À AUTODETERMINAÇÃO INFORMATIVA. AGENTE DE TRATAMENTO. VAZAMENTO DE DADOS NÃO SENSÍVEIS DO TITULAR. INCIDENTE DE SEGURANÇA. **ATAQUE HACKER**. RESPONSABILIDADE EXCLUSIVA DE TERCEIRO. NÃO COMPROVADA. RESPONSABILIDADE CIVIL PROATIVA. **EXPECTATIVA DE LEGÍTIMA PROTEÇÃO**. COMPLIANCE E REGULAÇÃO DE RISCO DA ATIVIDADE. DIREITOS DO TITULAR. CONCRETIZAÇÃO. APLICABILIDADE.
>
> [...]
>
> 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).
>
> [...]
>
> 7. Assim, correta a conclusão do TJSP de concretizar os direitos do titular ao condenar a recorrente na obrigação de apresentar informação das entidades públicas e privadas com as quais realizou o uso compartilhado dos dados da recorrida (art. 18, VII, da LGPD) e a fornecer declaração completa que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, bem como a cópia exata de todos os dados referentes ao titular constantes em seus bancos de dados (art. 19, II, da LGPD).
>
> 8. Recurso especial não provido. (REsp 2147374 / SP, RECURSO ESPECIAL 2022/0220922-8) **Grifei**

O tratamento de dados pessoais é considerado irregular quando não oferece a segurança que o titular legitimamente esperaria ("expectativa de legítima proteção"). Isso leva em conta as circunstâncias pertinentes, incluindo as técnicas de tratamento de dados pessoais que estavam disponíveis no momento em que o processamento foi realizado (Lei nº 13.709/2018, art. 44, III).

CONCLUSÃO

A presente pesquisa analisou a responsabilidade das empresas por falhas de segurança na proteção de dados pessoais a luz da LGPD. Ficou claro que a legislação atribui responsabilidades diretas aos agentes de tratamento, exigindo transparência a qualquer tempo, como a adoção de medidas de segurança mais eficazes. Haja visto, que, o descumprimento dessas obrigações pode acarretar sanções administrativas significativas e responsabilização civil por danos materiais causados e morais se houver evidências deste.

Ao longo da pesquisa ficou evidente que, a implementação da LGPD teve um impacto direto na confiança do público para com as empresas que trabalham com dados, pois a norma busca garantir que haja um bom serviço prestado por estes e punições severas caso isso não ocorra, influenciando o sucesso de negócios baseados em dados. Entretanto, falhas de segurança podem gerar perda de confiança, resultando em prejuízos financeiros e de reputação. Vimos a análise de casos reais de violações de dados, expondo as graves consequências tanto para os titulares dos dados que sofreram o dano, quanto para as empresas que foram penalizadas.

Por fim, o comportamento do judiciário sobre o tema ainda está em desenvolvimento, mas já se observa uma crescente judicialização de casos e a busca por responsabilizar os agentes de tratamento por incidentes de segurança. A consolidação da jurisprudência que será fundamental para definir os contornos da responsabilidade civil nesse contexto.

Com isso, conclui-se que os objetivos propostos foram integralmente alcançados. A natureza jurídica da responsabilidade civil é objetiva e solidária entre os agentes de tratamento. A LGPD, ao impor a obrigação de reparação por danos patrimoniais e morais e exigir a adoção de medidas técnicas e administrativas aptas a proteger os dados (Art. 46), estabelece mecanismos claros de responsabilização.

Ao passo que, o judiciário tem buscado responsabilizar os agentes por incidentes de segurança, alinhando-se aos deveres de segurança da LGPD e, em geral, exigindo a demonstração de um dano efetivo que transcenda o mero vazamento para a concessão de indenização por dano moral.

REFERÊNCIAS

AGÊNCIA SENADO. **Golpes digitais atingem 24% da população brasileira, revela DataSenado**. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. **Dispõe sobre a Proteção de Dados Pessoais**. Diário Oficial da União, Brasília-DF, 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 fev. 2025.

BRASIL. Superior Tribunal de Justiça. Titular de dados vazados deve comprovar dano efetivo ao buscar indenização, decide Segunda Turma. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/17032023-Titular-de-dados-vazados-deve-comprovar-dano-efetivo-ao-buscar-indenizacao--decide-Segunda-Turma.aspx. Acesso em: 10 abr. 2025.

CNN Brasil. **Cerca de 25% das empresas brasileiras tiveram perdas com hackers em 2022, diz pesquisa**. 10 abr. 2025. Disponível em: https://www.cnnbrasil.com.br/economia/negocios/cerca-de-25-das-empresas-brasileiras-tiveram-perdas-com-hackers-em-2022-diz-pesquisa/#:~:text=O%20levantamento%20afirma%20que%2078%25%20das%20empresas%20brasileiras,e%2023%25%20delas%20sofreram%20perdas%20financeiras%20como%20resultado. Acesso em: 10 abr. 2025.

CNN BRASIL. **Facebook é condenado a pagar R$ 20 milhões por vazamento de dados de usuários**. Disponível em: https://www.cnnbrasil.com.br/nacional/facebook-e-condenado-a-pagar-r-20-milhoes-por-vazamento-de-dados-de-usuarios/#:~:text=Facebook%20%25C3%25A9%20condenado%20a%20pagar%20R$%2020,de%20dados%20de%20usu%25C3%25A1rios%2520%257C%2520CNN%2520Brasil.&text=A%20Justi%25C3%25A7a%20de%20Minas%2520Gerais%2520condenou%25200,ocorreram%2520nos%2520anos%2520de%25202018%2520e%25202019. Acesso em: 8 abr. 2025.

CNN BRASIL. **Três anos de LGPD: mais de 600 casos já foram registrados na Agência Nacional de Proteção de Dados**. CNN Brasil, 18 set. 2023. Disponível em: https://www.dafont.com/pt/](https://www.dafont.com/pt/. Acesso em: 02 nov. 2025.

CONSELHO NACIONAL DE JUSTIÇA. **Judiciário reafirma compromisso com proteção de dados pessoais**. Brasília, DF, 09/10/2025. Disponível em: https://www.cnj.jus.br/judiciario-reafirma-compromisso-com-protecao-de-dados-pessoais/. Acesso em: 28 de out. 2025.

Consultor Jurídico. **Consumidor será indenizado por compartilhamento de dados**. Disponível em: https://www.conjur.com.br/2023-abr-21/consumidor-indenizado-compartilhamento-dados. Acesso em: 01 de abril de 2025.

DECISÕES judiciais relacionadas à LGPD cresceram 81% neste ano. Consultor Jurídico (ConJur), [S.l.], 24 dez. 2023. Disponível em: https://www.conjur.com.br/2023-dez-24/decisoes-judiciais-relacionadas-a-lgpd-crescem-81-neste-ano/. Acesso em: 28 out. 2025.

DINO. **Golpes digitais aumentaram 35% em 2023 no Brasil**. O Globo, 05 jan. 2024. Disponível em: https://oglobo.globo.com/patrocinado/dino/noticia/2024/01/05/golpes-digitais-aumentaram-35-em-2023-no-brasil.ghtml. Acesso em: 25 out. 2024.

EM.com.br. **Venda da Netshoes vai acelerar a consolidação do e-commerce**. 15 de abril de 2019. Disponível em: https://www.em.com.br/app/noticia/economia/2019/04/15/internas_economia,1046321/venda-da-netshoes-vai-acelerar-a-consolidacao-do-e-commerce.shtml. Acesso em: 10 abr. 2025.

FEBRABAN. **Brasileiro aumenta em 30% suas transações bancárias em 2022, e 8 em cada 10 operações são digitais**. Portal FEBRABAN, São Paulo, 28 jun. 2023. Disponível em: https://portal.febraban.org.br/noticia/3950/pt-br/. Acesso em: 10 abr. 2025.

GAGNO, L. N.; et al. **Efeitos da segurança e privacidade de dados na lealdade do consumidor no comércio eletrônico**. Revista de Administração da FACCAT, v. 20, n. 1, p. 1-20, 2022. Disponível em: https://www.spanishdict.com/translate/hipotética. Acesso em: 14 out. 2025.

GLOBO. **Netshoes terá de pagar R$ 500 mil por vazamento de dados de 2 milhões de clientes**. G1, Brasília, 05 fev. 2019. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2019/02/05/netshoes-tera-de-pagar-r-500-mil-por-vazamento-de-dados-de-2-milhoes-de-clientes.ghtml. Acesso em: 10 abr. 2025.

IT FORUM. **Governo Federal registra recorde de vazamentos de dados em 2024**. IT Forum, 16 set. 2024. Disponível em: https://www.dafont.com/one-1.font. Acesso em: 02 nov. 2025.

MACHADO, Felipe. **Brasil perde US$ 10 bilhões por ano com cibercrime**, diz McAfee. Veja, São Paulo, 21 fev. 2018. Disponível em: https://veja.abril.com.br/economia/brasil-perde-us-10-bilhoes-por-ano-com-cibercrime-diz-mcafee/. Acesso em: 10 abr. 2025.

MIGALHAS. **Especialista analisa principais incidentes de segurança em 2024**. Migalhas, 29 abr. 2025. Disponível em: https://www.dafont.com/pt/](https://www.dafont.com/pt/. Acesso em: 02 nov. 2025.

NETCONSULTING. **O impacto da proteção de dados nas empresas**. Disponível em: https://netconsulting.com.br/o-impacto-da-protecao-de-dados-nas-empresas/. Acesso em: 10 abr. 2025.

PORTAL DE PRIVACIDADE. **8 casos de vazamentos de dados tratados com a LGPD**. Portal de Privacidade, 03 abr. 2025. Disponível em: https://www.dafont.com/pt/](https://www.dafont.com/pt/. Acesso em: 02 nov. 2025.

AKOMOTO, Leonardo. **Ao vender nossos dados, farmácias tratam Lei Geral de Proteção como piada....** UOL Notícias. Disponível em: https://noticias.uol.com.br/colunas/leonardo-sakamoto/2023/09/01/ao-vender-nossos-dados-farmacias-tratam-lei-geral-de-protecao-como-piada.htm.

SILVA, M. M. **Modelo de comportamento do consumidor on-line de produtos e serviços turísticos via on-line travel agencies (OTAs)**. 2021. 250 f. Tese (Doutorado em Turismo) – Universidade Federal do Rio Grande do Norte, Natal, 2021

SUPERIOR TRIBUNAL DE JUSTIÇA. **Bancos e instituições de pagamento devem indenizar clientes por falhas que viabilizam golpe da falsa central**. Brasília, DF: STJ, 21 out. 2025. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2025/21102025-Bancos-e-instituicoes-de-pagamento-devem-indenizar-clientes-por-falhas-que-viabilizam-golpe-da-falsa-central.aspx. Acesso em: 1 nov. 2025.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. **Notas sobre o dano moral no direito brasileiro**. Revista Brasileira de Direito Civil – RBDCivil, Belo Horizonte, v. 30, n. 4, p. 33-60, out./dez. 2021 [publicado em 2022].

TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA. 18ª VARA DE RELAÇÕES DE CONSUMO DA COMARCA DE SALVADOR. Sentença. **Processo nº 8063270-09.2021.8.05.0001**. Salvador, 05 de abril de 2023. Disponível em: https://consultapublicapje.tjba.jus.br/pje/ConsultaPublica/DetalheProcessoConsultaPublica/listView.seam?ca=3557e47158008oa54c7f3c1d8e05a783de6416ab931336d6. Data de acesso:10 de abril de 2025.