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

doi.org/10.51891/rease.v12i5.25883

A RESPONSABILIDADE CIVIL OBJETIVA DAS PLATAFORMAS DIGITAIS POR VAZAMENTOS DE DADOS PESSOAIS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): FUNDAMENTOS, LIMITES E MEDIDAS DE SEGURANÇA DA INFORMAÇÃO

OBJECTIVE CIVIL LIABILITY OF DIGITAL PLATFORMS FOR PERSONAL DATA BREACHES IN LIGHT OF THE GENERAL DATA PROTECTION LAW (LGPD): FOUNDATIONS, LIMITS AND INFORMATION SECURITY MEASURES

RESPONSABILIDAD CIVIL OBJETIVA DE LAS PLATAFORMAS DIGITALES POR FUGAS DE DATOS PERSONALES A LA LUZ DE LA LEY GENERAL DE PROTECCIÓN DE DATOS (LGPD): FUNDAMENTOS, LÍMITES Y MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

Camilla Adriane da Silva Espinhara[1]
Larissa Rodrigues Almeida[2]
Itallo Marques Santana[3]

RESUMO: O presente artigo investiga de que maneira a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) fundamenta a responsabilidade civil objetiva das plataformas digitais em casos de vazamento de dados, bem como os limites dessa obrigação frente às exigências de segurança da informação e à atuação de terceiros. A crescente digitalização transformou o dado pessoal em um ativo de alto valor econômico, impulsionando a coleta massiva por plataformas de internet e redes sociais. Diante dos riscos inerentes, a pesquisa foi desenvolvida por meio de revisão bibliográfica qualitativa, com análise sistemática da legislação e da doutrina de Batistella (2025), Silva (2025), Fortes (2026), Constantino et al. (2025) e Carvalho Júnior e Rezende (2024). O estudo aborda a proteção de dados como um direito fundamental e uma dimensão da autodeterminação informativa. Os principais resultados indicam que o art. 42 da LGPD, conjugado com a teoria do risco-proveito (Código Civil, art. 927) e o Código de Defesa do Consumidor, consolida a responsabilidade objetiva das plataformas, dispensando a prova de culpa e exigindo apenas o nexo causal e o dano. Demonstra-se que incidentes decorrentes de ataques cibernéticos (hackers) configuram, em regra, fortuito interno, não rompendo o nexo causal quando evidenciada a negligência técnica ou a ausência do "estado da arte" em cibersegurança (arts. 46 e 47). Conclui-se que a LGPD atua como ferramenta de accountability digital, exigindo alinhamento ao Tema 1.199/DF do STJ (2025) para equilibrar a inovação tecnológica com a preservação da dignidade e da soberania informacional do titular.

Palavras-chave: LGPD. Responsabilidade civil objetiva. Plataformas digitais.

[1]Discente do curso de Direito pela Autarquia do Ensino Superior de Garanhuns (AESGA).
[2]Discente do curso de Direito pela Autarquia do Ensino Superior de Garanhuns (AESGA).
[3]Professor do curso de Direito pela Autarquia do Ensino Superior de Garanhuns (AESGA).

ABSTRACT: This article investigates how the General Personal Data Protection Law (LGPD – Law No. 13.709/2018) grounds the strict civil liability of digital platforms in cases of data breaches, as well as the limits of this obligation in the face of information security requirements and the actions of third parties. The growing digitalization has transformed personal data into a high-value economic asset, driving massive collection by internet platforms and social networks. Given the inherent risks, the research was developed through a qualitative bibliographic review, with systematic analysis of the legislation and the doctrine of Batistella (2025), Silva (2025), Fortes (2026), Constantino et al. (2025), and Carvalho Júnior and Rezende (2024). The study addresses data protection as a fundamental right and a dimension of informational self-determination. The main results indicate that Article 42 of the LGPD, combined with the risk-benefit theory (Civil Code, Article 927) and the Consumer Defense Code, consolidates the strict liability of platforms, dispensing with proof of fault and requiring only the causal nexus and damage. It is demonstrated that incidents resulting from cyberattacks (hackers) generally constitute internal fortuitous events, not breaking the causal nexus when technical negligence or the absence of the "state of the art" in cybersecurity is evidenced (Articles 46 and 47). It is concluded that the LGPD acts as a tool for digital accountability, requiring alignment with STJ Theme 1.199/DF (2025) to balance technological innovation with the preservation of the dignity and informational sovereignty of the data subject.

Keywords: LGPD. Strict civil liability. Digital platforms.

RESUMEN: El presente artículo investiga de qué manera la Ley General de Protección de Datos Personales (LGPD – Ley nº 13.709/2018) fundamenta la responsabilidad civil objetiva de las plataformas digitales en casos de fuga de datos, así como los límites de esta obligación frente a los requisitos de seguridad de la información y la actuación de terceros. La creciente digitalización ha transformado el dato personal en un activo de alto valor económico, impulsando la recolección masiva por plataformas de internet y redes sociales. Ante los riesgos inherentes, la investigación se desarrolló mediante revisión bibliográfica cualitativa, con análisis sistemático de la legislación y de la doctrina de Batistella (2025), Silva (2025), Fortes (2026), Constantino et al. (2025) y Carvalho Júnior y Rezende (2024). El estudio aborda la protección de datos como un derecho fundamental y una dimensión de la autodeterminación informativa. Los principales resultados indican que el art. 42 de la LGPD, conjugado con la teoría del riesgo-beneficio (Código Civil, art. 927) y el Código de Defensa del Consumidor, consolida la responsabilidad objetiva de las plataformas, prescindiendo de la prueba de culpa y exigiendo solo el nexo causal y el daño. Se demuestra que los incidentes derivados de ataques cibernéticos (hackers) configuran, en regla, fortuito interno, sin romper el nexo causal cuando se evidencia negligencia técnica o la ausencia del "estado del arte" en ciberseguridad (arts. 46 y 47). Se concluye que la LGPD actúa como herramienta de accountability digital, exigiendo alineamiento al Tema 1.199/DF del STJ (2025) para equilibrar la innovación tecnológica con la preservación de la dignidad y de la soberanía informacional del titular.

Palabras clave: LGPD. Responsabilidad civil objetiva. Plataformas digitales.

INTRODUÇÃO

A contemporaneidade é marcada por uma transição sem precedentes para a era digital, na qual a coleta, o armazenamento e o tratamento de dados pessoais deixaram de ser atividades acessórias para se tornarem o núcleo do modelo de negócio de plataformas de internet e redes sociais. Nesse cenário, o dado pessoal transmutou-se em um ativo de altíssimo valor econômico, o que impulsionou a vigilância e a monetização de hábitos comportamentais em escala global. No entanto, essa hiperconectividade expõe os indivíduos a riscos

multidimensionais, uma vez que a tecnologia, apesar de suas funções essenciais, atua como um potencial risco para a privacidade, exigindo transparência e regulamentação rigorosa (MINDÊLLO; LELIS, 2025).

Como resposta a essa vulnerabilidade estrutural, o Brasil promulgou a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), que estabelece diretrizes para o tratamento de informações por entidades públicas e privadas. A implementação da LGPD, contudo, enfrenta desafios significativos relacionados à cultura de proteção de dados ainda incipiente e à complexidade na fiscalização das atividades de tratamento (NASCIMENTO; BARROS; PINTO, 2024). A proteção de dados deve ser compreendida, portanto, como uma dimensão autônoma da personalidade e um direito fundamental, essencial para a preservação da dignidade humana frente ao desenvolvimento tecnológico acelerado (ALCÂNTARA, 2024).

A responsabilização civil por danos decorrentes do tratamento de dados atua como um mecanismo essencial para garantir a segurança e a transparência nas relações digitais brasileiras (SILVA, 2025). Todavia, a efetividade dessa proteção depende da compreensão da natureza jurídica da responsabilidade das plataformas, especialmente em casos de vazamentos que geram impactos patrimoniais e morais significativos (BATISTELLA, 2025). A aplicação da teoria do risco e a observância do dever de cuidado proativo tornam-se, assim, os pilares para a reparação de danos no ambiente virtual.

Diante do exposto, o presente artigo tem como objetivo geral investigar a responsabilidade civil das plataformas digitais perante a LGPD em casos de exposição indevida de informações dos usuários. Os objetivos específicos buscam: apresentar os fundamentos e princípios da LGPD; discutir a natureza da responsabilidade civil (objetiva versus subjetiva); e identificar as medidas preventivas de segurança da informação à luz dos impactos estratégicos e da consolidação jurisprudencial recente (FORTES, 2026). A relevância deste estudo sustenta-se na necessidade de harmonizar a inovação digital com a proteção dos direitos fundamentais, em conformidade com o entendimento do Superior Tribunal de Justiça (STJ), notadamente o Tema 1.199/DF (2025).

MÉTODOS

A presente pesquisa caracteriza-se como um estudo de natureza qualitativa e caráter exploratório-descritivo, desenvolvida por meio de um procedimento de revisão bibliográfica e

documental exaustiva. A metodologia foi estruturada em três eixos complementares para garantir o rigor científico e a profundidade analítica exigida pelo tema.

No primeiro eixo, realizou-se o levantamento bibliográfico em bases de dados científicas, como o Google Acadêmico e o portal da Revista REASE, priorizando produções recentes que discutem a interseção entre tecnologia e direito. O referencial teórico foi construído a partir de contribuições fundamentais, como as de Mindêllo e Lelis (2025), que analisam o direito à privacidade em redes sociais, e Alcântara (2024), que fundamenta a proteção de dados como direito fundamental. A análise da responsabilidade civil nas plataformas digitais e seus impactos estratégicos foi subsidiada pelas obras de Batistella (2025), Silva (2025) e Fortes (2026), permitindo uma visão multidisciplinar sobre os riscos inerentes ao tratamento de dados.

O segundo eixo consistiu no exame documental e normativo, tendo como núcleo central a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e o Código de Defesa do Consumidor (Lei nº 8.078/1990). Investigou-se a aplicação do art. 42 da LGPD em diálogo com os desafios e perspectivas apontados por Nascimento, Barros e Pinto (2024), focando na complexidade da fiscalização e nos gargalos culturais da proteção de dados no Brasil.

Por fim, o terceiro eixo metodológico dedicou-se à análise jurisprudencial sistemática, com ênfase nas decisões do Superior Tribunal de Justiça (STJ), especificamente o Tema Repetitivo 1.199/DF (2025), que baliza o entendimento sobre o dano moral em vazamentos de dados. A pesquisa incluiu, ainda, a análise de notas técnicas e orientações da Autoridade Nacional de Proteção de Dados (ANPD) publicadas até março de 2026. A técnica de análise adotada foi a exegese jurídica e a análise de conteúdo, o que permitiu confrontar as teorias de responsabilidade civil (objetiva versus subjetiva) com a realidade fática das plataformas digitais e as exigências contemporâneas de segurança da informação.

RESULTADOS

A investigação dos dados coletados revela que a estrutura da Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece um novo paradigma ético-jurídico no Brasil, ancorado em dez princípios fundamentais dispostos no art. 6º da Lei nº 13.709/2018. Observou-se que, no ecossistema das plataformas digitais, o tratamento de dados pessoais (art. 5º, X) constitui o núcleo da operação econômica, onde as empresas atuam predominantemente como controladoras, detendo o poder de decisão sobre os ativos informacionais, ou como operadoras.

O cerne da responsabilidade civil encontra-se no art. 42 da LGPD, que impõe ao agente que causar dano patrimonial ou moral em violação à legislação o dever inequívoco de repará-lo.

De acordo com o levantamento, a aplicação do art. 42 é frequentemente conjugada com a teoria do risco da atividade, prevista no art. 927, parágrafo único, do Código Civil, e com o art. 14 do Código de Defesa do Consumidor. A análise da jurisprudência do Superior Tribunal de Justiça (STJ), especificamente por meio do Tema 1.199/DF julgado em 2025, consolidou a diferenciação no tratamento dos danos: enquanto o vazamento de dados biográficos comuns exige a prova de prejuízo concreto para ensejar indenização, a exposição de dados sensíveis — como convicções religiosas, dados de saúde ou biometria — tem sido classificada como dano moral presumido (*in re ipsa*). Além disso, os resultados apontam que a implementação da LGPD no Brasil ainda enfrenta desafios estruturais e de fiscalização pela ANPD, conforme destacam Nascimento, Barros e Pinto (2024), refletindo uma cultura de proteção de dados ainda em estágio de maturação.

DISCUSSÃO

A proteção de dados pessoais no ordenamento jurídico brasileiro deve ser compreendida, primordialmente, como uma dimensão autônoma dos direitos da personalidade. Sob essa ótica, a simples quebra da legítima expectativa de privacidade ou o desvio das finalidades acordadas já representa uma violação direta à dignidade do titular (SILVA et al., 2025). Conforme sustentam Alcântara (2024) e Carvalho Júnior e Rezende (2024), essa autonomia do direito à proteção de dados — agora consolidada pela Emenda Constitucional nº 115/2022 — exige que o Judiciário reconheça o dano moral não apenas como uma perda financeira, mas como uma lesão à autodeterminação informativa. Diante da hiperconectividade, a violação da privacidade nas redes sociais e plataformas de *e-commerce* atua como um risco estrutural, demandando transparência e uma postura proativa dos agentes de tratamento (MINDÊLLO; LELIS, 2025).

Contudo, é imperativo ressaltar que a responsabilidade civil das plataformas digitais, embora objetiva, não possui natureza ilimitada. O sistema reparatório estruturado pelo art. 42 da LGPD pressupõe a existência de uma violação efetiva à legislação de proteção de dados para que se configure o dever de indenizar. Nesse sentido, as excludentes clássicas de responsabilidade, como o caso fortuito, a força maior ou o fato exclusivo de terceiro, permanecem como garantias de equilíbrio jurídico (art. 43, LGPD). Todavia, a aplicabilidade dessas excludentes está intrinsecamente vinculada à capacidade da plataforma de comprovar a

adoção rigorosa de medidas razoáveis e proporcionais de segurança. Como apontam Constantino et al. (2025), a "proteção real ao cidadão" depende de um judiciário que saiba distinguir a invasão inevitável da negligência operacional, combatendo a distância que muitas vezes separa a letra da lei da realidade técnica das invasões.

Os artigos 46 e 47 da LGPD estabelecem o dever de segurança como uma obrigação de meio robusta, exigindo que o controlador adote medidas técnicas e administrativas aptas a mitigar riscos. Tais medidas preventivas não são facultativas e incluem o emprego de criptografia de ponta a ponta, controles rigorosos de acesso, auditorias sistêmicas de vulnerabilidades e a implementação de planos de resposta a incidentes de segurança. A nomeação do Encarregado de Proteção de Dados (DPO), prevista no art. 41, atua como o pilar de governança dessa estrutura. Nascimento, Barros e Pinto (2024) destacam que o desafio brasileiro reside em transformar essas exigências em práticas culturais consolidadas, evitando que o *compliance* seja apenas documental. Quando as plataformas comprovam a implementação diligente e atualizada dessas salvaguardas e, ainda assim, o vazamento decorre de um ataque hacker de altíssima sofisticação (como os *Zero-Day exploits*), a jurisprudência, em linha com o Tema 1.199/DF do STJ, tem inclinação para mitigar ou excluir a responsabilidade, reconhecendo o rompimento do nexo causal pela imprevisibilidade técnica.

Todavia, a discussão sobre a atuação de terceiros criminosos ganha complexidade quando se confronta o dever de transparência. O art. 48 da LGPD impõe a comunicação obrigatória de incidentes à ANPD e aos titulares em prazo razoável. Para Fortes (2026), a gestão estratégica de um vazamento é o que define a extensão da responsabilidade civil: plataformas que agem com opacidade perante o titular agravam o dano moral, perdendo o direito de alegar o fato de terceiro como excludente, uma vez que a omissão pós-vazamento configura uma violação autônoma à boa-fé objetiva. Conclui-se, em diálogo com Carvalho Júnior e Rezende (2024), que o sistema brasileiro busca uma simbiose entre a segurança da informação e a responsabilidade civil, assegurando que o risco da tecnologia seja suportado por quem dela extrai lucro, mas preservando a viabilidade da inovação digital quando a diligência e a ética são plenamente demonstradas pelas corporações.

CONCLUSÃO

A investigação desenvolvida permite concluir que a Lei Geral de Proteção de Dados Pessoais (LGPD) fundamenta a responsabilidade civil objetiva das plataformas digitais em

episódios de vazamento de dados por meio de uma interpretação sistemática do seu art. 42. Este dispositivo, ao ser alinhado à teoria do risco da atividade prevista no Código Civil e ao sistema de proteção do Código de Defesa do Consumidor, opera a dispensa da prova de culpa, transferindo para o agente de tratamento o ônus de garantir a integridade dos ativos informacionais que explora economicamente. Como observado, os limites desse dever indenizatório não são absolutos, sendo demarcados pela observância rigorosa das medidas adequadas de segurança da informação estabelecidas nos arts. 46 e 48 da referida lei. A exequibilidade das excludentes legais, como o fato exclusivo de terceiro, condiciona-se à demonstração de que a plataforma não incorreu em negligência técnica ou omissão na custódia dos dados.

O estudo confirma que a jurisprudência do Superior Tribunal de Justiça (STJ), notadamente com a consolidação do Tema 1.199/DF em 2025, vem amadurecendo o regime de accountability no Brasil, estimulando a prevenção e a governança corporativa. Verificou-se que a figura do hacker, embora externamente criminosa, é absorvida pelo risco inerente ao negócio digital, caracterizando-se como fortuito interno sempre que houver falhas de segurança evitáveis. Segundo Constantino et al. (2025), a eficácia da proteção real ao cidadão depende de um Judiciário que reconheça a assimetria técnica entre o usuário e a plataforma, exigindo desta última o emprego do "estado da arte" em cibersegurança para que o nexo causal possa ser rompido. A análise das contribuições de Carvalho Júnior e Rezende (2024) reforça que a responsabilidade civil atua como um instrumento de pacificação social e de correção de rumos na economia digital, punindo a opacidade e recompensando a transparência proativa.

Para além da mera barreira técnica contra invasões, a responsabilização objetiva reafirma o compromisso inalienável do Estado Brasileiro com a autodeterminação informativa e a dignidade da pessoa humana. Conclui-se, em harmonia com Silva et al. (2025), que a proteção de dados pessoais transmutou-se de uma obrigação regulatória em um pilar fundamental da democracia digital. O equilíbrio entre o fomento à inovação tecnológica e a preservação da privacidade exige que as plataformas assumam o protagonismo na mitigação de danos, assegurando que o progresso da sociedade da informação não ocorra em sacrifício aos direitos fundamentais do titular. Assim, o dever de reparação por vazamentos não deve ser visto apenas como uma sanção pecuniária, mas como um mecanismo indispensável para a construção de um ambiente virtual ético, seguro e verdadeiramente centrado na proteção do indivíduo perante os riscos da hiperconectividade contemporânea.

REFERÊNCIAS

1. BATISTELLA, A. R. A responsabilidade civil pelo vazamento de dados nas plataformas digitais. *Revista de Direito Digital e Sociedade*, 2025; 12.

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

3. CARVALHO JÚNIOR, P. C. de; REZENDE, P. I. da S. Direito Digital e suas aplicações: a violação de privacidade, a proteção de dados e medidas de solução. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, v. 10, n. 11, p. 3720–3733, 2024. Disponível em: https://doi.org/10.51891/rease.v10i11.16960.

4. CONSTANTINO, E. da S.; CARVALHO, O. de S.; CONSTANTINO, E. da S.; FLORES, K. S. Entre a lei e a invasão: a LGPD e a proteção real ao cidadão. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, v. 11, n. 6, p. 3521–3533, 2025. Disponível em: https://doi.org/10.51891/rease.v11i6.19919.

5. FORTES, J. C. Responsabilidade civil por vazamento de dados: consolidação jurisprudencial e impactos estratégicos. 2026.

6. NASCIMENTO, F. F. do; BARROS, M. de L. C.; PINTO, A. de S. A proteção de dados pessoais e a LGPD no Brasil: desafios e perspectivas. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, v. 10, n. 12, p. 3679–3696, 2024. Disponível em: https://doi.org/10.51891/rease.v10i12.17628.

7. SILVA, A. L. C. Responsabilidade civil no vazamento de dados. *Revista Ibero-Americana de Humanidades, Ciências e Educação (REASE)*, 2025.

8. SUPERIOR TRIBUNAL DE JUSTIÇA. Tema 1.199/DF. Recurso Especial Repetitivo. Julgado em 2025.