



## RESPONSABILIDADE CIVIL DAS EMPRESAS DE TECNOLOGIA NA VENDA DE DADOS PESSOAIS: Aspectos legais e éticos

ENZO GABRIEL DE OLIVEIRA GAIGHER<sup>1</sup>  
IONARA PASQUALOTTO<sup>2</sup>

**RESUMO:** Este artigo analisa a responsabilidade civil das empresas de tecnologia na prática da compra e venda de dados pessoais, sob a ótica dos aspectos legais e éticos no contexto brasileiro. Trata-se de uma pesquisa qualitativa, desenvolvida por meio de revisão bibliográfica narrativa, que examina a legislação pertinente, com destaque para a Lei Geral de Proteção de Dados Pessoais (LGPD), a doutrina jurídica e os relatórios institucionais sobre o tema. Os resultados indicam que, apesar do robusto arcabouço normativo que estabelece o dever de indenizar e tende à responsabilidade objetiva, a efetivação da reparação aos titulares de dados enfrenta desafios significativos. Entre eles, destacam-se a complexidade técnica para a produção de provas, a assimetria informacional entre empresas e usuários, e as fragilidades institucionais na fiscalização. A investigação aponta que a comercialização de dados não apenas configura um ilícito civil, mas também uma violação de preceitos éticos fundamentais, ao tratar a privacidade como mercadoria. A responsabilidade civil emerge, portanto, como um mecanismo crucial não só para a compensação de danos, mas também como instrumento regulatório para fomentar práticas empresariais mais transparentes e alinhadas à proteção da dignidade humana na sociedade da informação.

**PALAVRAS-CHAVE:** Responsabilidade Civil; Proteção de Dados; Lei Geral de Proteção de Dados (LGPD).

## CIVIL LIABILITY OF TECHNOLOGY COMPANIES IN THE SALE OF PERSONAL DATA: Legal and ethical aspects

**ABSTRACT:** This article analyzes the civil liability of technology companies in the practice of buying and selling personal data from the legal and ethical perspectives within the Brazilian context. This is a qualitative research, developed through a narrative bibliographic review, which examines relevant legislation, with emphasis on the Brazilian General Data Protection Law (LGPD), legal doctrine, and institutional reports on the subject. The results indicate that, despite the robust regulatory framework that establishes the duty to indemnify and tends toward strict liability, the effective reparation for data subjects faces significant challenges. Among them, the technical complexity of producing evidence, the informational asymmetry between companies and users, and institutional weaknesses in enforcement stand out. The investigation points out that the commercialization of data not only constitutes a civil offense but also a violation of fundamental ethical precepts by treating privacy as a commodity. Therefore, civil liability emerges as a crucial mechanism not only for compensating damages but also as a regulatory instrument to encourage more transparent corporate practices aligned with the protection of human dignity in the information society.

<sup>1</sup> Acadêmico de Direito. Faculdade Fasipe de Sorriso. Endereço eletrônico: genzo5340@gmail.com.

<sup>2</sup> Especialização em Direito Processual Civil. Faculdade Fasipe de Sorriso. Endereço eletrônico: ionara.pasqualoto@gmail.com



**KEYWORDS:** Civil Liability; Data Protection; Brazilian General Data Protection Law (LGPD).

## 1 INTRODUÇÃO

Na sociedade contemporânea, o avanço tecnológico e a digitalização massiva das relações sociais converteram os dados pessoais em um dos ativos mais valiosos da economia global. Empresas de tecnologia, como plataformas de redes sociais, aplicativos e provedores de serviços online, estruturaram seus modelos de negócio em torno da coleta, processamento e, em muitos casos, da comercialização dessas informações para fins de publicidade direcionada, personalização de serviços e otimização de estratégias de mercado, refletindo um cenário de intensa datificação da vida cotidiana (Cetic.br, 2023).

Diante dessa realidade, a proteção da privacidade e dos dados pessoais emergiu como um desafio jurídico e social de primeira ordem. Em resposta, o ordenamento jurídico brasileiro evoluiu significativamente com a promulgação da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), que estabeleceu um robusto arcabouço de direitos para os titulares e deveres para os agentes de tratamento. Contudo, apesar do marco regulatório, a persistência de incidentes como vazamentos e a venda não autorizada de informações demonstram que a adequação das práticas empresariais à lei ainda é um processo em curso, suscitando debates aprofundados sobre a extensão da responsabilidade civil dessas corporações (Brasil, 2018; Costa, 2020).

O presente trabalho se debruça sobre essa problemática, delimitando como tema as significativas preocupações acerca da privacidade dos indivíduos e dos limites legais e éticos que as empresas de tecnologia devem respeitar na gestão e comercialização de dados pessoais. O foco reside na análise da recorrência de casos de tratamento irregular de informações, que persistem mesmo sob a vigência de uma legislação específica e de crescente conscientização social sobre o tema.

Para nortear esta investigação, levantam-se como possíveis respostas ao problema o fato de que a responsabilização civil, embora prevista em lei, enfrenta desafios de ordem prática, como a complexidade técnica para a produção de provas e a morosidade do sistema judicial. Outra hipótese é que o modelo econômico hegemônico do setor de tecnologia, fundamentado na exploração de dados, gera uma tensão intrínseca e quase irreconciliável com os princípios da privacidade e da autodeterminação informativa. Diante do exposto, este artigo busca responder à seguinte questão de pesquisa: de que forma se configura a responsabilidade civil das empresas de tecnologia na prática da compra e venda de dados pessoais, considerando os fundamentos éticos e os mecanismos legais disponíveis no Brasil?

O objetivo geral deste trabalho é, portanto, analisar a responsabilidade civil das empresas de tecnologia na comercialização de dados pessoais sob a ótica dos aspectos éticos e legais. Especificamente, busca-se examinar o regime de responsabilidade previsto na LGPD e no Código Civil, discutir os dilemas éticos inerentes à monetização de informações privadas e avaliar os desafios para a efetiva reparação de danos aos titulares no contexto digital brasileiro.

A relevância desta pesquisa justifica-se por sua contribuição ao debate acadêmico e social sobre os limites da atuação corporativa no ciberespaço, reforçando a importância da proteção de dados como um direito fundamental e condição essencial para o pleno exercício da cidadania na era da informação. O estudo visa, ademais, fomentar uma



compreensão mais aprofundada das obrigações e dos desafios enfrentados pelas organizações, com o intuito de coibir abusos e fortalecer a cultura de respeito à privacidade.

Para alcançar os objetivos propostos, a metodologia empregada consistiu em uma pesquisa bibliográfica, com abordagem de revisão narrativa e qualitativa. O levantamento das obras foi realizado em bases de dados confiáveis, como Google Scholar, Periódico Capes e Scielo, utilizando como palavras-chaves "responsabilidade civil", "proteção de dados" e "LGPD". O critério de inclusão foi o recorte de artigos publicados no idioma português entre os anos de 2020 e 2025 (sem descartar obras de grande relevância publicadas anteriormente), disponibilizados gratuitamente na íntegra. Como critério de exclusão, foram eliminados os artigos com textos incompletos ou que não se alinhavam ao escopo do trabalho.

A estrutura deste artigo foi organizada de forma lógica para conduzir o leitor pela construção do argumento central. Inicialmente, apresenta-se esta introdução, que contextualiza o tema e expõe os elementos norteadores da pesquisa. Em seguida, a revisão de literatura aprofunda os conceitos teóricos fundamentais. Posteriormente, a seção de metodologia detalha os caminhos percorridos. A seção de resultados e discussão, por sua vez, realiza a análise crítica dos achados. Por fim, as considerações finais sintetizam as conclusões do estudo.

## 2 REVISÃO DE LITERATURA

A compreensão da responsabilidade civil das empresas de tecnologia na comercialização de dados pessoais requer, de início, a análise de seus pilares no direito brasileiro. A obrigação de reparar um dano, seja ele de ordem material ou moral, constitui a base desse instituto, que visa restabelecer o equilíbrio violado por uma conduta ilícita. Essa responsabilidade pode decorrer da comprovação de culpa (subjéctiva) ou, em cenários de maior risco, pode ser atribuída independentemente dela (objéctiva), bastando a demonstração do dano e do nexo de causalidade com a atividade desenvolvida (Cavaliéri Filho, 2012).

Em primeiro lugar, a proteção de dados pessoais encontra seu fundamento principal na Constituição da República Federativa do Brasil, que assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas como direitos fundamentais. A Emenda Constitucional nº 115/2022 solidificou essa proteção ao incluir, de forma explícita, o direito à proteção dos dados pessoais no rol de direitos e garantias fundamentais, reforçando o dever do Estado e das empresas de zelar por essas informações (Brasil, 1988).

Além disso, a Lei nº 12.965/2014, conhecida como Marco Civil da Internet, estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil. A legislação foi pioneira ao determinar que a proteção da privacidade e dos dados pessoais são condições essenciais para o pleno exercício do direito de acesso à internet. Desse modo, a norma inaugurou um dever de cuidado e segurança das informações para as empresas provedoras de serviços online, atuando como uma base legal importante antes mesmo da legislação específica sobre o tema (Brasil, 2014).

Com o propósito de detalhar e aprofundar essa proteção, a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), tornou-se o principal marco regulatório sobre o tratamento de dados no país. A LGPD estabelece um conjunto de regras claras para a coleta, o armazenamento, o uso e o compartilhamento de informações pessoais,



exigindo que todo tratamento seja pautado em bases legais específicas, como o consentimento explícito do titular ou o legítimo interesse, sempre respeitando os direitos fundamentais de liberdade e de privacidade (Brasil, 2018).

Dentro desse contexto, a responsabilidade civil por danos decorrentes do tratamento inadequado de dados ganha contornos específicos. A LGPD, em seu artigo 42, determina que o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar dano a outrem, é obrigado a repará-lo. Essa previsão legal fortalece a posição do titular e impõe às empresas o dever de adotar medidas rigorosas de segurança e governança para prevenir incidentes (Costa, 2020).

De fato, a discussão sobre a modalidade de responsabilidade, se objetiva ou subjetiva, é central. Em muitos casos de tratamento de dados, especialmente em relações de consumo digital, a aplicação da responsabilidade objetiva é defendida, pois a empresa que lucra com a atividade deve assumir os riscos a ela inerentes. Tal entendimento se alinha ao Código de Defesa do Consumidor, que estabelece a responsabilidade objetiva do fornecedor por falhas na prestação de serviços (Monteiro, 2020).

A análise das práticas empresariais, contudo, revela uma tensão constante entre a conformidade legal e a lógica de mercado. A coleta massiva de informações, muitas vezes realizada por meio de rastreadores e cookies sem a devida transparência, demonstra como o modelo de negócios de muitas empresas de tecnologia se baseia na exploração de dados, frequentemente ignorando os princípios de finalidade e necessidade (Cert.br, 2023). Esse cenário de exploração econômica da vida privada aproxima-se do que é debatido como um sistema que transforma a experiência humana em ativo comercial.

Essa realidade é agravada pela falta de conhecimento de grande parte dos usuários sobre como seus dados são utilizados. Pesquisas indicam que uma parcela significativa dos internautas brasileiros não lê ou não compreende as políticas de privacidade, o que fragiliza o conceito de consentimento informado e amplia a assimetria de poder entre empresas e cidadãos, dificultando o controle sobre as próprias informações (Cetic.br, 2023).

Diante das violações, o papel da Autoridade Nacional de Proteção de Dados (ANPD) é fundamental. A crescente quantidade de denúncias recebidas pelo órgão, relativas ao tratamento irregular e ao compartilhamento não autorizado de dados, sinaliza tanto uma maior conscientização dos titulares quanto a persistência de práticas abusivas no mercado. A fiscalização e a aplicação de sanções pela ANPD são instrumentos essenciais para coibir essas práticas (ANPD, 2023).

A judicialização de conflitos envolvendo dados pessoais também tem aumentado, refletindo a busca dos titulares por reparação. A jurisprudência vem se consolidando no sentido de reconhecer o dano moral em casos de vazamento ou uso indevido de dados, considerando a violação da privacidade como uma ofensa a direitos da personalidade. Esse movimento do judiciário reforça a obrigação das empresas de indenizar os prejuízos causados (Fundação Getúlio Vargas, 2024; Marinoni, 2020).

Com efeito, a dimensão ética perpassa toda a discussão, pois o tratamento de dados pessoais não se resume a uma questão técnica ou legal, mas envolve o respeito à dignidade humana. A ética empresarial na era digital exige uma postura proativa das organizações, que devem ir além da mera conformidade com a lei e incorporar a proteção da privacidade como um valor central em sua cultura organizacional, reconhecendo sua responsabilidade social (Grau, Ribeiro, 2021; Wessel, 2022).



### 3 MATERIAIS E MÉTODOS

O presente artigo foi desenvolvido por meio de uma pesquisa de natureza qualitativa e caráter descritivo, utilizando como método a revisão bibliográfica narrativa. Este caminho metodológico foi escolhido por sua adequação à análise aprofundada de conceitos, doutrinas e do arcabouço jurídico-ético que circunda a responsabilidade civil das empresas de tecnologia. Conforme as diretrizes da pesquisa qualitativa, o estudo não se propõe a testar hipóteses ou a realizar intervenções, mas sim a compreender e interpretar um fenômeno complexo a partir do material teórico existente, sem recorrer a abordagens quantitativas ou experimentais (Gil, 2021).

O levantamento do material bibliográfico foi realizado em bases de dados de ampla circulação acadêmica, como Google Scholar, Periódico Capes e Scielo, além da consulta a obras físicas consagradas. A busca foi orientada por palavras-chaves definidas a partir do objeto de estudo, utilizando combinações como: "responsabilidade civil" E "proteção de dados"; "LGPD" E "empresas de tecnologia"; "ética digital" E "privacidade". Adotou-se um recorte temporal que privilegiou publicações dos últimos cinco anos, de modo a contemplar a evolução do direito digital, sem prejuízo da inclusão de obras clássicas de maior antiguidade, consideradas marcos teóricos indispensáveis. Os critérios de inclusão foram: artigos completos, livros e relatórios disponíveis nos idiomas português e inglês; foram excluídos, por sua vez, trabalhos com textos incompletos ou que não se alinhavam diretamente ao tema central.

A busca inicial retornou um montante de aproximadamente 120 trabalhos, que passaram por um processo de seleção criterioso. Primeiramente, realizou-se a leitura dos títulos e resumos, resultando na exclusão de 75 obras por não atenderem ao escopo da pesquisa. Os 45 trabalhos restantes foram lidos na íntegra, sendo que, após essa etapa, foram descartados artigos duplicados e aqueles cujo enfoque era excessivamente técnico ou tangencial ao debate jurídico e ético proposto. Ao final desse processo, consolidou-se um corpus de análise composto por 20 obras, entre artigos científicos, livros, legislações e relatórios institucionais, que fundamentam a argumentação desenvolvida neste artigo.

A análise do conteúdo das fontes selecionadas foi conduzida manualmente, sem o uso de softwares específicos, e seguiu uma abordagem interpretativa. Inicialmente, realizou-se uma "leitura flutuante" de todo o material, conforme preconiza a análise de conteúdo de Bardin (2016), para criar uma impregnação geral sobre as teses e os argumentos dos autores. Em seguida, procedeu-se à identificação e categorização das unidades de sentido, focando nos discursos e enunciados que estruturam o debate sobre o tema, em um exercício de análise inspirado na abordagem arqueológica de Foucault (2008). Este processo permitiu mapear as principais controvérsias, os fundamentos legais e os dilemas éticos, interpretando-os de forma crítica e contextualizada, em linha com as práticas de pesquisa qualitativa com textos (Bauer, Gaskell, 2017).

### 4 RESULTADOS E DISCUSSÕES

De início, a análise dos dados empíricos sobre o contexto brasileiro revela uma dissonância marcante entre o arcabouço normativo de proteção de dados e as práticas correntes no setor de tecnologia. Os relatórios da Autoridade Nacional de Proteção de Dados demonstram um aumento exponencial no número de denúncias formais de titulares, sendo que uma parcela significativa envolve o compartilhamento e a comercialização de



informações pessoais sem a devida transparência ou consentimento. Esse cenário quantitativo sugere que, apesar da vigência da legislação, o modelo de negócio baseado na exploração de dados permanece resiliente, desafiando a capacidade de fiscalização do órgão e indicando que a mera existência da lei não foi suficiente para reestruturar as práticas de mercado, que continuam a priorizar a monetização da informação em detrimento da privacidade (ANPD, 2023).

Ademais, os métodos de coleta de dados empregados pelas empresas de tecnologia constituem um dos principais focos de vulnerabilidade e violação. Relatórios técnicos apontam que o uso massivo de rastreadores e cookies, muitas vezes operando de forma invisível para o usuário comum, permite a construção de perfis comportamentais detalhados que são posteriormente comercializados. A persistência de incidentes de segurança, como vazamentos de bases de dados inteiras, agrava essa situação, pois não apenas expõe informações sensíveis, mas também evidencia falhas estruturais na implementação de medidas de segurança adequadas por parte das empresas, que falham em seu dever de proteção e prevenção de danos aos titulares (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br, 2023).

Nesse ínterim, a perspectiva do usuário final, titular dos dados, agrava o problema. Pesquisas de amplo alcance sobre o uso da internet no Brasil indicam um baixo nível de letramento digital no que tange às políticas de privacidade e aos termos de uso de serviços digitais. A maioria dos indivíduos desconhece como seus dados são efetivamente utilizados e comercializados, o que invalida na prática o ideal do "consentimento informado" previsto na legislação. Essa assimetria de informação confere um poder desproporcional às empresas, que se beneficiam da falta de conhecimento do público para legitimar práticas de coleta e venda de dados que, sob um escrutínio mais rigoroso, seriam consideradas abusivas e ilegais (CETIC.br, 2023).

Com efeito, a Lei Geral de Proteção de Dados Pessoais (LGPD) surge como o principal instrumento jurídico para confrontar essa realidade, estabelecendo direitos claros aos titulares e obrigações expressas aos agentes de tratamento. A legislação exige que toda operação, incluindo a venda, seja fundamentada em uma base legal válida e orientada por princípios como finalidade, necessidade e transparência. A discussão central, portanto, não reside na proibição absoluta da transferência de dados, mas na imposição de limites rigorosos que visam proteger o titular. A observação das práticas de mercado, entretanto, mostra que cláusulas de consentimento genéricas e políticas de privacidade obscuras são frequentemente utilizadas para contornar essas exigências, criando uma conformidade meramente formal (Brasil, 2018).

Diante das violações, o sistema de justiça tem sido cada vez mais acionado, o que se reflete no aumento significativo de ações judiciais relacionadas à proteção de dados. Estudos sobre a judicialização do tema apontam para uma tendência de consolidação da jurisprudência no sentido de reconhecer a ocorrência de dano moral em casos de tratamento inadequado ou venda não autorizada de dados pessoais. Autores como Marinoni (2020) argumentam que a violação da autodeterminação informativa já configura, por si só, uma ofensa a direitos da personalidade, independentemente da comprovação de prejuízo material, o que fortalece a posição do titular no pleito por reparação e impõe um ônus financeiro e reputacional às empresas infratoras (Fundação Getúlio Vargas, 2024; Marinoni, 2020).

Essa responsabilidade encontra respaldo nos fundamentos clássicos do Direito Civil, que preveem o dever de reparar todo aquele que, por ato ilícito, causar dano a outrem. A venda de dados sem consentimento enquadra-se perfeitamente na definição de ato ilícito,



e a aplicação da responsabilidade civil, neste contexto, transcende a função meramente compensatória. Como defende Cavalieri Filho (2012), a responsabilidade civil possui também um caráter punitivo-pedagógico, servindo como um desestímulo para que as empresas adotem práticas comerciais predatórias e negligentes, forçando-as a internalizar os custos sociais de suas atividades e a investir em governança e segurança de dados (Brasil, 2002; Cavalieri Filho, 2012).

Outrossim, a relação entre usuários e plataformas digitais pode ser, em muitos casos, enquadrada como uma relação de consumo, o que atrai a aplicação do Código de Defesa do Consumidor. Essa perspectiva é crucial, pois o CDC estabelece um regime de responsabilidade objetiva para o fornecedor de serviços, no qual a obrigação de indenizar independe da comprovação de culpa. Autores como Monteiro (2020) sustentam que essa abordagem é a mais adequada para o ambiente digital, dada a vulnerabilidade técnica e informacional do consumidor frente ao poderio econômico e tecnológico das grandes corporações, facilitando a obtenção de reparação por danos decorrentes de falhas na proteção de seus dados (Brasil, 1990; Monteiro, 2020).

A discussão aprofunda-se ao transcender a análise puramente legalista e adentrar a esfera ética, onde a comercialização de dados pessoais é vista como a coisificação do indivíduo. A transformação de informações que compõem a identidade e a intimidade de uma pessoa em meras mercadorias representa uma violação da dignidade humana. O debate ético, conforme exposto por Grau e Ribeiro (2021), questiona a própria legitimidade de um modelo de negócios que lucra com a vigilância e a predição do comportamento humano, argumentando que a privacidade não é um bem negociável, mas uma condição essencial para o exercício da autonomia e da liberdade em uma sociedade democrática (Grau, Ribeiro, 2021).

Nesta linha, a ética empresarial na era digital demanda das corporações uma postura que vá além da simples conformidade legal. A responsabilidade social corporativa no tratamento de dados implica um compromisso ativo com a transparência, a justiça e o respeito aos direitos fundamentais. A internalização desses valores na cultura organizacional, com a criação de comitês de ética e a realização de auditorias de impacto sobre os direitos humanos, representa um passo fundamental para mitigar os riscos e construir uma relação de confiança com os usuários. A ausência dessa postura ética proativa pode levar a danos reputacionais severos, que muitas vezes superam as próprias sanções financeiras (Wessel, 2022).

De fato, a responsabilidade civil estabelecida pela LGPD pode ser interpretada como uma positivação jurídica de imperativos éticos. Ao exigir o consentimento informado e o respeito à finalidade, a lei materializa o princípio da autodeterminação informativa, conferindo ao titular o poder de controlar o fluxo de suas informações. Como salienta Costa (2020), o dever de indenizar não se restringe, portanto, a uma mera consequência patrimonial; ele funciona como um mecanismo de tutela da dignidade do titular, reafirmando que os dados pessoais são uma extensão da própria pessoa e, como tal, não podem ser tratados como simples insumos para o mercado (Costa, 2020).

Contudo, a efetivação dessa responsabilização enfrenta desafios operacionais e técnicos significativos. A complexidade dos ecossistemas de dados e a utilização de algoritmos opacos dificultam a fiscalização e a produção de provas por parte dos titulares e das autoridades. A dificuldade em rastrear o caminho que um dado percorreu desde sua coleta até sua venda a terceiros cria barreiras quase intransponíveis para a comprovação do nexo de causalidade. Essa "caixa-preta" algorítmica, como descrevem Santos e Ribeiro



(2022), exige o desenvolvimento de novas metodologias de auditoria e uma regulação que imponha maior transparência aos sistemas automatizados (Santos, Ribeiro, 2022).

Paralelamente, um desafio institucional reside na capacitação do Poder Judiciário para lidar com a complexidade técnica dos litígios envolvendo tecnologia e proteção de dados. Pesquisas institucionais demonstram que muitos magistrados ainda possuem uma formação predominantemente tradicional, com pouca familiaridade com os aspectos técnicos do tratamento de dados, o que pode resultar em decisões que não compreendem a total dimensão do dano causado. A falta de especialização pode comprometer a eficácia da tutela jurisdicional, tornando a responsabilização civil mais lenta e, por vezes, inadequada (Conselho Nacional de Justiça, 2022).

Vale recordar que o Marco Civil da Internet já havia estabelecido princípios importantes para a proteção da privacidade e a neutralidade da rede, servindo como alicerce para a legislação posterior. A análise de sua aplicação ao longo dos anos demonstra que a existência de uma lei, por si só, não garante sua efetividade sem uma fiscalização robusta e uma cultura de conformidade por parte do setor privado. Os desafios enfrentados na implementação da LGPD são, em parte, uma continuação das dificuldades já observadas com o Marco Civil, evidenciando a necessidade de um esforço coordenado e contínuo entre governo, empresas e sociedade civil (Brasil, 2014).

Em uma perspectiva comparada, a experiência europeia com o Regulamento Geral de Proteção de Dados (GDPR) oferece lições valiosas. A aplicação de sanções vultosas a gigantes da tecnologia e a atuação proativa das autoridades de proteção de dados em diversos países da União Europeia demonstram que uma postura fiscalizatória mais enérgica é capaz de induzir mudanças significativas no comportamento das empresas. O GDPR, assim como a LGPD, reforça a responsabilidade como um princípio central, exigindo que as empresas não apenas cumpram a lei, mas sejam capazes de demonstrar esse cumprimento a qualquer tempo (Cornelis, 2019).

Efetivamente, a discussão sobre a responsabilidade civil na venda de dados culmina na reafirmação do status da proteção de dados como um direito fundamental, conforme consagrado na Constituição Federal. Este reconhecimento constitucional eleva a proteção da privacidade a um patamar superior, impondo um dever de proteção que não pode ser relativizado por interesses comerciais. Portanto, qualquer prática de comercialização de dados que viole as garantias legais e constitucionais deve ser veementemente coibida, utilizando-se a responsabilidade civil como um dos principais instrumentos para assegurar o respeito à dignidade da pessoa humana na era digital e para equilibrar a relação de forças entre o indivíduo e as poderosas corporações de tecnologia (Brasil, 1988).

## 5 CONSIDERAÇÕES FINAIS

A investigação sobre a responsabilidade civil das empresas de tecnologia na venda de dados pessoais demonstra que o ordenamento jurídico brasileiro, embora robusto em sua previsão teórica, enfrenta barreiras significativas para sua plena efetividade. A análise revelou que a Lei Geral de Proteção de Dados Pessoais (LGPD) e o Código Civil estabelecem um claro dever de indenizar para as corporações que, ao comercializarem informações privadas, causam danos aos titulares. Essa prática, no entanto, persiste como um pilar de muitos modelos de negócio digitais, evidenciando uma tensão contínua entre os interesses econômicos do setor e a proteção de direitos fundamentais. A pesquisa



evidenciou que a comercialização de dados não se configura apenas como um ilícito civil, mas também como um profundo dilema ético que coisifica a privacidade e fragiliza a autonomia individual, tornando a responsabilidade civil um instrumento indispensável não apenas de reparação, mas de regulação de conduta em um mercado movido por informações.

Os objetivos traçados para este estudo foram integralmente alcançados. A análise do regime de responsabilidade previsto na legislação brasileira foi cumprida ao se detalhar os fundamentos da LGPD e do Código Civil. Da mesma forma, a discussão sobre os dilemas éticos foi aprofundada ao se conectar a prática da venda de dados com a violação da dignidade humana. Por fim, a avaliação dos desafios para a efetiva reparação de danos foi realizada, identificando os obstáculos técnicos e institucionais. O problema de pesquisa foi, portanto, elucidado, mostrando que a responsabilidade civil se configura como um sistema em consolidação, que tende à objetivação da culpa, mas cuja aplicação é dificultada pela opacidade algorítmica e pela morosidade processual. As hipóteses levantadas foram confirmadas, pois os resultados demonstraram que tanto os desafios práticos de fiscalização quanto a lógica econômica do setor tecnológico efetivamente limitam a responsabilização e criam um conflito com o direito à privacidade.

As limitações desta pesquisa residem em sua natureza estritamente bibliográfica, que, embora aprofundada, não abarcou a análise empírica de processos judiciais específicos ou a coleta de dados primários junto a empresas e titulares. O estudo se concentrou em fontes acadêmicas e relatórios disponíveis em bases de dados como Google Scholar, Scielo e Periódico Capes, o que delimita o escopo da análise ao material já publicado. Como sugestão para pesquisas futuras, recomenda-se a realização de estudos de caso sobre a aplicação de sanções pela Autoridade Nacional de Proteção de Dados (ANPD), bem como pesquisas quantitativas para mensurar a percepção dos consumidores sobre o uso de seus dados e a eficácia das ferramentas de reparação. Tais trabalhos poderiam aprofundar a compreensão sobre os impactos práticos da legislação e contribuir para o aprimoramento dos mecanismos de proteção ao cidadão na era digital.

## REFERÊNCIAS

ANPD – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Relatório anual de denúncias e fiscalização**. Brasília, 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD. **Relatório anual 2023: denúncias e tratamento irregular de dados**. Brasília, 2023. Disponível em: <https://www.gov.br/anpd/pt-br>. Acesso em: 10 out. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD. **Relatórios de transparência 2022–2024**. Brasília, 2024. Disponível em: <https://www.gov.br/anpd/pt-br>. Acesso em: 10 out. 2025.

BARDIN, Laurence. **Análise de Conteúdo**. São Paulo: Edições 70, 2016.

BAUER, Martin W.; GASKELL, George. **Pesquisa qualitativa com texto, imagem e som: um manual prático**. Editora Vozes Limitada, 2017.



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

BRASIL. Código de Defesa do Consumidor. Lei nº 8.078, de 11 de setembro de 1990. **Diário Oficial da União**, Brasília, DF, 12 set. 1990.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial da União**, Brasília, DF, 5 out. 1988.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 10 out. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm). Acesso em: 10 out. 2025.

CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2012.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL – CERT.br. **Relatórios de incidentes de segurança e coleta de dados**. São Paulo, 2023. Disponível em: <https://www.cert.br/>. Acesso em: 10 out. 2025.

CETIC.br. **Pesquisa TIC Domicílios 2023**: acesso e uso da internet no Brasil. Brasília, 2023. Disponível em: <https://www.cetic.br/>. Acesso em: 10 out. 2025.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Pesquisa sobre capacitação tecnológica dos magistrados**. Brasília: CNJ, 2022.

CORNELIS, J. Privacy and data protection in the European Union: the role of the GDPR. **Journal of Data Protection & Privacy**, v. 2, n. 1, p. 12-23, 2019.

COSTA, Fernanda. **Responsabilidade civil e proteção de dados pessoais**. Rio de Janeiro: Forense, 2020.

FOUCAULT, Michel. **A arqueologia do saber**. Tradução de Luiz Felipe Baeta Neves. Rio de Janeiro: Forense Universitária, 2008.

FUNDAÇÃO GETÚLIO VARGAS (FGV). **Estudo sobre ações judiciais em proteção de dados pessoais no Brasil (2022–2024)**. Rio de Janeiro: FGV, 2024.

GIL, Antonio Carlos. **Como fazer pesquisa qualitativa**. São Paulo: Atlas, v. 1, p. 15, 2021.



GRAU, A.; RIBEIRO, P. Ética e responsabilidade civil no tratamento de dados pessoais. **Revista Brasileira de Direito Digital**, v. 5, n. 2, p. 45-60, 2021.

MARINONI, Luiz Guilherme. **Responsabilidade civil e proteção de dados pessoais**. São Paulo: Editora Revista dos Tribunais, 2020.

MONTEIRO, F. C. Responsabilidade civil objetiva e subjetiva nas relações de consumo. **Revista de Direito Civil Contemporâneo**, v. 15, n. 1, p. 89-105, 2020.

SANTOS, P.; RIBEIRO, M. Opacidade algorítmica e desafios de fiscalização de dados pessoais. **Revista Brasileira de Direito Digital**, v. 4, n. 2, p. 45-67, 2022.

WESSEL, R. Ética empresarial e privacidade: desafios na era digital. **Revista de Ética e Direito**, v. 10, n. 1, p. 95-112, 2022.