Revista Multidisciplinar do Nordeste Mineiro, v.11, 2025
ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4095

A RESPONSABILIDADE CIVIL DAS EMPRESAS DE TECNOLOGIA NO TRATAMENTO DE DADOS DO CONSUMIDOR NA ERA DIGITAL

THE CIVIL LIABILITY OF TECHNOLOGY COMPANIES IN THE PROCESSING OF CONSUMER DATA IN THE DIGITAL AGE

Pâmella Silva Rosa
Graduanda em Direito, Faculdade de Ensino Superior de Linhares, Brasil
E-mail: pamellarosa81@gmail.com
Alexandre Jacob
Mestre, Faculdade de Ensino Superior de Linhares, Brasil
E-mail: alexandre.jacob10@gmail.com

Recebido: 01/06/2025 – Aceito: 15/06/2025

Resumo:

O presente artigo analisa a responsabilidade civil das empresas de tecnologia no tratamento de dados pessoais de consumidores, considerando os desafios jurídicos e sociais da era digital. A crescente coleta e uso de informações por plataformas digitais impõe novas obrigações às empresas, especialmente no que se refere à proteção da privacidade e à prevenção de danos. A partir do marco legal estabelecido pela Lei Geral de Proteção de Dados Pessoais, discute-se o regime de responsabilidade aplicável, a exigência de segurança no tratamento de dados e os impactos do descumprimento dessas normas. O estudo também aborda o caso emblemático do vazamento de dados do Facebook em 2018, como exemplo das consequências da negligência no manuseio de informações pessoais. Conclui que a responsabilidade civil exerce papel fundamental na proteção do consumidor e na consolidação de práticas éticas e legais no ambiente digital.

Palavras-chave: Direito civil. Responsabilidade civil. Proteção de dados. Empresas de tecnologia. Consumidor digital.

Abstract:

This paper analyzes the civil liability of technology companies in the processing of personal data of consumers, considering the legal and social challenges of the digital age. The increasing collection and use of information by digital platforms imposes new obligations on companies, particularly regarding privacy protection and damage prevention. Based on the legal framework established by the General Data Protection Law, the study discusses the applicable liability regime, the security

requirements in data processing, and the impacts of non-compliance with these regulations. The paper also examines the emblematic case of the Facebook data breach in 2018 as an example of the consequences of negligence in handling personal information. It concludes that civil liability plays a key role in consumer protection and in the consolidation of ethical and legal practices in the digital environment.

***Keywords**: Civil Law. Civil liability. Data protection. Technology companies. Digital consumer.*

1. Introdução

O avanço das tecnologias digitais tem gerado profundas transformações nas relações de consumo e na maneira como as empresas coletam, armazenam e utilizam os dados pessoais dos consumidores. Nesse contexto, as empresas de tecnologia assumem um papel central na sociedade moderna, sendo responsáveis por grandes volumes de informações pessoais que são constantemente processadas e analisadas. No entanto, essa crescente dependência dos dados pessoais também levanta sérias questões jurídicas e éticas sobre a proteção da privacidade e a responsabilidade civil das empresas que lidam com essas informações.

Com a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) em 2018, o Brasil estabeleceu um marco regulatório para o tratamento de dados, impondo novas obrigações às empresas e criando um ambiente mais seguro para o consumidor digital. Nesse sentido, surge a necessidade de compreender os limites e as consequências da responsabilidade civil das empresas de tecnologia no tratamento de dados pessoais, especialmente no caso de violações que possam causar danos aos consumidores.

Este artigo se propõe a analisar a responsabilidade civil das empresas de tecnologia no tratamento de dados pessoais, com um enfoque específico no caso do vazamento de dados do Facebook® em 2018, que afetou milhões de usuários em todo o mundo. Este episódio, que envolveu o uso indevido de dados pessoais para manipulação de informações eleitorais, exemplifica os riscos e as consequências que podem surgir quando as empresas falham em garantir a segurança e a confidencialidade dos dados de seus usuários. A partir dessa análise, será possível discutir as implicações legais e sociais da violação da

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4095

privacidade, o papel da LGPD na proteção dos consumidores e a necessidade de responsabilização das empresas pela má gestão de dados pessoais.

2. Aumento do Consumo por Meio Digital

A ascensão das plataformas digitais enquanto mediadoras do consumo representa um fenômeno que transcende fronteiras geográficas e culturais. Impulsionado pela expansão da internet e pela evolução das Tecnologias da Informação e Comunicação (TICs), o consumo online passou a ocupar posição central nas relações econômicas contemporâneas. Essa reconfiguração atinge não apenas o comércio varejista, mas também serviços como transporte, alimentação, entretenimento e educação.

O conceito de consumo digital envolve a aquisição de bens e serviços por meios eletrônicos, em plataformas como e-commerces, aplicativos de delivery, serviços de assinatura e marketplaces. Segundo a imprensa, o comércio eletrônico brasileiro cresceu cerca de 24% no último ano, evidenciando uma aceleração iniciada durante a pandemia de Covid-19 e consolidada posteriormente (Nakamura, 2024).

Este processo tem sido marcado por três características principais: conveniência, acessibilidade e personalização. As plataformas digitais proporcionam uma experiência de consumo contínua, sem barreiras de tempo ou espaço, além de permitir que algoritmos identifiquem padrões de comportamento e ofereçam produtos direcionados aos interesses individuais de cada usuário (Kotler *et al*., 2021).

O consumidor digital difere substancialmente daquele observado em períodos anteriores. Ele é mais conectado, informado e exigente. A presença massiva nas redes sociais cria um ambiente onde opiniões e experiências de consumo são amplamente compartilhadas e valorizadas. Estudos indicam que mais de 80% dos consumidores verificam avaliações on-line antes de efetuar uma compra (Machado *et al*., 2019).

Além disso, os sistemas de recomendação baseados em inteligência artificial atuam como agentes de influência, sugerindo produtos com base em

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4095

comportamentos anteriores, localização e preferências de navegação (Sustein, 2021). Isso gera uma relação cada vez mais simbiótica entre consumidor e plataforma.

A transformação digital impôs às empresas uma revisão de suas estratégias comerciais. O investimento em marketing digital, análise de big data, experiência do usuário (UX) e canais omnichannel tornou-se fundamental para manter a competitividade em um ambiente cada vez mais dinâmico.

As startups de tecnologia, por sua vez, impulsionaram inovações disruptivas, como os sistemas de pagamento instantâneo (PIX), carteiras digitais e automação logística, que aceleraram ainda mais a digitalização do consumo (Schwab, 2016).

Apesar dos avanços, é necessário refletir sobre os impactos sociais e ambientais dessa nova forma de consumo. O aumento da coleta de dados pessoais levanta preocupações sobre privacidade e segurança cibernética. Ademais, a cultura do consumo rápido e a dependência dos sistemas logísticos têm gerado um aumento significativo na emissão de carbono e na geração de resíduos (Zuboff, 2019). Nesse contexto, torna-se essencial promover uma economia digital sustentável, que equilibre inovação com responsabilidade socioambiental.

O consumo mediado por plataformas digitais representa um fenômeno em expansão, cujas implicações ultrapassam a esfera econômica, alcançando dimensões sociais, culturais e ambientais. A tendência é que, com o avanço da inteligência artificial, realidade aumentada e tecnologias imersivas, o consumo digital se torne ainda mais integrado à vida cotidiana. Cabe à academia, ao setor produtivo e ao Estado refletirem conjuntamente sobre como orientar esse processo para que seja inclusivo, ético e sustentável.

3. LGPD e o Tratamento de Dados dos Consumidores

Com a crescente digitalização da sociedade, os dados pessoais tornaram-se recursos estratégicos nas mãos de grandes empresas de tecnologia. Como observa Zuboff (2019, p. 14), “os dados pessoais são a matéria-prima da nova

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4095

lógica do capitalismo de vigilância", sendo constantemente explorados para finalidades comerciais e políticas. Diante disso, a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil em 2018 representa um marco jurídico na defesa dos direitos do consumidor digital.

Inspirada na *General Data Protection Regulation* (GDPR) da União Europeia, a LGPD regulamenta o tratamento de dados pessoais com foco na proteção da privacidade e no fortalecimento do controle do cidadão sobre suas informações (Doneda, 2021). Este artigo discute como as grandes empresas de tecnologia estão se adaptando a esse novo cenário normativo e quais são os principais desafios envolvidos.

A LGPD define dado pessoal como "informação relacionada a pessoa natural identificada ou identificável" (Brasil, 2018). O tratamento desses dados deve observar princípios como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança e prevenção.

Doneda (2021, p. 6) afirma que "a LGPD representa não apenas uma tentativa de regulamentar o uso de dados, mas também de equilibrar os interesses econômicos com os direitos fundamentais do cidadão". O consentimento é um dos pilares centrais da norma, sendo exigido de forma livre, informada e inequívoca, salvo nas hipóteses legais de dispensa.

Adicionalmente, as organizações devem indicar um Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer – DPO), responsável por assegurar a conformidade com a legislação e intermediar o contato com a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares.

Empresas como Google®, Meta (Facebook®), Amazon® e Apple® detêm vastos volumes de dados pessoais e operam sistemas altamente sofisticados de coleta e análise. Esses dados são utilizados para personalizar experiências, direcionar publicidade e prever comportamentos, o que confere grande poder econômico e político a essas plataformas.

Segundo Zuboff (2019, p. 23), "essas empresas não apenas monitoram os comportamentos dos usuários, mas os moldam de maneira imperceptível para maximizar engajamento e lucro". Isso evidencia uma assimetria informacional

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4095

preocupante, pois os consumidores nem sempre têm plena consciência do que está sendo coletado e como será utilizado.

Embora a LGPD exija transparência e consentimento, a implementação prática dessas exigências é desafiadora. Muitas plataformas utilizam políticas de privacidade extensas e complexas, que dificultam a compreensão por parte dos usuários comuns (Mendes, 2022).

A adequação à LGPD implica investimentos significativos em tecnologia, treinamento e revisão de processos. Conforme Mendes (2022), “grande parte das empresas ainda encontra dificuldades em cumprir integralmente os requisitos da LGPD, especialmente quanto à governança de dados e ao tratamento automatizado de informações”.

Outro obstáculo é a atuação das empresas estrangeiras com sede fora do Brasil, o que complica a aplicação extraterritorial da legislação nacional. A ANPD possui o desafio de fiscalizar esses agentes e impor sanções quando necessário, mas enfrenta limitações de recursos e estrutura.

Além disso, é importante destacar que o consentimento, embora central, nem sempre é suficiente. Como ressalta Doneda (2021, p. 10), “o consentimento não pode ser visto como uma autorização absoluta para uso indiscriminado dos dados; deve haver limites, mesmo quando o titular concorda com o tratamento”.

A LGPD oferece uma estrutura importante para a proteção de dados no Brasil, especialmente no que diz respeito às práticas das grandes empresas de tecnologia. No entanto, para que seus objetivos sejam plenamente alcançados, é necessário promover uma cultura de proteção de dados que vá além da simples conformidade legal.

A atuação conjunta da ANPD, do setor privado e da sociedade civil é essencial para garantir a efetividade dos direitos do consumidor digital. Como conclui Zuboff (2019, p. 52), “a batalha pela privacidade é, no fundo, uma batalha pelo futuro da democracia”.

4. Estudo de Caso: Vazamento de Dados dos Consumidores pelo Facebook® em 2018

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4095

O escândalo do vazamento de dados do Facebook®, revelado em 2018, envolveu o uso indevido de informações de milhões de usuários pela empresa Cambridge Analytica, o que resultou em uma crise global de confiança nas plataformas digitais.

O avanço das tecnologias digitais e a popularização das redes sociais transformaram os dados pessoais em recursos estratégicos para empresas de tecnologia. No entanto, essa lógica de monetização da informação também trouxe riscos substanciais à privacidade dos usuários. Em 2018, veio à tona o caso envolvendo o vazamento de dados de aproximadamente 87 milhões de usuários do Facebook para a empresa britânica Cambridge Analytica, sem o devido consentimento dos titulares (Cadwalladr; Graham-Harrison, 2018).

Esse evento teve ampla repercussão internacional e expôs as fragilidades na governança de dados pessoais por parte de grandes corporações digitais. O episódio motivou debates sobre o papel das plataformas na proteção dos direitos dos usuários e impulsionou iniciativas legislativas em diversos países, com destaque para a *General Data Protection Regulation* (GDPR) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil.

O incidente teve como ponto central o uso do aplicativo *This Is Your Digital Life*, criado por Aleksandr Kogan, um acadêmico vinculado à Universidade de Cambridge. O aplicativo oferecia testes de personalidade, coletando informações pessoais não apenas dos usuários que o acessavam, mas também de seus contatos no Facebook, devido a permissões excessivas concedidas pela API da plataforma na época.

Segundo Cadwalladr e Graham-Harrison (2018), esses dados foram então compartilhados com a Cambridge Analytica, que os utilizou para construir perfis psicográficos detalhados. O objetivo era influenciar o comportamento político de eleitores por meio de publicidade altamente segmentada. A empresa atuou em campanhas como o referendo do Brexit e a eleição presidencial dos Estados Unidos em 2016, levantando questionamentos sobre manipulação da opinião pública.

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4095

Zuboff (2019, p. 137) destaca que “o caso mostrou como a extração de dados pessoais pode ser convertida em instrumentos de poder político e controle comportamental, comprometendo a autonomia dos cidadãos”.

Após a revelação do escândalo, o Facebook enfrentou uma série de audiências públicas e investigações regulatórias. O CEO da empresa, Mark Zuckerberg, foi chamado a depor no Congresso dos Estados Unidos e no Parlamento Europeu. Como consequência, a *Federal Trade Commission* (FTC) dos EUA impôs uma multa de US$ 5 bilhões à empresa em 2019 por violações de privacidade (Machado *et al*., 2019).

Além das sanções legais, o episódio resultou em uma crise reputacional. Movimentos como #DeleteFacebook ganharam força, e diversos usuários passaram a questionar os termos de uso e a transparência das redes sociais. Como observa Mendes (2022, p. 34), “o escândalo de 2018 marcou a transição da preocupação com privacidade como questão técnica para um debate público e político de escala global”.

O caso catalisou a adoção de leis mais rígidas sobre proteção de dados. A GDPR, implementada na União Europeia em maio de 2018, foi uma das primeiras a estabelecer regras claras sobre consentimento, portabilidade e exclusão de dados pessoais. No Brasil, a LGPD foi sancionada no mesmo ano, entrando em vigor em 2020. Ambas buscam assegurar os direitos dos titulares e responsabilizar controladores e operadores de dados (Brasil, 2018).

Doneda (2021, p. 8) afirma que “o episódio envolvendo o Facebook® e a Cambridge Analytica serviu de alerta para governos e cidadãos sobre a necessidade de um marco legal robusto que regulamente o uso de dados pessoais em ambientes digitais”.

Apesar disso, os desafios de implementação são significativos, especialmente no tocante à fiscalização das plataformas transnacionais e à educação digital dos usuários.

O vazamento de dados em 2018 revelou a vulnerabilidade dos sistemas de proteção de dados e a assimetria entre plataformas digitais e usuários. O caso representou um divisor de águas para a regulação do setor e contribuiu para uma maior conscientização sobre a importância da privacidade na era digital.

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4095

Ainda que avanços tenham sido conquistados no campo normativo, como a LGPD e a GDPR, persistem desafios relacionados à responsabilização efetiva das *big techs* e à transparência das práticas de coleta e uso de dados. O fortalecimento das autoridades reguladoras, o desenvolvimento de mecanismos de governança digital e a promoção da cidadania digital são passos essenciais para consolidar os direitos fundamentais no ambiente virtual.

5. Responsabilidade Civil por Tratamento Indevido de Dados de Consumidores

O avanço da tecnologia e a digitalização das relações de consumo ampliaram significativamente a coleta e o tratamento de dados pessoais pelos fornecedores. Neste contexto, o dado se tornou um ativo econômico de alto valor, mas também um elemento sensível da esfera privada do indivíduo. A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), em 2018, representou um marco regulatório ao estabelecer regras claras sobre o uso e a proteção das informações pessoais.

Com a entrada em vigor da LGPD, surge a necessidade de discutir os contornos da responsabilidade civil das empresas pelo uso indevido de dados de consumidores. A proteção da privacidade passou a ser considerada um direito fundamental, e a sua violação, passível de reparação. Como salienta Doneda (2021, p. 6), "a LGPD não apenas regula o uso de dados, mas reconhece sua íntima conexão com os direitos da personalidade".

A responsabilidade civil é o dever de reparar os danos causados a outrem por ato ilícito, nos termos do artigo 927 do Código Civil (Brasil, 2002). Em se tratando de dados pessoais, a LGPD estabelece, no artigo 42, que o controlador ou operador que causar dano patrimonial, moral, individual ou coletivo em razão de tratamento de dados em desconformidade com a legislação responderá pelos danos causados.

A responsabilidade prevista na LGPD tem natureza objetiva, ou seja, independe da comprovação de culpa do agente. Segundo Tartuce (2022), “trata-

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4095

se de uma responsabilidade de risco, típica das relações de consumo e das atividades que envolvem tratamento massivo de informações pessoais".

Além disso, o artigo 6º da LGPD estabelece princípios como a finalidade, adequação, necessidade, transparência, segurança e prevenção, que devem orientar toda atividade de tratamento de dados. O descumprimento desses princípios pode ensejar responsabilização civil, administrativa e, em alguns casos, até penal.

No âmbito das relações de consumo, o consumidor é considerado parte vulnerável, o que impõe ao fornecedor deveres acrescidos de cuidado e lealdade. Conforme o artigo 14 do Código de Defesa do Consumidor (CDC), o fornecedor responde objetivamente pela reparação de danos causados por defeitos na prestação do serviço (Brasil, 1990).

Ao tratar dados pessoais do consumidor, o fornecedor deve observar o princípio da boa-fé objetiva, que exige conduta ética, leal e transparente. Para Doneda (2021), a confiança é o elemento central da relação digital, e a violação dessa confiança, como ocorre em casos de vazamentos ou uso indevido de dados, compromete a integridade da relação de consumo.

Além disso, a proteção da privacidade é corolário do princípio da dignidade da pessoa humana, fundamento do Estado Democrático de Direito, previsto no artigo 1º, inciso III, da Constituição da República de 1988. Como observa Alexandre de Moraes (2020, p. 118), "a violação da privacidade não é apenas uma infração contratual, mas uma lesão aos direitos fundamentais do indivíduo".

A violação indevida de dados pode gerar tanto danos patrimoniais (fraudes, prejuízos financeiros, uso indevido de identidade) quanto danos morais, decorrentes do abalo à imagem, à honra ou à privacidade do titular.

Os tribunais brasileiros vêm reconhecendo, de forma crescente, a ocorrência de dano moral presumido em casos de exposição indevida de dados. Como afirma Dias (2022, p. 89), "não se exige a comprovação do sofrimento ou angústia, pois a própria divulgação indevida de dados sensíveis configura lesão moral".

Adicionalmente, o artigo 45 da LGPD assegura ao titular dos dados o direito à reparação integral, o que inclui não apenas a indenização, mas também

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4095

medidas corretivas como retratação, exclusão de dados ou comunicação aos afetados.

A responsabilidade civil por tratamento indevido de dados de consumidores representa uma importante ferramenta de proteção da privacidade na sociedade da informação. A LGPD veio consolidar direitos já previstos no Código Civil e no CDC, adaptando-os à nova realidade digital.

A partir de uma visão constitucionalizada do direito civil, a proteção de dados se insere no conjunto dos direitos da personalidade, sendo passível de tutela mesmo sem a ocorrência de dano material concreto. O desafio atual reside na aplicação efetiva da legislação e no fortalecimento de mecanismos de fiscalização e controle.

Dessa forma, o respeito à privacidade e à autodeterminação informativa deve ser um dos pilares da atuação empresarial no século XXI, em consonância com a boa-fé, a ética e a responsabilidade social.

A responsabilidade civil é o dever de reparar danos causados a outrem por ato ilícito, conforme disposto no Código Civil brasileiro. A LGPD, em seu artigo 42, estabelece que o controlador ou operador que causar dano patrimonial, moral, individual ou coletivo em razão de tratamento de dados pessoais em desconformidade com a legislação responderá pelos danos causados. A responsabilidade prevista na LGPD é objetiva, ou seja, independe da comprovação de culpa, bastando a demonstração do dano e do nexo causal.

No entanto, a aplicação da responsabilidade objetiva da LGPD tem sido objeto de debate. Alguns especialistas defendem que a responsabilidade deve ser subjetiva, exigindo a comprovação de culpa, dolo ou negligência. Embora a LGPD estabeleça a responsabilidade objetiva, a jurisprudência tem exigido a comprovação efetiva de danos para a configuração de responsabilidade civil. Em decisão recente, o Superior Tribunal de Justiça (STJ) entendeu que o vazamento de dados pessoais comuns não configura, por si só, dano moral, sendo necessária a comprovação de efetivo prejuízo (AREsp 2.130.619). O ministro Francisco Falcão, relator do recurso, destacou que "os dados pessoais vazados foram aqueles que o consumidor usualmente fornece em qualquer tipo de cadastro, sendo, portanto, considerados dados simples" (STJ, 2023).

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4095

Essa posição reflete a necessidade de equilibrar a proteção da privacidade com a prevenção de litígios infundados. No entanto, há divergências quanto à aplicação desse entendimento a dados sensíveis, que possuem maior potencial de causar danos à honra e à imagem do titular.

A LGPD prevê a possibilidade de responsabilidade solidária entre os agentes de tratamento de dados, ou seja, controlador e operador podem ser responsabilizados conjuntamente pelos danos causados. O artigo 45 da LGPD estabelece que as disposições sobre responsabilidade civil não excluem a aplicação de outras normas que tratam de reparação de danos, como o Código de Defesa do Consumidor (CDC). Isso significa que, em relações de consumo, a responsabilidade objetiva do CDC pode ser aplicada cumulativamente com a LGPD, facilitando a reparação de danos sem necessidade de comprovar culpa.

Além disso, a responsabilidade solidária pode ser estendida à cadeia produtiva, abrangendo fornecedores, prestadores de serviços e outros envolvidos no tratamento de dados. Essa abordagem amplia a proteção ao titular dos dados e incentiva a adoção de boas práticas por todas as partes envolvidas no tratamento.

A jurisprudência tem evoluído no sentido de exigir a comprovação efetiva de danos para a configuração de responsabilidade civil. Em decisão recente, o STJ reafirmou que o mero vazamento de dados pessoais comuns não configura dano moral, sendo necessária a demonstração de efetivo prejuízo (STJ, 2025). Essa decisão reforça a necessidade de comprovação de danos e estabelece um precedente importante para casos futuros.

No entanto, a jurisprudência também tem reconhecido a responsabilidade civil em casos de vazamento de dados sensíveis, mesmo na ausência de comprovação de danos materiais ou psicológicos. Em decisão envolvendo uma seguradora, o STJ entendeu que a exposição indevida de dados sensíveis compromete a privacidade e a segurança dos titulares, dispensando a comprovação de danos concretos (STJ, 2025).

A responsabilidade civil pelo tratamento indevido de dados de consumidores é um tema complexo que envolve aspectos legais, tecnológicos e éticos. A LGPD estabelece um regime de responsabilidade objetiva, mas a

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4095

jurisprudência tem exigido a comprovação efetiva de danos para a configuração de responsabilidade civil. A aplicação da responsabilidade solidária e a possibilidade de cumulação com outras normas, como o CDC, ampliam a proteção ao titular dos dados e incentivam a adoção de boas práticas pelas empresas.

É fundamental que as empresas adotem medidas eficazes de segurança da informação e promovam a conscientização sobre a importância da proteção de dados pessoais. Além disso, é necessário que o legislador e o judiciário busquem soluções que equilibrem a proteção da privacidade com a prevenção de litígios infundados, garantindo segurança jurídica e efetiva reparação dos danos.

6. Conclusão

A responsabilidade civil das empresas de tecnologia no tratamento de dados do consumidor na era digital assume uma relevância cada vez maior diante da centralidade dos dados pessoais como recurso estratégico e elemento sensível da esfera privada dos indivíduos. A transformação das relações sociais e econômicas pelo uso intensivo de tecnologias digitais ampliou exponencialmente a coleta, o armazenamento e a análise de informações, exigindo uma postura ética e legalmente responsável por parte das corporações.

O caso emblemático do vazamento de dados do Facebook® em 2018, envolvendo o uso indevido de informações de cerca de 87 milhões de usuários pela empresa Cambridge Analytica, ilustra de forma contundente os riscos decorrentes da ausência de transparência e do tratamento negligente de dados. Esse episódio demonstrou como o mau uso de informações pessoais pode comprometer não apenas a privacidade dos titulares, mas também influenciar processos democráticos e gerar danos de natureza coletiva e difusa. Como destaca Zuboff (2019), “a coleta invisível e não autorizada de dados constitui uma forma de controle que ameaça os fundamentos da autonomia individual”.

Nesse contexto, a responsabilidade civil das empresas deve ser entendida não apenas como um mecanismo de compensação por danos causados, mas também como um instrumento de prevenção, dissuasão e incentivo à

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4095

conformidade. A Lei Geral de Proteção de Dados Pessoais (LGPD), ao prever a responsabilização objetiva dos agentes de tratamento e estabelecer princípios como segurança, boa-fé e prevenção, impõe às empresas de tecnologia o dever de adotar medidas técnicas e organizacionais que assegurem o respeito aos direitos fundamentais dos consumidores.

Dessa forma, a responsabilização civil das empresas tecnológicas na era digital representa uma ferramenta indispensável para o fortalecimento da confiança nas relações digitais, para a defesa da privacidade e para a construção de uma sociedade mais justa e informacionalmente segura. A experiência de 2018 não pode ser vista como um caso isolado, mas como um alerta global sobre os perigos do descuido com os dados e a urgente necessidade de um compromisso corporativo com a ética da informação.

7. Referências

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília-DF: Senado, 1988. Disponível em: https://tinyurl.com/29ucwd3a. Acesso em: 18 abr. 2025.

BRASIL. **Lei nº. 8.078 de 11 de setembro de 1990**. Dispõe sobre a proteção ao consumidor e dá outras providências. Brasília-DF: Senado, 1990. Disponível em: https://tinyurl.com/3wkfbddx. Acesso em: 18 abr. 2025.

BRASIL. **Lei nº. 10.406 de 10 de janeiro de 2002**. Institui o Código Civil. Brasília-DF: Senado, 2002. Disponível em: https://tinyurl.com/2pmcas6z. Acesso em: 30 abr. 2025.

BRASIL. **Lei nº. 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília-DF: Senado, 2018. Disponível em: https://tinyurl.com/mtcea948. Acesso em: 22 abr. 2025.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. ***The Guardian***, 17 mar. 2018. Disponível em: https://tinyurl.com/3xacxekw. Acesso em: 22 abr. 2025.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados. *In*: DONEDA, Danilo *et al*. (Org.). **Comentários à lei geral de proteção de dados pessoais**. São Paulo: Revista dos Tribunais, 2021.

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4095

DIAS, M. T. Dano moral nas relações digitais: fundamentos e jurisprudência atual. **Revista de Direito do Consumidor**, v. 134, n. 4, 2022.

KOTLER, P. *et al*. **Marketing 5.0**: tecnologia para a humanidade. São Paulo: Alta Books, 2021.

MACHADO, Rodrigo; KREUTZ, Diego; PAZ, Giulliano; RODRIGUES, Gustavo. Vazamento de dados: histórico, impacto socioeconômico e as novas leis de proteção de dados. **Anais do XVII ERRC**, Porto Alegre, 2019.

MENDES, L. A. C. A proteção de dados pessoais e os desafios da regulação das plataformas digitais. **Revista de Direito, Estado e Internet**, v. 12, n. 1, 2022.

MORAES, Alexandre**. Direitos fundamentais e proteção da privacidade**. São Paulo: Atlas, 2020.

NAKAMURA, João. Menor que o do México, e-commerce do Brasil tem potencial para crescer, diz relatório. **CNN Brasil Negócios**, 21 out. 2024. Disponível em: https://tinyurl.com/3jpree2h. Acesso em: 18 abr. 2025.

SCHWAB, Klaus. **A quarta revolução industrial**. São Paulo: Edipro, 2016.

STJ. Superior Tribunal de Justiça. **Agravo em Recurso Especial nº. 2.130.619-SP**. Segunda Turma. Relator: Ministro Francisco Falcão, Brasília-DF: DJe, 10 mar. 2023.

STJ. Superior Tribunal de Justiça. **Recurso Especial nº. 2.121.904-SP**. Terceira Turma. Relatora: Ministra Nancy Andrighi, Brasília-DF: DJe, 17 fev. 2025.

SUNSTEIN, Cass. R. **Comportamento e nudge**: como tomamos decisões. Rio de Janeiro: Intrínseca, 2021.

TARTUCE, Flávio. **Manual de direito civil**: volume único. 9. ed. São Paulo: Método, 2022.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2019.