Proteção estatal dos dados pessoais e responsabilidade civil dos provedores na era digital

Edmur Campos Barretto[1]

Recebido em: 06/ julho/2026

Aprovado em: 11/agosto/2026

Resumo: O presente estudo aborda os desafios da proteção de dados pessoais e da responsabilidade civil dos provedores de internet no contexto da sociedade da informação e da crescente atuação de plataformas digitais estrangeiras. O objetivo da pesquisa consiste em analisar os principais obstáculos enfrentados pelo ordenamento jurídico brasileiro para assegurar a efetiva proteção dos dados pessoais, a responsabilização dos provedores e o cumprimento de decisões judiciais no ambiente digital. Para o desenvolvimento do trabalho, adotou-se metodologia de natureza bibliográfica e documental, fundamentada na análise da legislação vigente, especialmente a Lei Geral de Proteção de Dados Pessoais e o Marco Civil da Internet, bem como em doutrinas, artigos científicos e jurisprudências relacionadas ao tema. Os resultados evidenciaram que, apesar dos avanços legislativos observados nos últimos anos, persistem desafios relacionados à efetividade da proteção de dados, à prevenção de incidentes de segurança, à atuação transnacional das plataformas digitais e à execução de decisões judiciais. Conclui-se que a proteção dos direitos fundamentais no ambiente digital depende do fortalecimento da governança digital, da cooperação jurídica internacional, da atuação dos órgãos fiscalizadores e da constante atualização dos mecanismos jurídicos diante da evolução tecnológica.

Palavras-chave: proteção de dados pessoais. responsabilidade civil digital. provedores de internet. crimes cibernéticos. Lei Geral de Proteção de Dados Pessoais (LGPD).

State protection of personal data and civil liability of service providers in the digital age

Abstract: This study addresses the challenges related to personal data protection and the civil liability of internet service providers within the context of the information society and the growing presence of foreign digital platforms. The objective of the research is to analyze the main obstacles faced by the Brazilian legal system in ensuring the effective protection of personal data, the accountability of service providers, and the enforcement of judicial decisions in the digital environment. The study adopted a

[1] Graduando no curso de Direito da Faculdade Minas Gerais (FAMIG).

bibliographic and documentary research methodology, based on the analysis of current legislation, especially the General Data Protection Law (LGPD) and the Brazilian Civil Rights Framework for the Internet (Marco Civil da Internet), as well as legal doctrines, scientific articles, and judicial decisions related to the subject. The results showed that, despite the legislative advances achieved in recent years, significant challenges remain regarding the effectiveness of data protection, the prevention of security incidents, the transnational operation of digital platforms, and the enforcement of court decisions. It is concluded that the protection of fundamental rights in the digital environment depends on strengthening digital governance, international legal cooperation, the performance of regulatory authorities, and the continuous updating of legal mechanisms in response to technological developments.

Keywords: personal data protection. digital civil liability. internet service providers. cybercrime. General Personal Data Protection Law (LGPD).

1 INTRODUÇÃO

O avanço das tecnologias digitais provocou profundas transformações nas relações sociais, econômicas e jurídicas da sociedade contemporânea. A ampliação do acesso à internet, o crescimento das plataformas digitais e a intensa circulação de informações em ambiente virtual passaram a influenciar diretamente a forma como indivíduos, empresas e instituições se relacionam.

Nesse contexto, a utilização massiva de dados por plataformas digitais e sistemas automatizados intensificou debates acerca da tutela dos direitos fundamentais no ambiente virtual. A crescente exposição de informações pessoais, associada à expansão das relações digitais, ampliou os riscos relacionados ao uso inadequado de dados e fortaleceu discussões envolvendo a responsabilidade civil das empresas que atuam na internet.

Contudo, o crescimento da circulação de conteúdos digitais e o desenvolvimento de novas tecnologias passaram a exigir maior atuação do ordenamento jurídico na proteção dos usuários do ambiente virtual. Questões relacionadas ao vazamento de dados pessoais, à disseminação de informações falsas e à utilização indevida de conteúdos digitais demonstram a necessidade de mecanismos jurídicos mais eficientes para assegurar proteção aos direitos fundamentais na sociedade da informação.

Diante dessa realidade, a proteção de dados pessoais consolidou-se como importante instrumento de garantia da dignidade da pessoa humana, da liberdade e da autodeterminação informativa dos indivíduos. Nesse sentido, a promulgação da Lei Geral de Proteção de Dados Pessoais representou significativo avanço no ordenamento jurídico brasileiro ao estabelecer princípios, direitos e deveres relacionados ao tratamento de dados pessoais por agentes públicos e privados.

Da mesma forma, o Marco Civil da Internet passou a disciplinar direitos, garantias e deveres relacionados ao uso da internet no Brasil, estabelecendo parâmetros relevantes para a responsabilização civil dos provedores de aplicações e para a preservação da liberdade de expressão no ambiente digital.

Entretanto, apesar dos avanços legislativos observados nos últimos anos, ainda persistem dificuldades relacionadas à efetividade das normas jurídicas destinadas à proteção de dados pessoais e à responsabilização civil digital.

Diante da situação citada, questiona-se até que ponto o ordenamento jurídico brasileiro é capaz de garantir efetiva proteção de dados pessoais e responsabilização civil das plataformas digitais frente às constantes transformações tecnológicas.

A velocidade das transformações tecnológicas, a atuação transnacional das plataformas digitais e a crescente circulação internacional de informações demonstram que os desafios do direito digital ultrapassam os limites territoriais tradicionais, exigindo constante atualização dos mecanismos jurídicos voltados à proteção dos usuários da internet.

Dessa forma, o presente trabalho tem como objetivo analisar os principais desafios relacionados à proteção de dados pessoais e à responsabilidade civil das plataformas digitais no ordenamento jurídico brasileiro, examinando os mecanismos legais existentes, suas limitações práticas e os impactos decorrentes das transformações tecnológicas contemporâneas.

O referencial teórico da pesquisa está fundamentado principalmente nas contribuições de Patrícia Peck Pinheiro (2021), Tarcísio Teixeira (2021), Bruno Bioni

(2020), Viviane Maldonado e Rodrigo Opice Blum (2021), Rodrigo Pironti (2021) e Carlos Affonso Pereira de Souza e Ronaldo Lemos (2017). Os autores oferecem importantes contribuições para a compreensão da proteção de dados pessoais, da responsabilidade civil digital, da governança informacional, da aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) e do Marco Civil da Internet, bem como dos desafios jurídicos decorrentes da atuação das plataformas digitais, da circulação de informações no ambiente virtual e da efetividade das decisões judiciais no contexto digital.

Para o desenvolvimento da pesquisa, adotou-se metodologia de natureza bibliográfica e documental, mediante análise da legislação pertinente, especialmente a Constituição Federal de 1988, o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais, além de doutrinas, artigos científicos e jurisprudências relacionadas ao direito digital, à proteção de dados pessoais e à responsabilidade civil no ambiente virtual, buscando compreender os principais desafios jurídicos decorrentes da sociedade da informação e das relações digitais contemporâneas.

2 MARCOS LEGAIS PARA PROTEÇÃO DE DADOS

O cenário contemporâneo da proteção de dados pessoais é marcado pela existência de interesses jurídicos, econômicos e sociais que frequentemente entram em conflito. De um lado, encontra-se a necessidade de preservação da privacidade e dos direitos fundamentais dos titulares de dados; de outro, estão presentes interesses relacionados à segurança pública, ao desenvolvimento econômico, à atividade empresarial e à utilização estratégica das informações no ambiente digital. Nesse contexto, a proteção de dados passou a ocupar posição central no debate jurídico contemporâneo, especialmente diante da expansão das plataformas digitais e da intensificação da circulação de informações pessoais na sociedade da informação.

A proteção de dados pessoais foi reconhecida como direito fundamental autônomo no ordenamento jurídico brasileiro por meio da Emenda Constitucional nº 115/2022, que inseriu expressamente a proteção de dados no art. 5º da Constituição

Federal. Além disso, a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) estabeleceu normas específicas para disciplinar o tratamento de dados

pessoais realizado por pessoas físicas e jurídicas, garantindo maior segurança jurídica aos titulares das informações. O art. 6º da LGPD determina que o tratamento de dados deve observar princípios como finalidade, adequação, necessidade, livre acesso, transparência, segurança e responsabilização (Brasil, 2018).

Segundo Patrícia Peck Pinheiro (2021), a crescente utilização de tecnologias digitais ampliou significativamente os riscos relacionados ao tratamento inadequado de dados pessoais, especialmente em razão da elevada capacidade tecnológica das organizações responsáveis pela coleta, armazenamento e compartilhamento de informações. A autora destaca que, na sociedade contemporânea, os usuários frequentemente desconhecem a dimensão da utilização de seus dados, situação que evidencia uma considerável desigualdade informacional entre titulares e agentes de tratamento.

Nesse sentido, Viviane Maldonado (2021) afirma que a proteção de dados pessoais não pode ser compreendida apenas sob uma perspectiva individualista, pois os impactos decorrentes do uso inadequado das informações atingem também interesses coletivos e sociais. Para a autora, a proteção de dados deve ser analisada de maneira estrutural e institucional, considerando a necessidade de criação de mecanismos regulatórios capazes de equilibrar as relações entre usuários, empresas e Estado no ambiente digital.

Além disso, Tarcísio Teixeira (2021) ressalta que o direito à autodeterminação informativa garante ao titular dos dados a possibilidade de controlar a coleta, utilização, armazenamento e compartilhamento de suas informações pessoais. O autor destaca que a ausência de transparência sobre o tratamento de dados compromete a efetividade da proteção jurídica da privacidade e limita o exercício dos direitos fundamentais dos usuários no ambiente virtual.

A proteção de dados pessoais também está diretamente relacionada ao princípio da dignidade da pessoa humana, previsto no art. 1º, inciso III, da Constituição Federal de 1988. Conforme explica Rodrigo Pironti (2021), a tutela das informações pessoais representa importante mecanismo de preservação da liberdade, autonomia e privacidade dos indivíduos diante do avanço das tecnologias digitais e da crescente

exploração econômica dos dados pessoais. Nesse contexto, a proteção jurídica dos dados pessoais ultrapassa a noção tradicional de privacidade, assumindo papel fundamental na defesa dos direitos da personalidade e na preservação da dignidade humana.

Do mesmo modo, Márcio Cots e Ricardo Oliveira (2021) destacam que o desenvolvimento das tecnologias de informação e o crescimento do tratamento automatizado de dados tornaram indispensável a criação de mecanismos legais voltados à proteção dos titulares de dados pessoais. Segundo os autores, a LGPD representa importante instrumento de responsabilização dos agentes de tratamento, estabelecendo deveres relacionados à transparência, segurança da informação e prevenção de danos decorrentes do uso indevido das informações pessoais.

Portanto, a proteção de dados pessoais constitui um dos principais desafios jurídicos da sociedade contemporânea, exigindo constante atualização legislativa e

interpretação doutrinária capaz de acompanhar a evolução tecnológica. A consolidação da proteção de dados como direito fundamental demonstra a necessidade de harmonização entre inovação tecnológica, desenvolvimento econômico e preservação dos direitos fundamentais dos cidadãos no ambiente digital.

A primeira geração das normas relacionadas à proteção de dados pessoais surgiu na década de 1970, em um contexto marcado pelo crescimento da informatização estatal e pela preocupação com o armazenamento automatizado de informações pessoais em grandes bancos de dados públicos. Nesse período, destacam-se legislações pioneiras como o Privacy Act dos Estados Unidos, de 1974, criado para regulamentar a coleta, manutenção, uso e compartilhamento de dados pessoais por órgãos governamentais federais. A referida legislação buscou limitar a atuação estatal no tratamento de informações pessoais, assegurando aos cidadãos maior controle sobre os dados armazenados pela administração pública (Teixeira, 2021).

No cenário europeu, também se destacaram importantes iniciativas legislativas voltadas à proteção da privacidade informacional, como a Lei de Proteção de Dados do Estado de Hesse, na Alemanha, promulgada em 1970, considerada uma das primeiras

legislações específicas sobre proteção de dados no mundo. Essas normas iniciais concentravam-se principalmente na regulamentação de bancos de dados públicos e na limitação do uso indiscriminado de informações pessoais por parte do Estado (Teixeira, 2021).

Posteriormente, a evolução tecnológica e o crescimento da circulação de dados pessoais levaram ao desenvolvimento de novas diretrizes internacionais voltadas à proteção da privacidade e da autodeterminação informativa. Nesse contexto, destacam-se as Diretrizes da Organização para Cooperação e Desenvolvimento Econômico (OCDE), publicadas em 1980, que estabeleceram princípios fundamentais para o tratamento de dados pessoais, como limitação da coleta, qualidade dos dados, especificação da finalidade, segurança da informação e transparência. Essas diretrizes influenciaram significativamente a construção das legislações modernas de proteção de dados em diversos países (Teixeira, 2021).

Segundo Tarcísio Teixeira (2021), a evolução histórica da proteção de dados demonstra a transição de um modelo focado apenas no controle estatal das informações para um sistema jurídico mais amplo, voltado à tutela dos direitos fundamentais dos titulares de dados pessoais. Para o autor, o avanço das tecnologias digitais e o crescimento do tratamento automatizado de informações tornaram necessária a criação de mecanismos legais mais rigorosos para garantir segurança, transparência e responsabilização no tratamento de dados pessoais.

Em seguida, a terceira geração das normas de proteção de dados passou a reconhecer o direito à autodeterminação informativa, garantindo ao indivíduo maior participação e controle sobre o tratamento de suas informações pessoais. Esse modelo buscou fortalecer os direitos dos titulares de dados, assegurando mecanismos relacionados ao consentimento, acesso, correção e exclusão de informações pessoais. Segundo Patrícia Peck Pinheiro (2021), a autodeterminação informativa representa a capacidade conferida ao titular de decidir sobre a coleta, utilização e compartilhamento de seus dados, fortalecendo a proteção da privacidade e da liberdade individual no ambiente digital.

Posteriormente, a quarta geração da proteção de dados foi marcada pela criação de legislações mais técnicas, abrangentes e rigorosas, voltadas à redução das desigualdades existentes entre titulares de dados e grandes organizações públicas e privadas responsáveis pelo tratamento das informações. Nesse contexto, as normas passaram a estabelecer deveres específicos relacionados à transparência, segurança da informação, prevenção de danos e responsabilização dos agentes de tratamento. Conforme explica Viviane Maldonado (2021), essa nova fase da proteção de dados busca assegurar maior efetividade na tutela dos direitos fundamentais diante da crescente utilização de tecnologias digitais e sistemas automatizados de tratamento de informações pessoais.

No cenário internacional, destaca-se o Regulamento Geral sobre a Proteção de Dados da União Europeia (General Data Protection Regulation – GDPR), aprovado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho da União Europeia, em 27 de abril de 2016, entrando em vigor em 25 de maio de 2018. O GDPR tornou-se referência mundial em proteção de dados pessoais ao estabelecer regras rigorosas sobre coleta, armazenamento, compartilhamento e tratamento de informações pessoais, além de prever sanções severas para casos de descumprimento das normas. Segundo Tarcísio Teixeira (2021), o GDPR influenciou diretamente diversas legislações nacionais, inclusive a Lei Geral de Proteção de Dados brasileira, consolidando um modelo regulatório baseado na proteção dos direitos fundamentais dos titulares de dados.

No Brasil, esse movimento legislativo resultou na criação da Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), que entrou em vigor em setembro de 2020. A LGPD representa importante marco regulatório no ordenamento jurídico brasileiro ao disciplinar o tratamento de dados pessoais realizado por pessoas físicas e jurídicas, de direito público e privado. A legislação estabelece regras relacionadas à coleta, utilização, armazenamento, compartilhamento e eliminação de dados pessoais, buscando garantir maior proteção aos titulares das informações.

Os princípios que orientam o tratamento de dados pessoais estão previstos no art. 6º da LGPD, destacando-se os princípios da finalidade, adequação, necessidade, livre

acesso, transparência, segurança, prevenção, não discriminação e responsabilização (Brasil, 2018). Segundo Márcio Cots e Ricardo Oliveira (2021), tais princípios funcionam como diretrizes fundamentais para limitar a atuação dos agentes de tratamento e garantir que o uso das informações pessoais ocorra de maneira ética, legítima e proporcional. Para os autores, a efetividade da proteção de dados depende não apenas da previsão legal desses princípios, mas também de sua implementação prática pelas organizações responsáveis pelo tratamento das informações.

Além disso, a LGPD estabelece, em seu art. 7º, as bases legais que autorizam o tratamento de dados pessoais, sendo o consentimento uma das principais hipóteses previstas na legislação (Brasil, 2018). O consentimento é definido no art. 5º, inciso XII, da LGPD como manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Conforme explica Rodrigo Pironti (2021), o consentimento válido exige que o titular tenha pleno conhecimento sobre quais dados serão coletados, para quais finalidades serão utilizados e quais consequências poderão decorrer desse tratamento.

Entretanto, a obtenção de consentimento válido no ambiente digital representa um dos principais desafios da proteção de dados contemporânea. Segundo Patrícia Peck Pinheiro (2021), muitas plataformas digitais utilizam termos extensos, linguagem excessivamente técnica e mecanismos de aceite automatizado, dificultando a compreensão efetiva dos usuários acerca do tratamento de suas informações pessoais. Dessa forma, embora o consentimento seja um importante instrumento jurídico de proteção dos titulares de dados, sua efetividade depende da existência de transparência, acessibilidade e equilíbrio informacional entre usuários e agentes de tratamento.

Os Termos de Uso e as Políticas de Privacidade, responsáveis por regulamentar as relações jurídicas entre usuários e plataformas digitais, frequentemente são elaborados com linguagem excessivamente técnica, extensa e de difícil compreensão para o cidadão comum. Essa situação compromete a efetiva compreensão acerca do tratamento de dados pessoais realizado pelas empresas, dificultando o exercício consciente da autodeterminação informativa pelos titulares dos dados.

A Lei Geral de Proteção de Dados estabelece, em seu art. 5º, inciso XII, que o consentimento corresponde à manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para finalidade determinada (Brasil, 2018). Além disso, o art. 8º da LGPD determina que o consentimento deve ser fornecido por escrito ou por outro meio capaz de demonstrar a manifestação de vontade do titular, devendo as cláusulas relacionadas ao tratamento de dados estar destacadas das demais cláusulas contratuais (Brasil, 2018).

Segundo Patrícia Peck Pinheiro (2021), embora o consentimento represente importante mecanismo de proteção jurídica dos titulares de dados, sua validade depende da existência de transparência e clareza na comunicação das informações fornecidas pelas plataformas digitais. Para a autora, o aceite automático de termos extensos e complexos compromete a efetiva compreensão dos usuários acerca do tratamento de seus dados pessoais, reduzindo a transparência e dificultando o exercício da autodeterminação informativa.

Além disso, a Lei Geral de Proteção de Dados estabelece sanções administrativas aplicáveis aos agentes de tratamento que realizarem o uso inadequado de dados pessoais ou descumprirem as normas previstas na legislação. O art. 52 da LGPD prevê penalidades como advertência, multa simples, multa diária, publicização da infração, bloqueio dos dados pessoais e eliminação dos dados relacionados à infração (Brasil, 2018). Segundo Rodrigo Pironti (2021), essas sanções possuem caráter preventivo e pedagógico, buscando incentivar a adoção de medidas de conformidade e segurança pelas organizações responsáveis pelo tratamento de dados pessoais.

Entretanto, a efetividade dessas penalidades depende diretamente da atuação contínua da Autoridade Nacional de Proteção de Dados, órgão responsável pela fiscalização e regulamentação da aplicação da LGPD no Brasil (Brasil, 2021). Conforme destaca Viviane Maldonado (2021), a proteção de dados pessoais não depende apenas da existência de normas legais, mas também da criação de mecanismos eficientes de fiscalização, responsabilização e promoção da cultura de proteção de dados no ambiente institucional e empresarial.

Assim, legislações como o Regulamento Geral sobre a Proteção de Dados da União Europeia e a Lei Geral de Proteção de Dados Pessoais brasileira – LGPD (Lei nº 13.709/2018) representam importantes respostas jurídicas às transformações tecnológicas e sociais ocorridas nas últimas décadas. Essas normas foram desenvolvidas com o objetivo de regulamentar o tratamento de dados pessoais, estabelecer direitos aos titulares das informações e impor deveres de transparência, segurança e responsabilização aos agentes de tratamento.

Contudo, os desafios contemporâneos ultrapassam a simples criação de normas, envolvendo também dificuldades relacionadas à atuação das grandes empresas de tecnologia, à circulação internacional de informações e à elevada concentração de dados pessoais por plataformas digitais de alcance global.

Nesse contexto, Patrícia Peck Pinheiro (2021) ressalta que a globalização dos fluxos informacionais e a expansão das atividades econômicas digitais exigem constante atualização dos mecanismos jurídicos de proteção de dados, especialmente diante do crescimento das tecnologias de monitoramento, inteligência artificial e tratamento automatizado de informações pessoais.

Portanto, conclui-se que a proteção de dados pessoais vai além de sua mera formalização legislativa, exigindo constante evolução normativa, fiscalização efetiva e fortalecimento de uma cultura jurídica voltada à preservação dos direitos fundamentais no ambiente digital. A efetividade da proteção de dados depende da atuação conjunta do Estado, das organizações privadas e da própria sociedade na promoção de práticas responsáveis, transparentes e compatíveis com os princípios estabelecidos pela legislação brasileira.

2.1 Lacunas e desafios na aplicação da legislação vigente

Nesse cenário, destaca-se uma crítica significativa à eficácia da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), principalmente no que diz respeito à sua natureza majoritariamente reativa. Apesar de a legislação definir orientações importantes para o manuseio de dados pessoais, nota-se que sua ação é mais eficaz na responsabilização após ocorrências de violações do que na

prevenção de eventos problemáticos, evidenciando, assim, limitações práticas em sua implementação.

A investigação de casos específicos corrobora essa ideia. As ocorrências de vazamentos de dados em grande volume mostram que, mesmo após a implementação da LGPD, ainda existem deficiências na segurança da informação que persistem. Nesse contexto, Aragão (2022) destaca que os episódios relacionados a empresas privadas revelam a continuidade de fragilidades sistêmicas, ameaçando a proteção adequada dos dados pessoais.

Ademais, ocorrências envolvendo bancos de dados públicos demonstram que as vulnerabilidades relacionadas à proteção das informações pessoais não se restringem ao setor privado. No Brasil, diversos incidentes de segurança revelaram falhas no armazenamento e tratamento de dados realizados por órgãos governamentais, evidenciando a necessidade de fortalecimento das medidas de segurança da informação também na administração pública.

Nesse contexto, destaca-se o caso envolvendo o Ministério da Saúde, no qual dados pessoais de milhões de brasileiros cadastrados no Sistema Único de Saúde (SUS) ficaram expostos em razão de falhas de segurança em sistemas governamentais. A Autoridade Nacional de Proteção de Dados informou que realizou procedimentos de apuração relacionados ao vazamento de dados de aproximadamente 223 milhões de cidadãos brasileiros, situação que demonstrou a dimensão dos riscos associados ao tratamento inadequado de informações pessoais no ambiente digital (Brasil, 2021).

Segundo Rodrigo Pironti (2021), incidentes de segurança envolvendo dados pessoais evidenciam que a efetividade da proteção de dados depende não apenas da existência de legislação específica, mas também da implementação concreta de políticas de governança, fiscalização contínua e mecanismos técnicos de segurança da informação. Para o autor, a crescente circulação de dados no ambiente digital exige atuação preventiva tanto do setor privado quanto da administração pública, especialmente diante dos riscos decorrentes de falhas estruturais nos sistemas de armazenamento e compartilhamento de informações pessoais.

Nesse contexto, parte da doutrina sustenta que a Lei Geral de Proteção de Dados possui forte caráter repressivo, concentrando-se na responsabilização dos agentes de tratamento após a ocorrência de incidentes envolvendo dados pessoais. Segundo Patrícia Peck Pinheiro (2021), a efetividade da LGPD depende não apenas da previsão de sanções legais, mas também da adoção de práticas preventivas, programas de conformidade e desenvolvimento de uma cultura organizacional voltada à segurança da informação e à proteção dos dados pessoais.

Entretanto, existem posicionamentos doutrinários divergentes acerca da natureza predominantemente punitiva da LGPD. Para Viviane Maldonado e Rodrigo Opice Blum (2021), a legislação brasileira apresenta importante caráter preventivo ao estabelecer princípios, deveres de governança, medidas de segurança da informação e mecanismos de responsabilização capazes de incentivar a prevenção de danos antes mesmo da ocorrência de incidentes de segurança. Os autores destacam que dispositivos como os arts. 6º, 46 e 50 da LGPD impõem aos agentes de tratamento a obrigação de adotar medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados, vazamentos e situações acidentais ou ilícitas de destruição, perda e alteração de informações (Brasil, 2018).

Além disso, Tarcísio Teixeira (2021) ressalta que a LGPD não deve ser interpretada exclusivamente sob uma perspectiva sancionatória, pois a legislação também busca promover boas práticas de governança corporativa e estimular a adoção de mecanismos preventivos pelas organizações públicas e privadas. Segundo o autor, a prevenção constitui elemento central da proteção de dados contemporânea, especialmente diante da crescente complexidade das relações digitais e da intensificação do tratamento automatizado de informações pessoais.

Nesse sentido, a proteção efetiva dos dados pessoais exige não apenas atualização legislativa, mas também fortalecimento institucional, fiscalização contínua e implementação concreta de práticas preventivas de segurança da informação compatíveis com os princípios e deveres estabelecidos pela LGPD. Nesse contexto, destaca-se que a principal falha na implementação da Lei nº 13.709/2018 (Brasil, 2018) está na sua efetividade limitada em termos de prevenção, uma vez que sua abordagem

continua sendo maioritariamente reativa, focando na responsabilização após as violações ocorrerem. Essa situação ressalta a urgência de fortalecer os mecanismos de prevenção, governança e segurança da informação, visando aumentar a eficácia na proteção de dados pessoais e garantir a realização dos direitos fundamentais dos titulares.

3 RESPONSABILIDADE CIVIL DOS PROVEDORES DE INTERNET

A responsabilidade civil dos provedores de internet constitui tema de grande relevância no âmbito do direito digital contemporâneo, especialmente diante da intensificação do fluxo de informações no ambiente virtual e dos riscos decorrentes da utilização inadequada das plataformas digitais. A definição dos limites da responsabilidade dos provedores tornou-se essencial para equilibrar a liberdade de expressão, a proteção dos dados pessoais, a privacidade e a tutela dos direitos fundamentais dos usuários da internet.

Nesse contexto, Patrícia Peck Pinheiro (2021) destaca que o crescimento das plataformas digitais e da circulação de informações no ambiente virtual ampliou significativamente os desafios relacionados à responsabilização dos provedores por danos causados a terceiros. Segundo a autora, o desenvolvimento tecnológico exige constante adaptação do ordenamento jurídico para garantir equilíbrio entre inovação, liberdade de comunicação e proteção dos direitos fundamentais dos usuários.

Em entendimento convergente, Tarcísio Teixeira (2021) afirma que a responsabilidade civil dos provedores de internet deve ser analisada à luz dos princípios constitucionais da dignidade da pessoa humana, liberdade de expressão, privacidade e proteção de dados pessoais. Para o autor, a complexidade das relações digitais exige mecanismos jurídicos capazes de responsabilizar condutas ilícitas sem comprometer o funcionamento das plataformas digitais e o livre fluxo de informações no ambiente virtual. No sistema jurídico brasileiro, a principal legislação que regula a internet é o Marco Civil da Internet, que define princípios, direitos, garantias e responsabilidades relacionados ao uso da rede no Brasil.

A norma estabelece, em regra, a responsabilidade civil subjetiva dos provedores de aplicações de internet, vinculando sua responsabilização ao descumprimento de ordem judicial específica para remoção de conteúdos considerados ilícitos. O art. 19 do Marco Civil da Internet (Lei nº 12.965/2014) dispõe que o provedor de aplicações somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros caso, após ordem judicial específica, não tome as providências necessárias para tornar indisponível o conteúdo apontado como infringente (Brasil, 2014).

Segundo Patrícia Peck Pinheiro (2021), o art. 19 do Marco Civil da Internet buscou estabelecer equilíbrio entre a proteção da liberdade de expressão e a responsabilização das plataformas digitais, evitando a remoção indiscriminada de conteúdo sem apreciação judicial prévia. Para a autora, a exigência de ordem judicial representa importante mecanismo de preservação da segurança jurídica nas relações digitais. Nesse contexto, como ressaltam Carlos Affonso Pereira de Souza e Ronaldo Lemos (2017), a estrutura do Marco Civil inibe a censura antecipada ao evitar a atribuição de responsabilidade de maneira automática por conteúdos gerados por terceiros, protegendo assim a liberdade de expressão e garantindo um espaço digital acessível.

Contudo, essa limitação da responsabilidade civil dos provedores também gera críticas relevantes no âmbito jurídico. A exigência de ordem judicial específica para remoção de conteúdos ilícitos pode retardar a exclusão de publicações ofensivas, prolongando danos à honra, à imagem, à privacidade e aos direitos da personalidade dos usuários da internet. Em muitos casos, a demora na retirada do conteúdo permite ampla disseminação das informações ilícitas, comprometendo a efetividade da tutela jurisdicional e a proteção dos direitos fundamentais no ambiente digital.

Segundo Patrícia Peck Pinheiro (2021), embora o art. 19 do Marco Civil da Internet tenha sido criado para preservar a liberdade de expressão e evitar censura privada pelas plataformas digitais, o modelo também apresenta dificuldades práticas relacionadas à rápida contenção de danos decorrentes de conteúdos ilícitos divulgados na internet. Para a autora, a velocidade de propagação das informações no ambiente

virtual exige mecanismos jurídicos capazes de conciliar segurança jurídica, proteção da dignidade humana e efetividade na remoção de conteúdos manifestamente ilegais.

Em entendimento convergente, Guilherme Martins e João Victor Longhi (2021) destacam que a demora na remoção de conteúdos ofensivos pode comprometer a efetividade da proteção constitucional da honra, imagem, privacidade e proteção de dados pessoais, especialmente diante do elevado potencial de compartilhamento das plataformas digitais contemporâneas. Os autores ressaltam que o modelo de responsabilização previsto no Marco Civil da Internet ainda enfrenta desafios relacionados à rapidez das medidas de proteção e à dimensão global da circulação de informações no ambiente virtual.

Por outro lado, Souza e Lemos (2017) sustentam que a exigência de ordem judicial específica prevista no art. 19 do Marco Civil da Internet constitui importante mecanismo de proteção da liberdade de expressão e da segurança jurídica. Segundo os autores, a responsabilização automática dos provedores por conteúdos gerados por terceiros poderia incentivar a remoção excessiva de conteúdos pelas plataformas digitais, favorecendo práticas de censura privada e restringindo indevidamente a livre circulação de informações no ambiente digital.

Assim a responsabilidade civil dos provedores de internet exige constante equilíbrio entre proteção dos direitos fundamentais, liberdade de expressão e efetividade das medidas de remoção de conteúdos ilícitos, tema que permanece em intenso debate doutrinário e jurisprudencial no direito digital contemporâneo.

Ademais, a complexidade das plataformas digitais intensifica o debate acerca da atuação preventiva dos provedores de aplicações de internet e dos limites de sua responsabilidade civil. O crescimento das redes sociais, mecanismos de recomendação automatizada e sistemas de impulsionamento de conteúdo ampliou significativamente o poder dessas plataformas sobre a circulação de informações no ambiente virtual, tornando mais relevante a discussão sobre seus deveres de monitoramento, prevenção e remoção de conteúdos ilícitos.

Segundo Patrícia Peck Pinheiro (2021), as plataformas digitais não atuam apenas como intermediárias neutras na circulação de informações, mas também exercem influência direta na organização, moderação e disseminação de conteúdos por meio de algoritmos, políticas internas e sistemas automatizados de recomendação. Para a autora, essa atuação pode justificar ampliação dos deveres de cuidado dos provedores, especialmente em situações relacionadas à omissão diante de conteúdos manifestamente ilícitos, falhas de segurança da informação ou vazamentos de dados pessoais.

No ordenamento jurídico brasileiro, a responsabilidade civil dos provedores de internet encontra fundamento principalmente nos arts. 18, 19 e 21 do Marco Civil da Internet (Lei nº 12.965/2014). O art. 18 estabelece que os provedores de conexão não serão responsabilizados civilmente por danos decorrentes de conteúdo gerado por terceiros (Brasil, 2014). Já o art. 19 prevê que os provedores de aplicações de internet poderão ser responsabilizados civilmente caso, após ordem judicial específica, não removam conteúdo ilícito apontado como infringente (Brasil, 2014). Além disso, o art. 21 prevê hipótese excepcional de responsabilização mediante simples notificação extrajudicial nos casos de divulgação não autorizada de imagens, vídeos ou materiais íntimos de caráter privado (Brasil, 2014).

Nesse contexto, a responsabilidade civil dos provedores pode ocorrer em diferentes situações jurídicas. Entre elas, destacam-se: omissão na remoção de conteúdos ilícitos após ordem judicial; falhas na proteção de dados pessoais; vazamento de informações sigilosas; ausência de medidas adequadas de segurança da informação; manutenção de perfis falsos utilizados para prática de ilícitos; e omissão diante de conteúdos que violem direitos da personalidade, como honra, imagem e privacidade dos usuários.

Segundo Juliana Evangelista de Almeida e Gabriella Mundim Penaforte (2025), o aumento da disseminação de fake news, discursos de ódio e violações de direitos fundamentais no ambiente digital tem intensificado o debate acerca da necessidade de revisão do modelo tradicional de responsabilização previsto no art. 19 do Marco Civil da Internet. As autoras destacam que a crescente capacidade de moderação,

recomendação e impulsionamento de conteúdos pelas plataformas digitais amplia os deveres de cuidado dos provedores de aplicações, especialmente em situações envolvendo conteúdos manifestamente ilícitos e riscos à proteção dos direitos fundamentais dos usuários. As autoras destacam que a crescente capacidade de moderação e controle exercida pelas plataformas digitais tem ampliado o debate acerca da necessidade de revisão do modelo tradicional previsto no art. 19 do Marco Civil da Internet, especialmente diante do aumento da disseminação de discursos ilícitos, desinformação e violações de direitos fundamentais no ambiente virtual.

Além disso, decisões recentes do Supremo Tribunal Federal passaram a discutir a insuficiência do modelo de responsabilização baseado exclusivamente no descumprimento de ordem judicial. Em 2025, o STF reconheceu a inconstitucionalidade parcial do art. 19 do Marco Civil da Internet, entendendo que a regra geral prevista na legislação nem sempre oferece proteção adequada aos direitos fundamentais dos usuários da internet, especialmente em situações envolvendo conteúdos ilícitos de elevada gravidade.

Por outro lado, Souza e Lemos (2017) sustentam que a ampliação excessiva da responsabilidade civil dos provedores pode gerar riscos à liberdade de expressão e estimular remoções preventivas indiscriminadas de conteúdo pelas plataformas digitais. Segundo os autores, a responsabilização automática dos provedores por conteúdos gerados por terceiros pode incentivar práticas de censura privada, levando as plataformas a remover conteúdos de forma excessiva para evitar futuras sanções, o que comprometeria o livre fluxo de informações no ambiente digital.

Desse modo, a responsabilidade civil dos provedores de internet exige constante equilíbrio entre proteção dos direitos fundamentais, segurança digital, liberdade de expressão e preservação da dinâmica comunicacional própria do ambiente virtual, constituindo um dos principais desafios do direito digital contemporâneo.

Na seara da proteção de dados pessoais, a Lei Geral de Proteção de Dados Pessoais estabelece importantes diretrizes relacionadas à responsabilização civil dos agentes de tratamento. O art. 42 da LGPD dispõe que o controlador ou operador que, em razão do exercício da atividade de tratamento de dados pessoais, causar dano

patrimonial, moral, individual ou coletivo a outrem, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (Brasil, 2018). Além disso, os arts. 46 e 50 da referida legislação determinam que os agentes de tratamento devem adotar medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados, vazamentos e situações ilícitas de tratamento, bem como implementar programas de governança e boas práticas voltados à segurança da informação (Brasil, 2018).

Segundo Viviane Maldonado e Rodrigo Opice Blum (2021), a responsabilização prevista na LGPD representa importante mecanismo de fortalecimento da cultura de proteção de dados no ambiente digital, impondo aos agentes de tratamento elevados deveres de diligência, transparência e prevenção de riscos informacionais. Para os autores, a legislação brasileira passou a exigir das organizações não apenas adequação formal às normas legais, mas também a implementação de programas de conformidade e governança digital, consistentes em políticas internas, mecanismos de fiscalização, auditorias, treinamentos e medidas de segurança voltadas à prevenção de incidentes envolvendo dados pessoais.

Além disso, a responsabilidade civil no contexto digital deve ser analisada à luz dos direitos fundamentais previstos na Constituição Federal de 1988, especialmente os direitos à privacidade, intimidade, honra, imagem e dignidade da pessoa humana, assegurados pelo art. 5º, incisos X e LXXIX, da Constituição Federal (Brasil, 1988).

A Emenda Constitucional nº 115/2022 também reconheceu expressamente a proteção de dados pessoais como direito fundamental autônomo no ordenamento jurídico brasileiro.

Nesse contexto, Patrícia Peck Pinheiro (2021) ressalta que a proteção de dados pessoais ultrapassa a esfera meramente patrimonial, constituindo importante instrumento de preservação da liberdade, autonomia e dignidade dos indivíduos na sociedade da informação. Segundo a autora, o avanço das tecnologias digitais e da circulação massiva de dados pessoais exige instrumentos jurídicos capazes de assegurar equilíbrio entre inovação tecnológica, desenvolvimento econômico e proteção dos direitos fundamentais dos titulares de dados.

Em entendimento convergente, Tarcísio Teixeira (2021) destaca que a responsabilidade civil digital deve ser interpretada de forma compatível com os princípios constitucionais da dignidade da pessoa humana e da proteção da personalidade, especialmente diante do crescimento dos riscos decorrentes do tratamento automatizado de dados pessoais e da ampliação das atividades econômicas realizadas no ambiente digital.

Um aspecto relevante na análise da responsabilidade civil digital consiste na diferenciação entre provedores de conexão e provedores de aplicação. Segundo Patrícia Peck Pinheiro (2020), essa distinção decorre das diferentes funções exercidas por esses agentes no ambiente digital. Os provedores de conexão são responsáveis por viabilizar o acesso dos usuários à internet, enquanto os provedores de aplicação disponibilizam serviços e funcionalidades digitais. A diferenciação também encontra respaldo nos arts. 18 e 19 do Marco Civil da Internet (Brasil, 2014).

O Marco Civil da Internet reconhece essa distinção ao estabelecer regimes jurídicos distintos de responsabilização. O art. 18 da Lei nº 12.965/2014 prevê que o provedor de conexão não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros, enquanto o art. 19 disciplina a responsabilização dos provedores de aplicação nos casos de descumprimento de ordem judicial específica para remoção de conteúdo ilícito (Brasil, 2014).

Segundo Patrícia Peck Pinheiro (2021), a diferenciação entre provedores decorre da própria estrutura funcional da internet, considerando os distintos níveis de participação e controle exercidos pelos agentes envolvidos na circulação das informações digitais. Para a autora, os provedores de aplicação exercem papel mais ativo no ambiente virtual, especialmente diante da utilização de algoritmos, sistemas de recomendação e mecanismos de moderação de conteúdo.

No contexto da sociedade conectada, a dimensão global da circulação de informações amplia significativamente os desafios relacionados à responsabilização civil no ambiente digital. A velocidade da disseminação de conteúdos, a atuação transnacional das plataformas digitais e a descentralização da internet dificultam a

aplicação uniforme das legislações nacionais e a efetividade das medidas de proteção dos direitos fundamentais dos usuários.

Nesse cenário, Tarcísio Teixeira (2021) destaca que o caráter transnacional das relações digitais exige constante atualização dos mecanismos jurídicos de responsabilização, especialmente diante da atuação de grandes plataformas tecnológicas que operam simultaneamente em diferentes países e sistemas jurídicos. Segundo o autor, a proteção dos direitos fundamentais no ambiente digital depende da harmonização entre liberdade de expressão, segurança jurídica e proteção de dados pessoais.

Além disso, Viviane Maldonado e Rodrigo Opice Blum (2021) ressaltam que a responsabilidade civil digital deve considerar não apenas os danos individuais causados pelas plataformas digitais, mas também os impactos coletivos decorrentes da circulação massiva de informações, da desinformação e das falhas de segurança envolvendo dados pessoais.

Em suma, a responsabilização dos provedores de internet constitui tema complexo e em constante transformação, exigindo interpretação compatível com os princípios constitucionais da dignidade da pessoa humana, proteção da privacidade, liberdade de expressão e segurança digital. Embora o ordenamento jurídico brasileiro tenha avançado significativamente com a criação do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais, ainda persistem desafios relacionados à efetividade das medidas preventivas, à atuação das plataformas digitais e à proteção adequada dos usuários diante da crescente circulação de informações no ambiente virtual.

Portanto, os provedores devem buscar equilíbrio entre a preservação da liberdade no ambiente digital e a proteção efetiva dos direitos fundamentais dos usuários, exigindo atuação preventiva, transparência, segurança da informação e fortalecimento contínuo dos mecanismos jurídicos de governança digital.

3.1 Estrutura e funcionamento dos provedores estrangeiros no Brasil

A atuação de provedores estrangeiros no Brasil está diretamente relacionada à expansão da economia digital e ao avanço das tecnologias da informação, especialmente diante da crescente circulação internacional de dados pessoais e da ampliação das plataformas digitais no ambiente virtual. Empresas responsáveis por redes sociais, aplicativos de mensagens instantâneas, serviços de armazenamento em nuvem e mecanismos de busca passaram a exercer significativa influência sobre as relações sociais, econômicas e jurídicas contemporâneas, intensificando debates relacionados à soberania estatal, jurisdição, responsabilidade civil e proteção de dados pessoais.

Segundo Patrícia Peck Pinheiro (2021), a internacionalização das plataformas digitais ampliou os desafios relacionados à aplicação territorial das normas jurídicas nacionais, especialmente em matérias envolvendo privacidade, proteção de dados pessoais e cumprimento de decisões judiciais por empresas sediadas no exterior. A autora destaca que a natureza global da internet exige constante atualização dos mecanismos jurídicos destinados à proteção dos direitos fundamentais dos usuários no ambiente virtual.

No ordenamento jurídico brasileiro, as empresas estrangeiras podem exercer atividades econômicas no território nacional desde que observem as exigências previstas na legislação brasileira. O Código Civil estabelece, em seu art. 1.134, que a sociedade estrangeira depende de autorização do Poder Executivo para funcionar no Brasil, salvo nas hipóteses previstas em lei ou tratados internacionais (Brasil, 2002). Além disso, o art. 1.135 do Código Civil determina que a sociedade estrangeira autorizada a funcionar no país ficará sujeita às leis e aos tribunais brasileiros quanto aos atos ou operações realizados em território nacional (Brasil, 2002).

Nesse contexto, empresas internacionais podem atuar no Brasil por meio de subsidiárias, filiais, sucursais, agências ou representações comerciais, adequando sua estrutura organizacional às exigências do sistema jurídico nacional e às particularidades do mercado brasileiro. A expansão das atividades econômicas digitais ampliou significativamente a presença de empresas estrangeiras no país, sobretudo no setor de tecnologia e comunicação digital.

Além disso, o Marco Civil da Internet estabeleceu importantes diretrizes relacionadas à atuação dos provedores no ambiente digital brasileiro. O art. 11 da Lei nº 12.965/2014 dispõe que qualquer operação de coleta, armazenamento, guarda ou tratamento de registros, dados pessoais ou comunicações realizadas por provedores de conexão e aplicações de internet deverá respeitar a legislação brasileira sempre que pelo menos um dos atos de tratamento ocorrer em território nacional (Brasil, 2014).

Da mesma forma, a Lei Geral de Proteção de Dados Pessoais ampliou o alcance territorial da legislação brasileira ao estabelecer, em seu art. 3º, que a LGPD se aplica a qualquer operação de tratamento de dados pessoais realizada no território nacional ou destinada à oferta de bens e serviços para indivíduos localizados no Brasil, independentemente da localização da sede da empresa responsável pelo tratamento das informações (Brasil, 2018).

Segundo Viviane Maldonado e Rodrigo Opice Blum (2021), a previsão de aplicação extraterritorial da LGPD representa importante mecanismo de fortalecimento da soberania digital brasileira, permitindo maior proteção aos titulares de dados pessoais diante da atuação transnacional das plataformas digitais. Os autores destacam que a crescente circulação internacional de informações exige instrumentos jurídicos capazes de assegurar efetividade à proteção de dados e à responsabilização das empresas que operam no ambiente virtual.

No contexto do direito internacional, a atuação dessas entidades também está relacionada aos mecanismos de cooperação jurídica entre Estados soberanos. Ainda que os tratados internacionais representem importantes instrumentos de regulamentação das relações entre países, a cooperação internacional não se limita à existência de acordos formais, podendo ocorrer com fundamento no princípio da reciprocidade, amplamente reconhecido no direito internacional como instrumento de equilíbrio e colaboração entre as nações.

No ordenamento jurídico brasileiro, a cooperação internacional encontra fundamento no art. 4º, inciso IX, da Constituição Federal de 1988, que estabelece como princípio das relações internacionais da República Federativa do Brasil a cooperação entre os povos para o progresso da humanidade (Brasil, 1988). Além disso, o Código de

Processo Civil disciplina instrumentos de cooperação jurídica internacional, como a carta rogatória e o auxílio direto, previstos nos arts. 26 a 41 da Lei nº 13.105/2015 (Brasil, 2015).

Segundo Rosa (2022), a cooperação jurídica internacional tornou-se elemento indispensável para o compartilhamento transnacional de dados pessoais e para a efetividade das decisões judiciais envolvendo plataformas digitais, especialmente em situações relacionadas à proteção de dados pessoais, aos crimes cibernéticos e à responsabilização civil no ambiente virtual.

Além disso, a própria Lei Geral de Proteção de Dados reconhece a relevância da cooperação internacional ao disciplinar a transferência internacional de dados pessoais em seus arts. 33 e 34. O art. 33 da LGPD estabelece hipóteses em que a transferência internacional de dados é permitida, incluindo situações relacionadas à cooperação jurídica internacional entre órgãos públicos de investigação e persecução penal (Brasil, 2018).

A jurisprudência recente do Superior Tribunal de Justiça também tem reconhecido que empresas de tecnologia que oferecem serviços em território brasileiro devem se submeter à legislação nacional, ainda que possuam sede ou servidores localizados no exterior. Nesse sentido, a Quinta Turma do Superior Tribunal de Justiça, no julgamento do Recurso em Mandado de Segurança n. 66.392/SC, de relatoria do Ministro João Otávio de Noronha, decidiu que empresas de internet que atuam no Brasil estão sujeitas ao cumprimento das decisões judiciais brasileiras, independentemente do armazenamento dos dados ocorrer em servidores localizados fora do país (Brasil, 2022). Tal entendimento está em consonância com as observações de Almeida e Penaforte (2025), segundo as quais a atuação transnacional das plataformas digitais não afasta a incidência da legislação brasileira quando os serviços são ofertados e produzem efeitos em território nacional.

Além disso, no julgamento do Recurso Especial n. 2.147.711/SP, de relatoria da Ministra Nancy Andrighi, a Terceira Turma do Superior Tribunal de Justiça reconheceu a possibilidade de atribuição de efeitos extraterritoriais a ordens judiciais brasileiras de remoção de conteúdos ilícitos da internet, entendendo que a natureza global da internet

justifica, em determinadas situações, a remoção internacional de conteúdos ofensivos para garantir efetiva proteção aos direitos da personalidade (Brasil, 2024). Tal entendimento revela os desafios decorrentes da atuação transnacional das plataformas digitais e da necessidade de mecanismos jurídicos capazes de assegurar efetividade à tutela dos direitos fundamentais no ambiente digital, conforme observam Almeida e Penaforte (2025).

Segundo Tarcísio Teixeira (2021), a expansão das plataformas digitais e a internacionalização das relações virtuais desafiam os modelos tradicionais de jurisdição territorial, exigindo fortalecimento dos mecanismos de cooperação jurídica internacional e adaptação constante das normas relacionadas à proteção de dados pessoais e responsabilidade civil digital.

Dessa forma, observa-se que a organização e o funcionamento dos provedores internacionais no Brasil envolvem complexa articulação entre soberania estatal, proteção de dados pessoais, atividade econômica e efetividade da jurisdição nacional. A crescente internacionalização das relações digitais demonstra que a atuação dessas empresas exige compatibilidade entre inovação tecnológica, cumprimento da legislação brasileira e proteção dos direitos fundamentais dos usuários, evidenciando a necessidade de constante aperfeiçoamento dos mecanismos jurídicos destinados à regulação das relações digitais contemporâneas.

3.2 Responsabilidade Civil e obrigações legais

A responsabilidade civil no ambiente digital constitui tema de elevada relevância no ordenamento jurídico contemporâneo, especialmente diante da intensificação das relações realizadas por meios eletrônicos e da crescente circulação de dados pessoais na internet. No contexto das plataformas digitais e dos provedores de aplicações, a responsabilização jurídica decorre da necessidade de proteção dos direitos fundamentais dos usuários, incluindo privacidade, honra, imagem, proteção de dados pessoais e segurança das informações.

No ordenamento jurídico brasileiro, a responsabilidade civil encontra fundamento geral nos arts. 186 e 927 do Código Civil de 2002. O art. 186 dispõe que aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito (Brasil, 2002). Já o art. 927 estabelece o dever de reparação dos danos causados em decorrência da prática de ato ilícito (Brasil, 2002).

Além disso, o Código Civil também prevê hipóteses de responsabilidade objetiva em determinadas situações, especialmente quando a atividade desenvolvida pelo agente implicar riscos para os direitos de terceiros, conforme estabelece o parágrafo único do art. 927 (Brasil, 2002). Segundo Tarcísio Teixeira (2021), a aplicação da responsabilidade objetiva no ambiente digital tem ganhado relevância diante da crescente complexidade das atividades desenvolvidas pelas plataformas digitais, especialmente em situações envolvendo tratamento massivo de dados pessoais, falhas de segurança da informação e riscos inerentes à atividade tecnológica.

No âmbito das relações de consumo realizadas no ambiente virtual, também se aplica o Código de Defesa do Consumidor (Lei nº 8.078/1990). O art. 14 do CDC estabelece a responsabilidade objetiva do fornecedor de serviços pelos danos causados aos consumidores em decorrência de defeitos relativos à prestação dos serviços, independentemente da existência de culpa (Brasil, 1990). Segundo Patrícia Peck Pinheiro (2021), as plataformas digitais frequentemente se enquadram na condição de fornecedoras de serviços, submetendo-se às normas protetivas do direito do consumidor quando houver relação de consumo envolvendo usuários e serviços digitais.

Além disso, o art. 6º, inciso VI, do Código de Defesa do Consumidor assegura ao consumidor o direito à efetiva prevenção e reparação de danos patrimoniais e morais decorrentes da prestação inadequada de serviços (Brasil, 1990). Nesse contexto, a responsabilidade civil das empresas digitais também pode decorrer de falhas relacionadas à segurança da informação, vazamento de dados pessoais, publicidade enganosa, omissão na prestação de informações e defeitos na prestação de serviços eletrônicos.

A responsabilidade civil digital também deve ser analisada à luz do Marco Civil da Internet (Lei nº 12.965/2014), que estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil. O art. 19 da referida legislação prevê que os provedores de aplicações de internet somente poderão ser responsabilizados civilmente por conteúdos gerados por terceiros caso, após ordem judicial específica, não promovam a remoção do conteúdo ilícito apontado como infringente (Brasil, 2014).

Segundo Viviane Maldonado e Rodrigo Opice Blum (2021), o modelo de responsabilização previsto no Marco Civil da Internet buscou equilibrar a proteção da liberdade de expressão com a necessidade de responsabilização das plataformas digitais por danos causados aos usuários. Para os autores, a exigência de ordem judicial específica procura evitar práticas de censura privada e remoções arbitrárias de conteúdo pelas empresas responsáveis pelas plataformas digitais.

Entretanto, parte da doutrina critica a limitação da responsabilidade civil prevista no art. 19 do Marco Civil da Internet. Segundo Juliana Evangelista de Almeida e Gabriella Mundim Penaforte (2025), a exigência de decisão judicial prévia pode retardar a remoção de conteúdos ilícitos e comprometer a efetividade da proteção dos direitos fundamentais dos usuários, especialmente em situações envolvendo discurso de ódio, desinformação, vazamento de dados pessoais e divulgação indevida de conteúdos íntimos.

No campo específico da proteção de dados pessoais, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) estabeleceu importantes regras relacionadas à responsabilização civil dos agentes de tratamento. O art. 42 da LGPD dispõe que o controlador ou operador que causar dano patrimonial, moral, individual ou coletivo em razão do tratamento inadequado de dados pessoais é obrigado a repará-lo (Brasil, 2018).

Além disso, os arts. 46 e 50 da LGPD determinam que os agentes de tratamento devem adotar medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados, vazamentos e situações ilícitas de tratamento, bem como implementar programas de governança e boas práticas voltados à proteção das informações pessoais (Brasil, 2018).

Segundo Rodrigo Pironti (2021), a LGPD ampliou significativamente os deveres jurídicos relacionados à segurança da informação e à proteção de dados pessoais, exigindo das organizações atuação preventiva contínua e implementação de mecanismos efetivos de gestão de riscos informacionais. Para o autor, a responsabilidade civil prevista na LGPD possui não apenas caráter reparatório, mas também função preventiva e pedagógica.

Além da legislação nacional, a jurisprudência dos tribunais superiores também vem desempenhando importante papel na consolidação da responsabilidade civil digital. O Superior Tribunal de Justiça possui entendimento consolidado no sentido de que provedores de aplicações podem ser responsabilizados quando houver omissão no cumprimento de ordens judiciais de remoção de conteúdo ilícito ou falhas relacionadas à segurança da informação e proteção de dados pessoais.

Nesse contexto, observa-se que a responsabilidade civil no ambiente digital exige interpretação integrada entre Constituição Federal, Código Civil, Código de Defesa do Consumidor, Marco Civil da Internet e Lei Geral de Proteção de Dados pessoais. A crescente complexidade das relações virtuais demanda mecanismos jurídicos capazes de garantir proteção efetiva aos usuários sem comprometer direitos fundamentais como liberdade de expressão, inovação tecnológica e livre desenvolvimento econômico.

Dessa forma, conclui-se que a responsabilização civil das plataformas digitais e dos agentes de tratamento de dados deve ocorrer de maneira proporcional, preventiva e compatível com os princípios constitucionais da dignidade da pessoa humana, proteção da privacidade, segurança jurídica e proteção dos dados pessoais. A efetividade dessas normas depende não apenas da aplicação de sanções legais, mas também do fortalecimento das práticas de governança digital, fiscalização estatal e prevenção de danos no ambiente virtual.

4 A RESISTÊNCIA DOS PROVEDORES ESTRANGEIROS AO CUMPRIMENTO DE ORDENS JUDICIAIS

A crescente expansão das plataformas digitais e da circulação internacional de dados pessoais intensificou os desafios relacionados à efetividade das decisões judiciais

no ambiente virtual. Empresas estrangeiras responsáveis por redes sociais, aplicativos de mensagens, serviços de armazenamento em nuvem e mecanismos de busca passaram a desempenhar papel central na economia digital contemporânea, exercendo influência direta sobre a circulação de informações, proteção de dados pessoais e exercício dos direitos fundamentais dos usuários da internet. Nesse contexto, Patrícia Peck Pinheiro (2021) destaca que a evolução das tecnologias digitais e a atuação transnacional das plataformas ampliaram os conflitos relacionados à soberania estatal, proteção de dados pessoais e aplicação territorial das normas jurídicas no ambiente digital.

O Código de Processo Civil de 2015 disciplina, nos arts. 26 a 41, instrumentos de cooperação jurídica internacional, como auxílio direto e cartas rogatórias, destinados à prática de atos processuais em território estrangeiro e ao intercâmbio de informações entre autoridades judiciais nacionais e internacionais (Brasil, 2015).

Além disso, a Lei Geral de Proteção de Dados estabelece regras específicas relacionadas à transferência internacional de dados pessoais. O art. 33 da LGPD prevê hipóteses autorizadoras para transferência internacional de dados, incluindo situações relacionadas à cooperação jurídica internacional entre órgãos públicos de investigação e persecução penal (Brasil, 2018).

Segundo Viviane Maldonado e Rodrigo Opice Blum (2021), a cooperação internacional tornou-se elemento indispensável para efetividade da proteção de dados pessoais e responsabilização das plataformas digitais, especialmente diante da atuação transnacional das empresas de tecnologia e da circulação global de informações.

Outro importante mecanismo de enfrentamento consiste na atuação da Autoridade Nacional de Proteção de Dados. A Autoridade Nacional de Proteção de Dados, possui competência para fiscalizar o cumprimento da LGPD, aplicar sanções administrativas e promover diretrizes relacionadas à proteção de dados pessoais e segurança da informação, conforme as atribuições previstas no art. 55-J da Lei nº 13.709/2018 (Brasil, 2018).

Em 2021, a Autoridade Nacional de Proteção de Dados, informou a apuração de incidente relacionado ao vazamento de dados pessoais de mais de 220 milhões de pessoas, fato que evidenciou a necessidade de fortalecimento das políticas de segurança da informação, prevenção de riscos e fiscalização do tratamento de dados pessoais no Brasil (Brasil, 2021).

Segundo Rodrigo Pironti (2021), a efetividade da proteção de dados pessoais depende não apenas da existência de legislação específica, mas também da implementação concreta de mecanismos de governança, fiscalização contínua e prevenção de incidentes de segurança da informação.

Além disso, o fortalecimento da educação digital, da transparência no tratamento de dados e das políticas preventivas de segurança da informação constitui importante instrumento de proteção dos direitos fundamentais no ambiente virtual contemporâneo.

Dessa forma, observa-se que os mecanismos de enfrentamento relacionados à resistência dos provedores estrangeiros exigem constante integração entre legislação nacional, cooperação internacional, atuação jurisdicional e fiscalização administrativa. A crescente internacionalização das relações digitais demonstra que a efetividade da jurisdição no ambiente virtual depende do fortalecimento dos instrumentos de proteção de dados pessoais, responsabilização civil digital e cooperação jurídica internacional, garantindo equilíbrio entre inovação tecnológica, soberania estatal e proteção dos direitos fundamentais dos usuários brasileiros.

4.1 Responsabilidades entre provedores de backbone, acesso e conteúdo: dificuldades práticas de aplicação

A determinação das obrigações entre os variados provedores de internet é um dos grandes desafios do direito digital atual, especialmente considerando a

complexidade estrutural da internet. O funcionamento da rede global é resultado da colaboração de diversos agentes econômicos e tecnológicos, cada um com suas funções específicas na transmissão, disponibilização e controle de informações digitais. Nesse sentido, a literatura especializada passou a categorizar os provedores em três grupos principais: provedores de backbone, provedores de acesso e provedores de conteúdo, sendo imprescindível a definição jurídica das responsabilidades que cabem a cada um desses grupos.

Os provedores de backbone são as companhias encarregadas da infraestrutura fundamental da internet, gerenciando redes de grande capacidade que facilitam a transferência de elevados volumes de dados entre várias regiões, nações e distintos sistemas de telecomunicações. Sua função forma a espinha dorsal da internet, possibilitando a conexão entre diferentes redes e assegurando o fluxo mundial de informações digitais. Ao contrário de outros provedores, os provedores de backbone não possuem interação direta com o usuário final nem exercem controle sobre os conteúdos que circulam na rede, atuando essencialmente na transmissão de dados e na manutenção da conectividade entre redes (Teixeira, 2021).

Em sua análise teórica, Teixeira (2021) argumenta que a sociedade atual é organizada em redes globais de informação, onde a troca de dados se dá de forma descentralizada e ultrapassa fronteiras nacionais. O autor observa que a infraestrutura da internet transforma radicalmente as relações de poder estabelecidas e torna mais desafiadora a implementação dos métodos tradicionais de controle legal, principalmente devido à fragmentação técnica que caracteriza a rede.

Nesse cenário, a atribuição de responsabilidade aos provedores de backbone enfrenta limitações práticas significativas, já que sua função se limita ao transporte de dados, sem envolvimento direto na criação, armazenamento ou moderação de conteúdo. Como Patrícia Peck Pinheiro (2020) observa, esses provedores desempenham um papel puramente estrutural, análogo às concessionárias que gerenciam a infraestrutura física das telecomunicações, e não é justo considerar que possam ser automaticamente responsabilizados pelos conteúdos gerados por terceiros.

Ademais, a própria característica técnica da atividade torna inviável o controle antecipado de todo o fluxo de dados que ocorre na rede. A implementação de extensos mecanismos de supervisão por parte dos provedores de backbone poderia colocar em risco princípios essenciais da internet, tais como a neutralidade da rede, a proteção da privacidade nas comunicações e a liberdade de expressão.

No Brasil, o Marco Civil da Internet estabeleceu uma abordagem similar ao definir restrições à responsabilização das entidades que apenas transmitem dados. Segundo Souza e Lemos (2017), o legislador brasileiro teve como objetivo evitar que as empresas que gerenciam a infraestrutura técnica da internet se tornassem entidades privadas de controle e censura da informação.

Os provedores de acesso têm a responsabilidade de conectar os usuários à internet, fornecendo os recursos necessários para a navegação online. Apesar de possuírem relação direta com os usuários, não exercem controle sobre os conteúdos disponibilizados na rede. Por essa razão, o Marco Civil da Internet estabelece que o provedor de conexão não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros, conforme previsto em seu art. 18 (Brasil, 2014).

Em contrapartida, os fornecedores de conteúdo — conhecidos também como fornecedores de aplicativos — desempenham uma função significativamente mais proativa na atual dinâmica digital. As redes sociais, plataformas de vídeo, serviços de armazenamento e ferramentas de busca não se limitam a guardar dados, mas também estruturam, sugerem e promovem conteúdos utilizando algoritmos e sistemas automatizados.

De acordo com Patrícia Peck Pinheiro (2020), as plataformas digitais não se limitam mais a ser meras intermediárias tecnológicas; elas agora desempenham um papel crucial na regulação do fluxo de informações na era atual. Essa nova função amplia as discussões sobre a urgência da implementação de responsabilidades preventivas que envolvem a segurança digital, a governança e a moderação de conteúdos.

Diante desse contexto, o Marco Civil da Internet estabeleceu, em seu art. 19, um sistema de responsabilidade subjetiva para os provedores de aplicação, tornando sua

responsabilização vinculada ao descumprimento de ordem judicial específica que determine a indisponibilização de conteúdo considerado ilícito (Brasil, 2014). Segundo Souza e Lemos (2017), esse modelo busca evitar a denominada "censura privada", preservando a liberdade de expressão e impedindo a remoção arbitrária de conteúdos pelas plataformas digitais.

Contudo, a implementação real desse sistema enfrenta vários desafios. O mais significativo se origina da rapidez com que as informações se espalham na internet, possibilitando que conteúdos ilegais se tornem amplamente acessíveis antes que uma decisão judicial para remoção seja alcançada. Em diversas situações, o prejuízo à reputação, imagem ou intimidade da pessoa já está estabelecido quando a ação judicial é iniciada.

Além disso, a expansão da coleta e processamento de dados pessoais intensificou as discussões sobre a responsabilidade civil no ambiente digital. A Lei Geral de Proteção de Dados Pessoais agora requer que as organizações implementem medidas preventivas para garantir a segurança da informação e a proteção dos dados pessoais.

Bruno Bioni (2020) argumenta que a proteção dos dados pessoais não deve ser vista apenas como um recurso individual de autorização, mas sim como uma ferramenta coletiva para equilibrar as interações digitais, que são influenciadas pela desigualdade de poder entre os usuários e as grandes empresas de tecnologia.

Igualmente, Danilo Doneda (2006) destaca que a salvaguarda das informações pessoais se estabeleceu como um direito fundamental por si só, o que demanda o aprimoramento dos mecanismos de governança informacional e a responsabilização no ambiente digital.

Um outro desafio significativo diz respeito à atuação de fornecedores internacionais dentro do país. Diversas plataformas online realizam atividades econômicas no Brasil sem uma presença física estabelecida, o que torna mais complexo o cumprimento de decisões judiciais e a responsabilização civil dessas companhias. Como enfatiza Portela (2015), o caráter global da internet impõe restrições à soberania

dos Estados e demanda um aprimoramento dos sistemas de cooperação jurídica internacional.

Ademais, os recorrentes vazamentos substanciais de informações pessoais evidenciam deficiências nos sistemas de segurança online. Aragão (2022) aponta que os recentes episódios de exposição inadequada de dados revelam as limitações práticas da legislação brasileira em matéria de proteção de dados, especialmente no que tange à prevenção de conflitos cibernéticos.

Sob a ótica constitucional, a proteção dos dados pessoais está diretamente relacionada à tutela da dignidade da pessoa humana e dos direitos fundamentais. Conforme Bioni (2020), o tratamento inadequado ou o vazamento de dados pessoais pode gerar impactos significativos na esfera individual dos titulares, justificando a adoção de instrumentos jurídicos voltados à prevenção de danos e à responsabilização dos agentes envolvidos.

Assim, observa-se que os desafios práticos para a implementação da responsabilidade entre os provedores resultam da própria natureza descentralizada da internet e da inadequação dos métodos tradicionais de responsabilização frente às novas dinâmicas digitais. A rapidez na disseminação de informações, a operação transnacional das plataformas e a concentração econômica das grandes corporações de tecnologia evidenciam a urgência de um aprimoramento contínuo dos instrumentos legais de governança e proteção no ambiente digital.

4.2 Casos paradigmáticos na jurisprudência brasileira

A jurisprudência brasileira tem desempenhado papel fundamental na definição dos limites da responsabilidade civil digital e na interpretação das normas relacionadas à proteção de dados pessoais, à atuação das plataformas digitais e à efetividade das decisões judiciais no ambiente virtual. Diante da constante evolução tecnológica, os tribunais passaram a exercer papel relevante na consolidação de entendimentos capazes de equilibrar a proteção dos direitos fundamentais com a liberdade de expressão e o desenvolvimento das atividades digitais.

Um dos precedentes relevantes sobre a atuação das plataformas digitais foi o Recurso em Mandado de Segurança n. 66.392/SC, julgado pela Quinta Turma do

Superior Tribunal de Justiça, sob relatoria do Ministro João Otávio de Noronha, em 08 de novembro de 2022. Na decisão, o STJ firmou entendimento de que empresas que prestam serviços de internet em território nacional devem se submeter ao ordenamento jurídico brasileiro, independentemente da localização de seus servidores ou da existência de sede no exterior. O julgamento reforçou a efetividade da jurisdição nacional em questões envolvendo plataformas digitais e proteção de direitos fundamentais (STJ, 2022).

Outro precedente paradigmático foi o Recurso Especial n. 2.147.711/SP, julgado pela Terceira Turma do Superior Tribunal de Justiça, sob relatoria da Ministra Nancy Andrighi, em 12 de novembro de 2024. A controvérsia envolveu a remoção de conteúdo considerado ilícito na internet e a possibilidade de cumprimento da ordem judicial com efeitos além do território nacional. O STJ entendeu que, em determinadas situações, a remoção pode produzir efeitos globais para assegurar a efetividade da tutela jurisdicional e a proteção dos direitos da personalidade. A decisão também reforçou a importância do art. 19 da Lei nº 12.965/2014 (Marco Civil da Internet), que estabelece a responsabilização dos provedores de aplicação quando houver descumprimento de ordem judicial específica para retirada de conteúdo ilícito (STJ, 2024).

As decisões analisadas demonstram que a jurisprudência brasileira vem consolidando mecanismos de responsabilização compatíveis com a realidade digital contemporânea. Ao mesmo tempo em que protege direitos fundamentais como honra, privacidade, imagem e proteção de dados pessoais, o Poder Judiciário busca evitar a censura prévia e preservar a liberdade de expressão, observando os critérios estabelecidos pelo Marco Civil da Internet. Dessa forma, os julgados do Superior Tribunal de Justiça evidenciam a crescente importância da atuação jurisdicional na construção de soluções adequadas para os conflitos surgidos no ambiente digital.

Um assunto de significativa importância no âmbito jurídico diz respeito aos grandes vazamentos de dados pessoais ocorridos após a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD). O aumento expressivo da coleta,

armazenamento e compartilhamento de informações por empresas e órgãos públicos ampliou os riscos relacionados à privacidade e à segurança dos dados dos cidadãos, resultando em discussões cada vez mais frequentes acerca da responsabilidade civil dos agentes envolvidos em incidentes de segurança.

Um exemplo relevante ocorreu em 2021, quando foi identificado um dos maiores vazamentos de dados já registrados no Brasil, envolvendo informações pessoais de mais de 220 milhões de pessoas. Em razão da gravidade do caso, a Autoridade Nacional de Proteção de Dados instaurou procedimento de apuração para investigar as circunstâncias do incidente e verificar possíveis violações à legislação de proteção de dados (Brasil, 2021). O episódio evidenciou a necessidade de fortalecimento dos mecanismos de segurança da informação e da fiscalização do tratamento de dados pessoais no país.

De acordo com Aragão (2022), os recorrentes vazamentos de dados no Brasil demonstram fragilidades significativas nos sistemas de proteção das informações, evidenciando que a existência de legislação específica, por si só, não é suficiente para garantir a efetiva proteção dos titulares de dados.

Nesse contexto, Bioni (2020) sustenta que a proteção de dados pessoais deve ser compreendida como instrumento de equilíbrio nas relações digitais, considerando a assimetria existente entre os titulares dos dados e as grandes organizações que realizam o tratamento dessas informações. Para o autor, a responsabilização civil deve ser acompanhada da adoção de medidas preventivas voltadas à governança, à transparência e à segurança da informação.

De forma semelhante, Pinheiro (2021) destaca que a proteção de dados pessoais está diretamente relacionada à tutela da privacidade e dos direitos fundamentais, exigindo das organizações a implementação de práticas adequadas de conformidade e segurança para prevenir incidentes que possam causar danos aos titulares. No mesmo sentido, Maldonado e Blum (2021) defendem que a efetividade da LGPD depende não apenas da aplicação de sanções, mas também da criação de uma cultura organizacional voltada à proteção dos dados pessoais.

Dessa forma, os grandes vazamentos de dados ocorridos nos últimos anos demonstram que a proteção das informações pessoais constitui um dos principais desafios do direito digital contemporâneo, exigindo atuação conjunta do Estado, das empresas e dos órgãos de fiscalização para garantir maior segurança jurídica e proteção aos direitos fundamentais dos cidadãos.

Dessa forma, a análise das decisões do Superior Tribunal de Justiça e dos casos concretos de vazamento de dados demonstra que a proteção das informações pessoais constitui um dos principais desafios do direito digital contemporâneo. Os precedentes examinados evidenciam a crescente preocupação do Poder Judiciário com a efetividade da jurisdição nacional diante da atuação transnacional das plataformas digitais, bem como com a responsabilização dos provedores em situações que envolvem conteúdos ilícitos e violações a direitos fundamentais. Além disso, os episódios de vazamento de dados reforçam a necessidade de fortalecimento das políticas de segurança da informação, da fiscalização exercida pela Autoridade Nacional de Proteção de Dados e da adoção de mecanismos preventivos capazes de assegurar maior proteção aos titulares de dados pessoais.

4.3 Mecanismos de enfrentamento

Confrontar os desafios dos crimes virtuais, a atribuição de responsabilidade aos provedores e a salvaguarda de dados pessoais demanda a implementação de instrumentos legais, institucionais e tecnológicos que possam acompanhar a complexidade da atual sociedade digital. A característica global da internet, combinada com a rapidez na troca de informações e o progresso das tecnologias digitais, torna inadequado depender apenas de ações punitivas, necessitando de abordagens preventivas, colaborativas e interdisciplinares para uma gestão eficaz da era digital.

Nesse cenário, um dos mecanismos mais relevantes para lidar com a situação é o aprimoramento das leis que visam a defesa dos dados e a responsabilização dos indivíduos que atuam no espaço digital. No Brasil, o Marco Civil da Internet e a Lei Geral

de Proteção de Dados são marcos significativos na evolução da legislação, visando a salvaguarda dos direitos fundamentais no ambiente online.

De acordo com Souza e Lemos (2017), o Marco Civil da Internet definiu diretrizes essenciais para o uso da internet no Brasil, com foco na preservação da liberdade de expressão, da privacidade e da neutralidade da rede. Os autores afirmam que a legislação brasileira teve como objetivo promover um equilíbrio entre a inovação tecnológica, o crescimento econômico e a salvaguarda dos direitos dos usuários no meio digital.

No entanto, a simples presença de normas legais não assegura a efetividade na salvaguarda dos direitos fundamentais. Nesse contexto, Bruno Bioni (2020) ressalta que a proteção de informações pessoais requer não apenas medidas punitivas de responsabilização, mas também o desenvolvimento de estruturas duradouras de governança, conformidade e gestão de riscos. Para o autor, a prevenção deve ser o foco principal na política de proteção de dados, substituindo abordagens que apenas reagem às situações.

De maneira semelhante, Danilo Doneda (2006) argumenta que a proteção jurídica dos dados pessoais deve focar em medidas preventivas que garantam a autodeterminação informativa, principalmente considerando a crescente habilidade tecnológica das grandes empresas digitais em coletar e processar informações pessoais. Segundo ele, a mera compensação após a ocorrência de um dano não é suficiente quando se observa a magnitude coletiva dos riscos gerados pela sociedade da informação.

Neste contexto, é fundamental ressaltar o papel da Autoridade Nacional de Proteção de Dados (ANPD), estabelecida para monitorar a observância da LGPD e impor penalidades administrativas às entidades que não cumprirem as diretrizes referentes à proteção de dados pessoais. A atuação da ANPD é um elemento crucial para o fortalecimento da governança digital no Brasil.

A implementação de iniciativas de conformidade digital e proteção da informação se tornou fundamental para evitar incidentes cibernéticos. As organizações

começaram a incorporar ações técnicas e administrativas para salvaguardar os dados pessoais dos usuários, como criptografia, autenticação em múltiplos fatores, vigilância contínua de sistemas e diretrizes internas para a gestão de riscos.

Patrícia Peck Pinheiro (2020) defende que a proteção das informações deve ser vista como um componente estratégico nas empresas modernas, demandando uma sinergia entre tecnologia, governança e compromisso legal. A autora destaca que a implementação de medidas preventivas é essencial para minimizar os riscos associados a vazamentos de dados e incidentes cibernéticos.

Os constantes casos de vazamentos em larga escala de informações pessoais evidenciam essa urgência. Aragão (2022) aponta que os incidentes recentes de divulgação inadequada de dados no Brasil revelam fragilidades nos sistemas de segurança digital, tanto em entidades públicas quanto em privadas, mostrando as limitações reais na eficácia da legislação brasileira.

Um outro mecanismo significativo de combate diz respeito à cooperação jurídica em âmbito internacional. Tendo em vista que muitas plataformas digitais atuam em escala global e possuem servidores fora do país, a eficácia das decisões judiciais no Brasil muitas vezes está atrelada à colaboração entre nações soberanas.

Outro importante mecanismo de enfrentamento aos crimes cibernéticos consiste na cooperação jurídica internacional fortalecida pela Convenção sobre o Crime Cibernético, conhecida como Convenção de Budapeste. O tratado internacional foi promulgado no Brasil por meio do Decreto nº 11.491, de 12 de abril de 2023, tendo como objetivo ampliar a cooperação entre os países na investigação e repressão de crimes praticados por meio de sistemas informáticos, além de facilitar a obtenção de provas eletrônicas e o intercâmbio de informações entre autoridades competentes (Brasil, 2023).

A promulgação da Convenção de Budapeste representa importante avanço para o ordenamento jurídico brasileiro, especialmente diante da atuação transnacional das plataformas digitais e da crescente complexidade dos crimes cibernéticos. Nesse sentido, o instrumento internacional complementa os mecanismos de cooperação já

mencionados por Rezek (2017) e Cavallieri (2015), fortalecendo a efetividade das investigações e das decisões judiciais que envolvem agentes localizados em diferentes países. Além disso, a Convenção estabelece medidas voltadas à preservação de provas digitais, assistência jurídica mútua e cooperação permanente entre os Estados signatários, contribuindo para maior segurança jurídica no ambiente digital.

De maneira similar, Portela (2015) argumenta que a internet desafia os tradicionais modelos de soberania nacional, demandando abordagens inovadoras de integração legal entre nações para lidar de forma eficaz com as transgressões digitais.

Além dos instrumentos legais e das estruturas institucionais, a promoção da educação digital constitui importante mecanismo de enfrentamento dos desafios relacionados à proteção de dados pessoais. Embora a Lei Geral de Proteção de Dados Pessoais represente significativo avanço normativo ao estabelecer direitos, deveres e mecanismos de responsabilização, sua efetividade depende da conscientização dos usuários e da adoção de boas práticas de segurança da informação por parte da sociedade e das organizações.

Nesse contexto, Pinheiro (2021) destaca que a proteção de dados pessoais não se limita ao cumprimento formal da legislação, exigindo também a construção de uma cultura de proteção digital baseada na educação, na transparência e na prevenção de riscos. De forma semelhante, Bioni (2020) sustenta que a efetividade da proteção de dados depende da participação ativa dos titulares e do fortalecimento de mecanismos de governança capazes de promover maior controle sobre o tratamento das informações pessoais.

Dessa forma, observa-se que a LGPD representou importante marco para a proteção dos dados pessoais no Brasil, porém a sua plena efetividade exige investimentos contínuos em educação digital, conscientização dos usuários e desenvolvimento de práticas preventivas voltadas à segurança da informação e à proteção dos direitos fundamentais no ambiente digital.Na visão sociológica de Teixeira (2021), a sociedade em rede transformou de maneira significativa as dinâmicas tradicionais de poder e comunicação, dando origem a estruturas globais de fluxo informacional que colocam em xeque os modelos clássicos de regulação governamental.

Segundo ele, é necessário desenvolver mecanismos colaborativos e integrados em nível internacional para enfrentar os desafios do ambiente digital.

Ademais, Moraes (2003) argumenta que a salvaguarda dos direitos fundamentais no contexto digital precisa levar em conta as consequências das infrações informacionais na vida das pessoas. Assim, a proteção legal da privacidade, da reputação e da dignidade torna-se essencial nas abordagens atuais para lidar com as violações que ocorrem no ambiente digital.

Dessa forma, observa-se que as estratégias para lidar com os desafios digitais não devem restringir-se à responsabilização tardia dos indivíduos envolvidos. A complexidade da sociedade da informação demanda a criação de modelos de governança que priorizem a prevenção, o aumento da colaboração internacional, a adoção de políticas de segurança da informação e a promoção de uma cultura jurídica focada na salvaguarda efetiva dos direitos fundamentais no espaço digital.

5 CONCLUSÃO

O presente trabalho teve como objetivo analisar os principais desafios relacionados à proteção de dados pessoais e à responsabilidade civil das plataformas digitais no ordenamento jurídico brasileiro. Nesse sentido, a presente pesquisa evidenciou que o avanço das tecnologias digitais transformou profundamente as relações sociais, econômicas e jurídicas na sociedade contemporânea, ampliando os desafios relacionados à proteção de dados pessoais, à privacidade e à responsabilização civil no ambiente virtual.

A presente pesquisa evidenciou que o avanço das tecnologias digitais transformou profundamente as relações sociais, econômicas e jurídicas na sociedade contemporânea, ampliando os desafios relacionados à proteção de dados pessoais, à privacidade e à responsabilização civil no ambiente virtual. Nesse contexto, verificou-se que a Lei Geral de Proteção de Dados Pessoais e o Marco Civil da Internet representam importantes instrumentos jurídicos destinados à proteção dos direitos fundamentais

dos usuários da internet, estabelecendo parâmetros relevantes para o tratamento de dados pessoais e para a atuação das plataformas digitais no Brasil.

Contudo, apesar dos avanços legislativos observados nos últimos anos, a efetividade dessas normas ainda enfrenta obstáculos decorrentes da rápida evolução tecnológica, da atuação transnacional das grandes plataformas digitais e da intensa circulação de informações em escala global, fatores que dificultam a plena aplicação dos mecanismos jurídicos de proteção existentes no ordenamento brasileiro.

Diante desse cenário, observou-se que a responsabilidade civil digital exige constante equilíbrio entre diferentes garantias constitucionais, especialmente no que se refere à proteção da privacidade, à liberdade de expressão, à segurança jurídica e ao desenvolvimento tecnológico.

A crescente utilização de algoritmos e sistemas automatizados pelas plataformas digitais ampliou significativamente os debates acerca dos deveres de cuidado, transparência e responsabilização das empresas que atuam no ambiente virtual. Nesse cenário, tornou-se evidente que a proteção efetiva dos dados pessoais não depende exclusivamente da existência de legislação específica, sendo igualmente necessário o fortalecimento das práticas de governança digital, da segurança da informação e da atuação eficiente dos órgãos responsáveis pela fiscalização e aplicação das normas jurídicas. Da mesma forma, verificou-se que a cooperação jurídica internacional assume papel essencial diante da natureza global das relações digitais e das dificuldades relacionadas ao cumprimento de decisões judiciais envolvendo empresas sediadas no exterior.

Dessa forma, conclui-se que o direito digital constitui um campo jurídico em permanente transformação, exigindo atualização contínua dos mecanismos normativos destinados à proteção dos direitos fundamentais no ambiente virtual. Assim, torna-se indispensável o fortalecimento das políticas públicas voltadas à educação digital, à conscientização acerca da proteção de dados pessoais e ao aprimoramento da segurança da informação, buscando garantir maior proteção aos usuários sem comprometer a liberdade de expressão, a inovação tecnológica e o desenvolvimento das relações digitais contemporâneas.

REFERÊNCIAS

ALMEIDA, Juliana Evangelista de; PENAFORTE, Gabriella Mundim. Marco Civil da Internet (Lei nº 12.965/14) e os desafios contemporâneos à responsabilidade civil dos provedores na era das fake news. *Revista de Ciências do Estado*, Belo Horizonte, v. 10, n. 1, p. 1–23, 2025. DOI: 10.35699/2525-8036.2025.54425.

ARAGÃO, Alexandre. Vazamentos de dados no Brasil e suas consequências. *JOTA*, 2022. Disponível em: https://www.jota.info/tributos-e-

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020.

BRASIL. Autoridade Nacional de Proteção de Dados. ANPD está apurando no caso do vazamento de dados de mais de 220 milhões de pessoas. *Notícias*, Brasília, DF: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpdesta-apurando-no-caso-do-vazamento-de-dados-de-mais-de-220-milhoes-depessoas. Acesso em: 16 maio 2026.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988.

BRASIL. *Decreto nº 11.491, de 12 de abril de 2023.* Promulga a Convenção sobre o Crime Cibernético (Convenção de Budapeste). Brasília, DF: Presidência da República, 2023.

BRASIL. *Emenda Constitucional nº 115, de 10 de fevereiro de 2022*. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Brasília, DF: Presidência da República, 2022.

BRASIL. *Lei nº 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Brasília, DF: Presidência da República, 2002.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014.* Marco Civil da Internet. Brasília, DF: Presidência da República, 2014.

BRASIL. *Lei nº 13.105, de 16 de março de 2015.* Código de Processo Civil. Brasília, DF: Presidência da República, 2015.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*. Código de Defesa do Consumidor. Brasília, DF: Presidência da República, 1990.

BRASIL. Superior Tribunal de Justiça. *Recurso em Mandado de Segurança n. 66.392/SC*. Rel. Min. João Otávio de Noronha. Quinta Turma. Julgado em 08 nov. 2022.

BRASIL. Superior Tribunal de Justiça. *Recurso Especial n. 2.147.711/SP*. Rel. Min. Nancy Andrighi. Terceira Turma. Julgado em 12 nov. 2024.

CASTELLS, Manuel. *A sociedade em rede***.** 6. ed. São Paulo: Paz e Terra, 1999.

CAVALLIERI, Luiz Antonio. *A cooperação internacional***.** Revista de Direito, [S. l.], v. 7, n. 1, p. 195–220, 2015.

COTS, Márcio; OLIVEIRA, Ricardo de. *Lei Geral de Proteção de Dados Pessoais comentada***.** 4. ed. São Paulo: Revista dos Tribunais, 2021.

Disponível em: https://periodicos.ufmg.br/index.php/revice/article/view/e54425. Acesso em: 15 maio 2026.

DONEDA, Danilo*. Da privacidade à proteção de dados pessoais***.** Rio de Janeiro: Renovar, 2006.

empresas/mercado/vazamentos-de-dados-no-brasil-28012022. Acesso em: 01 maio 2026.

MALDONADO, Viviane Nóbrega; BLUM, Rodrigo Opice. *LGPD comentada***.** 3. ed. São Paulo: Revista dos Tribunais, 2021.

MARTINS, Guilherme; LONGHI, João Victor Rozatti. *Proteção de dados pessoais na sociedade da informação: entre dados e danos***.** São Paulo: Editora Foco, 2021.

MORAES, Maria Celina Bodin de. *Danos à pessoa humana: uma leitura civil constitucional dos danos morais***.** Rio de Janeiro: Renovar, 2003.

PECK PINHEIRO, Patrícia. *Direito digital***.** 6. ed. São Paulo: Saraiva, 2020.

PINHEIRO, Patrícia Peck. *Proteção de dados pessoais***.** 3. ed. São Paulo: Saraiva Jur, 2021.

PIRONTI, Rodrigo. *Lei Geral de Proteção de Dados no setor público***.** São Paulo: Fórum, 2021.

PORTELA, Carlos Henrique Gonçalves. *Direito Internacional Público e Privado***:** incluindo noções de Direitos Humanos e de Direito Comunitário. 7. ed. Salvador: JusPodivm, 2015.

REZEK, Francisco. *Direito internacional público*: curso elementar**.** 15. ed. São Paulo: Saraiva, 2017.

ROSA, Raíssa Roese da. Cooperação jurídica internacional e proteção de dados pessoais no ambiente digital**.** *Revista de Direito Internacional*, Brasília, v. 19, n. 1, p. 210-230, 2022.

SOUZA, Carlos Affonso Pereira de; LEMOS, Ronaldo. *Marco Civil da Internet: comentários à Lei nº 12.965/2014***.** São Paulo: Atlas, 2017.

SOUZA, Carlos Affonso Pereira de; LEMOS, Ronaldo. *Marco Civil da Internet: construção e aplicação***.** Juiz de Fora: Editar Editora Associada Ltda., 2017.

TEIXEIRA, Tarcisio. *Direito digital e proteção de dados pessoais.* São Paulo: Saraiva Educação, 2021.