

**FACULDADE DE ADMINISTRAÇÃO, NEGÓCIOS E SAÚDE DE SERGIPE -
FANESE
CURSO DE DIREITO**

HILTON LINHARES NETO

**RESPONSABILIDADE CIVIL DE PLATAFORMAS DIGITAIS POR CONTEÚDOS
POSTADOS POR USUÁRIOS**

**ARACAJU
2025**

L755r

LINHARES NETO, Hilton

Responsabilidade civil de plataformas digitais por conteúdos postados por usuários / Hilton Linhares Neto. - Aracaju, 2025.

29 f.

Trabalho de Conclusão de Curso (Artigo)
Faculdade de Administração, Negócios e Saúde de Sergipe. Coordenação de Direito.

Orientador(a): Prof. Me. Thiago de Menezes Ramos

1. Direito 2. Plataformas digitais
3. Responsabilidade civil 4. Proteção de dados
I. Título

CDU 34 (045)

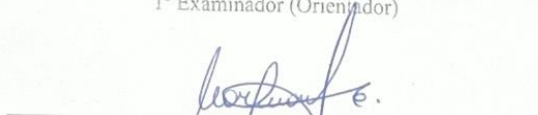
HILTON LINHARES NETO

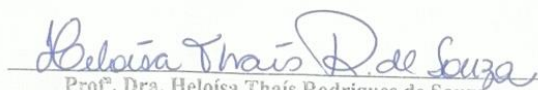
**RESPONSABILIDADE CIVIL DE PLATAFORMA DIGITAIS POR CONTEÚDOS
POSTADOS POR USUÁRIOS.**

Artigo Científico apresentado à Faculdade de Administração e Negócios de Sergipe - FANESE,
como requisito parcial e elemento obrigatório para a obtenção do grau bacharel em Direito no
período de 2025.2.

Aprovado (a) com média: 10,00


Prof. Me. Thiago de Menezes Ramos
1º Examinador (Orientador)


Prof. Me. Marluany Sales Guimarães
2º Examinadora


Prof. Dra. Heloísa Thaís Rodrigues de Souza
3º Examinadora

Aracaju, 04 de dezembro de 2025

Responsabilidade Civil de Plataformas Digitais por Conteúdos Postados por Usuários^{1*}

Hilton Linhares Neto

RESUMO

O presente estudo tem como objeto a responsabilidade civil das plataformas digitais por conteúdos postados por usuários, com enfoque na proteção de dados pessoais, privacidade e liberdade de expressão. O problema investigado consiste em compreender como o ordenamento jurídico brasileiro estabelece os limites da responsabilização civil das plataformas diante de conteúdos ilícitos, ofensivos ou falsos, e de que forma a jurisprudência do Superior Tribunal de Justiça contribui para a definição dessas responsabilidades. O objetivo geral da pesquisa foi analisar a responsabilidade civil das plataformas digitais considerando os direitos fundamentais dos usuários, enquanto os objetivos específicos envolveram: examinar os fundamentos da responsabilidade civil no contexto digital; avaliar a proteção de dados pessoais, a privacidade e a liberdade de expressão; e investigar a jurisprudência do STJ sobre a responsabilização por conteúdos de usuários. A metodologia adotada consistiu em pesquisa qualitativa, exploratória e bibliográfica, complementada pela análise de jurisprudência recente do STJ, considerando legislação aplicável, como o Código Civil, o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD). Os principais resultados indicam que a responsabilidade dos provedores de serviços digitais é, em regra, subjetiva, sendo acionada quando há notificação prévia sobre conteúdo ilícito e inércia injustificada na remoção da informação. A análise também evidenciou que a proteção de dados e a preservação da privacidade são princípios centrais na regulamentação das plataformas, que devem equilibrar a liberdade de expressão dos usuários com os direitos da personalidade de terceiros. Concluiu-se que a harmonização entre inovação tecnológica, liberdade de expressão e responsabilidade civil é possível, mas requer atuação diligente das plataformas, aplicação adequada das normas e constante atualização jurisprudencial. A pesquisa contribui para compreender os desafios jurídicos na governança digital e reforça a importância da responsabilidade civil como mecanismo de proteção de direitos fundamentais no ambiente online.

Palavras-chave: Liberdade de expressão; Plataformas digitais; Proteção de dados; Privacidade; Responsabilidade civil.

1 INTRODUÇÃO

A expansão das plataformas digitais transformou significativamente a forma como indivíduos se comunicam, compartilham informações e interagem socialmente. Com o crescimento das redes sociais, aplicativos de mensagens e serviços online, emergiram novos

^{1*} Artigo apresentado à banca examinadora do curso de Direito da Faculdade de Administração e Negócios de Sergipe, em Novembro de 2025, como critério parcial e obrigatório para a obtenção do título de Bacharel em Direito. Orientador: Prof. MSc. Thiago De Menezes Ramos

desafios jurídicos relacionados à proteção de direitos fundamentais, como a privacidade, a honra e a imagem dos usuários. Nesse contexto, o debate sobre a responsabilidade civil das plataformas torna-se central, sobretudo diante da proliferação de conteúdos ilícitos, ofensivos ou falsos.

O avanço tecnológico e a ampla utilização de serviços digitais revelam a necessidade de compreender como os provedores se inserem na cadeia de responsabilidades jurídicas. Conteúdos postados por terceiros podem causar danos significativos a indivíduos ou empresas, gerando repercussões sociais, econômicas e jurídicas. A complexidade dessa temática exige uma análise minuciosa, considerando não apenas os aspectos legais, mas também os impactos práticos da atuação das plataformas digitais e o papel das normas protetivas, como o Marco Civil da Internet e a LGPD.

Além disso, a globalização da internet impõe desafios adicionais ao ordenamento jurídico brasileiro, que precisa conciliar liberdade de expressão e proteção da privacidade. Questões envolvendo fake news, violação de dados pessoais e difamação demandam medidas eficazes de responsabilização, sem, entretanto, comprometer direitos fundamentais. Nesse cenário, a atuação do Superior Tribunal de Justiça (STJ) se torna relevante, uma vez que suas decisões ajudam a definir parâmetros para a responsabilidade civil das plataformas digitais.

A relevância desta pesquisa se justifica pelo impacto crescente das interações digitais na vida cotidiana e pelo aumento de casos em que usuários têm seus direitos violados em ambientes online. Compreender a forma como o direito brasileiro regula a responsabilidade das plataformas, especialmente diante de conteúdos ofensivos ou ilegais, é essencial para aprimorar a proteção jurídica e orientar políticas de governança digital, além de fortalecer a segurança e a confiança dos usuários.

O objetivo geral deste estudo é analisar a responsabilidade civil das plataformas digitais por conteúdos postados por usuários, considerando a proteção de dados pessoais, a privacidade e a liberdade de expressão. Os objetivos específicos, são: Conceituar a responsabilidade civil no contexto digital; Dissertar sobre a Proteção de dados pessoais, privacidade e liberdade de expressão; Analisar a Jurisprudência do STJ e a responsabilização civil por conteúdos de usuários.

Diante do exposto, a problemática desta pesquisa pode ser formulada da seguinte maneira: como o ordenamento jurídico brasileiro estabelece a responsabilização civil das plataformas digitais por conteúdos postados por usuários, conciliando proteção de dados pessoais, liberdade de expressão e prevenção de danos à imagem e à honra de indivíduos, e de

que forma a jurisprudência do STJ têm contribuído para definir os limites e as responsabilidades dessas plataformas?

A metodologia adotada consiste em uma pesquisa qualitativa e exploratória, baseada em revisão bibliográfica e análise de jurisprudência recente do STJ. Serão examinadas obras doutrinárias, artigos científicos e legislação pertinente, como o Código Civil, o Marco Civil da Internet e a Lei Geral de Proteção de Dados, com o objetivo de compreender os fundamentos legais e a aplicação prática da responsabilidade civil das plataformas digitais no Brasil.

A presente pesquisa inicia-se com uma introdução, na qual se delimitam o problema, a relevância, os objetivos e o método adotado, e, na sequência, desenvolve-se o Capítulo 2, dedicado aos fundamentos da responsabilidade civil no contexto digital, abrangendo o conceito e a natureza da responsabilidade das plataformas (2.1) e os parâmetros normativos do Marco Civil da Internet (2.2); o Capítulo 3 aprofunda a proteção de dados pessoais, a privacidade e a liberdade de expressão, examinando a LGPD e o dever de proteção nas plataformas digitais (3.1) e a tensão entre liberdade de expressão e tutela da privacidade (3.2); o Capítulo 4 analisa a jurisprudência do STJ sobre responsabilização por conteúdos de usuários, com foco nos casos de conteúdos ofensivos (4.1) e nos desafios relativos a dados pessoais, fake news e à atuação das plataformas (4.2); por fim, o Capítulo 5 apresenta as considerações finais, sintetizando os achados e apontando os critérios jurídico-interpretativos que balizam a responsabilização civil das plataformas digitais no ordenamento brasileiro.

2 FUNDAMENTOS DA RESPONSABILIDADE CIVIL NO CONTEXTO DIGITAL

O avanço das tecnologias digitais e a popularização das plataformas online transformaram significativamente as relações sociais e comerciais, criando novos desafios para o Direito, especialmente no campo da responsabilidade civil. A dinâmica das interações virtuais, marcada pela velocidade da informação e pela ampla disseminação de conteúdos, exige uma análise jurídica capaz de equilibrar a proteção de direitos individuais e coletivos com a liberdade de atuação das plataformas digitais. Nesse contexto, torna-se necessário compreender os fundamentos que orientam a responsabilização civil dessas empresas frente aos conteúdos produzidos por terceiros.

Segundo Nunes e Lehfeld (2018), a responsabilidade civil no ambiente digital não se limita à reparação de danos tradicionais, mas envolve questões relacionadas à mediação de conflitos, à prevenção de abusos e à tutela de direitos fundamentais, como a privacidade, a

honra e a liberdade de expressão. A atuação das plataformas digitais, muitas vezes classificadas como intermediárias, suscita debates acerca da extensão de sua responsabilidade, sobretudo diante de conteúdos ilícitos, falsos ou ofensivos.

Além disso, Almeida, Sombra e Azevedo (2025) destacam que as plataformas digitais devem observar não apenas a legislação civil tradicional, mas também normas específicas do Direito do Consumidor e do Direito Digital, considerando os impactos econômicos e sociais de suas ações. A compreensão desses fundamentos é essencial para estabelecer parâmetros claros sobre os deveres e limites das plataformas, bem como para garantir a proteção dos usuários e terceiros em um ambiente digital cada vez mais complexo.

Essa seção se estrutura, portanto, em dois subcapítulos: o primeiro abordará o conceito e a natureza da responsabilidade civil das plataformas digitais, enquanto o segundo analisará os parâmetros normativos estabelecidos pelo Marco Civil da Internet, com o objetivo de contextualizar o ordenamento jurídico brasileiro frente aos desafios impostos pelo meio digital.

1.1 Conceito e natureza da responsabilidade civil das plataformas digitais

Inicialmente, é importante destacar que a responsabilidade civil está prevista no Livro I da Parte Especial do Código Civil, dentro da disciplina das obrigações. A matéria encontra-se regulada no Título IX, Capítulos I e II, sob as denominações “Da obrigação de indenizar” e “Da indenização”, abrangendo os artigos 927 a 954. No Código Civil de 1916, também era tratada no âmbito do direito das obrigações, situado no Livro III da Parte Especial, nos Títulos VII e VIII, Capítulos I e II, sob os títulos “Das obrigações por atos ilícitos” e “Da liquidação das obrigações”, entre os artigos 1.518 e 1.553. No atual Código, a liquidação deixou de constar, por se tratar de tema de natureza eminentemente processual.

O conceito de culpa, ato ilícito e responsabilidade subjetiva e objetiva é descrito por Rizzardo (2019, p. 77):

Sabe-se que a culpa no sentido estrito equivale à ação ou omissão involuntária que causa danos, e que se dá por negligência ou imprudência, no que se expande em sentidos equivalentes, como descuido, imperícia, distração, indolência, desatenção e levandade. No sentido lato, abrange o dolo, isto é, a ação ou omissão voluntária, pretendida, procurada, almejada, que também traz danos. Em ambas as dimensões, desrespeita-se a ordem legal estabelecida pelo direito positivo. Pelos prejuízos ou danos que decorrem das condutas acima, a pessoa responde, isto é, torna-se responsável, ou deve arcar com os resultados ou as consequências. A ação humana evitada de tais máculas, isto é, de culpa no sentido estrito ou lato denomina-se ‘ato ilícito’, porque afronta a ordem jurídica, ou desrespeita o que está implantado pela lei. E a responsabilidade consiste na obrigação de sanar, ou recompor, ou ressarcir os males e prejuízos que decorrem de mencionadas ações.

Diante do exposto, pode-se afirmar que a responsabilidade civil continua tendo como base principal a culpa, ainda que a responsabilidade objetiva tenha ganhado relevância e espaço no ordenamento jurídico atual.

Sabe-se que a culpa no sentido estrito equivale à ação ou omissão involuntária que causa danos, e que se dá por negligência ou imprudência, no que se expande em sentidos equivalentes, como descuido, imperícia, distração, indolência, desatenção e leviandade. No sentido lato, abrange o dolo, isto é, a ação ou omissão voluntária, pretendida, procurada, almejada, que também traz danos. Em ambas as dimensões, desrespeita-se a ordem legal estabelecida pelo direito positivo. Pelos prejuízos ou danos que decorrem das condutas acima, a pessoa responde, isto é, torna-se responsável, ou deve arcar com os resultados ou as consequências. A ação humana evitada de tais máculas, isto é, de culpa no sentido estrito ou lato

A responsabilidade civil, em sua concepção clássica, é compreendida como o dever de reparar o dano causado a outrem em virtude de um ato ilícito, seja ele doloso ou culposos. Rizzardo (2019) enfatiza que a função primordial da responsabilidade é a recomposição do equilíbrio jurídico rompido, restaurando, na medida do possível, a situação anterior à lesão. Esse conceito, consolidado no direito civil tradicional, serve de base para as novas discussões no ambiente digital, onde as plataformas assumem papel central na intermediação de relações.

Foi incorporada de forma mais evidente no Código Civil de 2002, cuja norma central encontra-se prevista no parágrafo único do artigo 927, que estabelece: “Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem”. Seu surgimento decorreu de uma exigência imposta pelas circunstâncias da própria vida.

A adaptação da Teoria da Responsabilidade Civil Subjetiva ao contexto das plataformas digitais de intermediação mostra-se complexa e repleta de obstáculos. Ainda que o Código Civil, em regra, não condicione a reparação de danos à prova de culpa, a diversidade de funções e o modelo econômico dessas empresas tornam muitas vezes difícil a comprovação de uma conduta culposa. Trata-se, nesse cenário, de averiguar eventual negligência, imprudência ou imperícia da plataforma intermediadora diante dos prejuízos ocasionados por prestadores de serviços autônomos que utilizam sua infraestrutura tecnológica.

No ambiente virtual, a responsabilidade civil adquire contornos peculiares, pois não se trata apenas da ação direta de um indivíduo, mas da disponibilização de espaços digitais em que milhões de usuários podem publicar e compartilhar conteúdos. Como observa Melo (2025), o

avanço tecnológico exige uma releitura da teoria da responsabilidade, adaptando-a às novas formas de ilicitude que emergem em rede, como a divulgação de informações falsas, o discurso de ódio e a exposição indevida de dados pessoais.

As plataformas digitais se posicionam como intermediárias, oferecendo infraestrutura para comunicação e troca de informações. Entretanto, a grande questão está em determinar até que ponto podem ser responsabilizadas pelos danos causados por terceiros que utilizam seus serviços. Gagliano e Pamplona Filho (2020) ressaltam que a responsabilidade civil não pode ser aplicada de forma mecânica; é necessário observar a natureza da atividade desempenhada e a posição ocupada pelo agente no ciclo do dano.

A natureza jurídica da responsabilidade civil das plataformas digitais, portanto, oscila entre a responsabilidade subjetiva e objetiva, dependendo do caso concreto. Rizzardo (2019) lembra que, em regra, a responsabilidade subjetiva exige a comprovação de culpa ou dolo, mas em determinadas hipóteses a lei impõe a responsabilidade objetiva, bastando a demonstração do dano e do nexo causal. No ambiente digital, o legislador e a jurisprudência têm buscado um equilíbrio entre esses dois modelos.

No Brasil, o Marco Civil da Internet (Lei nº 12.965/2014) estabeleceu que a responsabilidade civil das plataformas por conteúdos gerados por usuários depende, em regra, da não remoção de material considerado ilícito após ordem judicial. Essa previsão reforça a ideia de que não há responsabilidade automática ou objetiva. Melo (2025) observa que essa solução busca proteger a liberdade de expressão, mas não isenta as plataformas de um dever de cuidado mínimo diante de situações manifestamente ilícitas.

O conceito de responsabilidade civil aplicado às plataformas digitais deve considerar não apenas os danos materiais, mas também os danos morais e coletivos. Gagliano e Pamplona Filho (2020) destacam que a expansão da responsabilidade civil contemporânea abrange a tutela da dignidade da pessoa humana, núcleo central do sistema constitucional brasileiro. Assim, conteúdos ofensivos, discriminatórios ou que atentem contra a honra podem ensejar reparação.

Outro aspecto relevante é a função social desempenhada pelas plataformas. Rizzardo (2019) explica que a responsabilidade civil também possui caráter pedagógico e preventivo, servindo como instrumento de desestímulo a práticas nocivas. Ao se aplicar esse raciocínio ao ambiente digital, pode-se defender que as plataformas, ao desenvolverem políticas de moderação e mecanismos de denúncia, cumprem não apenas um dever contratual, mas também uma função social voltada à proteção de direitos fundamentais.

A natureza da responsabilidade civil das plataformas digitais, portanto, não pode ser reduzida a um modelo único. Em alguns casos, a responsabilidade é subjetiva, vinculada à

omissão diante de ordem judicial; em outros, pode se aproximar da objetiva, quando se trata de danos derivados de falhas no sistema de segurança ou no tratamento de dados pessoais. Melo (2025) adverte que a elasticidade da responsabilidade civil não deve comprometer a segurança jurídica, devendo haver critérios claros para sua aplicação.

Sob essa ótica, a teoria do risco surge como elemento importante. Gagliano e Pamplona Filho (2020) ressaltam que aquele que exerce atividade de risco, potencialmente danosa à coletividade, deve arcar com as consequências dos prejuízos gerados. As plataformas digitais, pela amplitude de sua atuação e pelo impacto social de seus serviços, podem ser enquadradas nessa lógica em determinadas situações, especialmente quando falham em impedir a propagação de ilícitos.

Contudo, a aplicação irrestrita da responsabilidade objetiva às plataformas encontra críticas, pois poderia inviabilizar a livre circulação de informações e sobrecarregar os provedores de internet com ônus excessivo. Rizzardo (2019) argumenta que a função do direito civil é harmonizar interesses, evitando tanto a impunidade dos agentes quanto o desestímulo às atividades econômicas essenciais. Essa ponderação é fundamental para o desenvolvimento de soluções equilibradas.

O conceito de responsabilidade civil digital também deve ser analisado sob a perspectiva da confiança legítima dos usuários. Melo (2025) observa que as plataformas se apresentam como ambientes seguros e de fácil utilização, o que cria expectativas de proteção contra abusos. Quando essa confiança é quebrada, surge um dever de reparação, ainda que não decorrente diretamente de ato ilícito próprio, mas de omissão em garantir condições mínimas de segurança e privacidade.

Ademais, a multiplicidade de danos possíveis no ambiente digital exige um alargamento da noção de responsabilidade. Gagliano e Pamplona Filho (2020) sustentam que a responsabilidade civil moderna deve abranger não apenas o ressarcimento individual, mas também a proteção de bens coletivos e difusos. Dessa forma, casos de vazamentos massivos de dados, que afetam milhares de pessoas, exemplificam a necessidade de um modelo mais abrangente de tutela.

A responsabilidade civil das plataformas digitais, portanto, deve ser entendida como uma categoria híbrida, que mescla institutos clássicos do direito civil com elementos próprios do direito digital. Rizzardo (2019) sublinha que a evolução da responsabilidade civil acompanha as transformações sociais, ajustando-se às novas formas de lesão. No contexto atual, isso significa repensar categorias tradicionais, como culpa e nexo causal, à luz das especificidades tecnológicas.

No campo normativo, as plataformas digitais enfrentam um duplo desafio: atender às exigências legais nacionais, como o Marco Civil da Internet, e às obrigações transnacionais, como as regras de proteção de dados pessoais. Melo (2025) observa que essa pluralidade de fontes jurídicas aumenta a complexidade da responsabilização, tornando indispensável uma análise casuística para definir os limites do dever de reparação.

Em síntese, o conceito e a natureza da responsabilidade civil das plataformas digitais não podem ser compreendidos apenas sob a ótica da responsabilidade subjetiva tradicional. Trata-se de uma categoria em construção, que busca equilibrar direitos fundamentais, interesses econômicos e a função social da tecnologia. Como afirmam Gagliano e Pamplona Filho (2020), a responsabilidade civil contemporânea é dinâmica e adaptativa, refletindo os novos riscos e desafios impostos pela sociedade digital.

2.2 Marco Civil da Internet e os parâmetros normativos

O Marco Civil da Internet tem início afirmando que nele são fixados os princípios, garantias, direitos e deveres relacionados ao uso da internet no Brasil. Contudo, tal previsão revela uma falha de técnica legislativa, por destoar do próprio sistema jurídico em que está inserida. A definição de princípios, garantias, direitos e deveres cabe, em verdade, à Constituição Federal, enquanto o Marco Civil, como norma infraconstitucional, deveria apenas regulamentar e concretizar tais disposições constitucionais. Entretanto, o que se observa é que o texto legal repete, de forma descontextualizada, dispositivos constitucionais, sem avançar na análise dos problemas específicos ligados às tecnologias de informação e comunicação.

O Marco Civil da Internet, instituído pela Lei nº 12.965/2014, consolidou-se como o principal marco regulatório do uso da internet no Brasil. Conhecido como a “Constituição da Internet”, estabelece princípios, direitos e deveres para usuários, provedores e plataformas digitais. Segundo Gonçalves (2017), a lei representou uma inovação legislativa ao colocar no centro do debate valores como liberdade de expressão, proteção da privacidade e neutralidade da rede, equilibrando interesses públicos e privados.

Um dos pilares do Marco Civil é a garantia da neutralidade da rede, que obriga os provedores a tratar de forma isonômica os pacotes de dados, sem discriminação por conteúdo, origem, destino ou aplicação. Marques *et al.* (2024) destacam que esse princípio assegura a livre circulação de informações, protegendo o usuário de práticas abusivas como a priorização de determinados serviços. Tal garantia, contudo, enfrenta desafios diante das pressões econômicas e tecnológicas que buscam flexibilizar sua aplicação.

Outro aspecto fundamental da legislação é a proteção da privacidade e dos dados pessoais. Embora a LGPD (Lei nº 13.709/2018) tenha aprofundado esse tema, o Marco Civil já previa regras de coleta, uso, armazenamento e compartilhamento de dados. Para Gonçalves (2017), essa preocupação foi pioneira, antecipando discussões que se tornaram centrais anos depois, especialmente diante da massificação das redes sociais e do uso comercial das informações dos usuários.

No que se refere à responsabilidade civil, o Marco Civil estabeleceu critérios específicos para as plataformas digitais. O artigo 19 determina que provedores de aplicações só poderão ser responsabilizados por conteúdos de terceiros caso descumpram ordem judicial para sua remoção. Marques et al. (2024) observam que esse modelo busca evitar a censura prévia e preservar a liberdade de expressão, transferindo ao Poder Judiciário a competência de decidir sobre a ilicitude de um conteúdo.

Essa sistemática, entretanto, não é absoluta. O próprio Marco Civil prevê exceções, como nos casos de conteúdos relacionados à violação de direitos autorais e materiais de nudez ou pornografia não consentida, em que a exclusão pode ser exigida sem ordem judicial. Gonçalves (2017) explica que essas exceções refletem o esforço do legislador em proteger a dignidade da pessoa humana, especialmente em situações que configuram danos graves e imediatos à vítima.

O Marco Civil também trouxe parâmetros para a guarda de registros de conexão e de acesso a aplicações. O artigo 15 obriga provedores a manter esses registros, de forma sigilosa, pelo prazo de seis meses, garantindo que possam ser utilizados em investigações judiciais. Para Marques *et al.* (2024), essa medida equilibra a necessidade de segurança pública e persecução penal com a proteção da privacidade, uma vez que o acesso só pode ocorrer mediante ordem judicial.

Do ponto de vista normativo, o Marco Civil reafirma o princípio da finalidade, estabelecendo que os dados coletados pelas plataformas devem ser utilizados apenas para os fins autorizados pelo usuário. Gonçalves (2017) ressalta que tal previsão impõe limites importantes às práticas comerciais das empresas digitais, evitando abusos relacionados ao marketing direcionado e à exploração indiscriminada de informações pessoais.

A lei também reforça a ideia de que a internet deve ser um ambiente de promoção da cidadania e do desenvolvimento humano. Marques *et al.* (2024) lembram que, ao completar dez anos de vigência, o Marco Civil demonstrou ser um instrumento essencial para a inclusão digital e a garantia de direitos fundamentais no espaço virtual. Ainda assim, persistem desafios

relacionados à sua efetividade diante da rápida evolução tecnológica e das novas formas de interação social online.

Outro ponto relevante é a cooperação internacional. Como a internet não possui fronteiras, o Marco Civil prevê mecanismos de cooperação com autoridades estrangeiras para a investigação de crimes e a proteção de usuários. Gonçalves (2017) enfatiza que a aplicação prática desse dispositivo ainda enfrenta obstáculos, sobretudo em razão das diferenças legislativas entre países e da resistência de grandes empresas multinacionais em se submeterem às normas nacionais.

Por fim, pode-se afirmar que o Marco Civil da Internet representa um avanço significativo no ordenamento jurídico brasileiro, estabelecendo parâmetros normativos sólidos para a regulação do ambiente digital. No entanto, como destacam Marques *et al.* (2024), seu futuro depende da constante atualização interpretativa, de modo a lidar com novos fenômenos, como a inteligência artificial, a desinformação em massa e os desafios da proteção de dados. Trata-se de um marco em permanente construção, que exige diálogo entre legisladores, juristas, sociedade civil e as próprias plataformas digitais.

3 PROTEÇÃO DE DADOS PESSOAIS, PRIVACIDADE E LIBERDADE DE EXPRESSÃO

A crescente digitalização das relações sociais, econômicas e jurídicas trouxe à tona relevantes debates sobre a tutela da privacidade, a proteção de dados pessoais e os limites da liberdade de expressão. Com o avanço das plataformas digitais (CHIARINI *et al.*, 2023), tornou-se inevitável refletir sobre os riscos da coleta, tratamento e compartilhamento de informações sensíveis, em especial diante do volume massivo de dados que circulam diariamente na internet. Nesse cenário, emergem conflitos entre direitos fundamentais, exigindo do ordenamento jurídico mecanismos capazes de harmonizar interesses individuais e coletivos.

A promulgação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) representa um marco nesse processo, ao estabelecer normas específicas para disciplinar a forma como dados pessoais devem ser tratados pelas plataformas digitais (Maldonado, 2019). O diploma legal impõe deveres às empresas de tecnologia, reforçando princípios como a transparência, a finalidade e a segurança da informação, ao mesmo tempo em que reconhece os direitos dos titulares dos dados. A LGPD, portanto, configura um avanço normativo na tentativa de equilibrar inovação tecnológica e proteção da dignidade humana.

Por outro lado, a questão da liberdade de expressão, assegurada pela Constituição Federal de 1988, precisa ser analisada em paralelo com a garantia da privacidade. Nas plataformas digitais, esse embate ganha contornos delicados, pois a manifestação do pensamento pode, muitas vezes, entrar em colisão com o direito de não ter sua intimidade e seus dados expostos ou utilizados de maneira abusiva. O desafio jurídico contemporâneo consiste em compatibilizar tais direitos, evitando tanto a censura quanto a violação indevida da esfera privada dos indivíduos.

Dessa forma, a presente seção busca examinar os fundamentos da proteção de dados pessoais e da privacidade no contexto digital, à luz da LGPD, bem como discutir as tensões existentes entre esse direito e a liberdade de expressão, propondo uma reflexão crítica sobre os caminhos adotados pelo direito brasileiro para enfrentar tais dilemas.

3.1 A LGPD e o dever de proteção de dados nas plataformas digitais

A promulgação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) representou um marco regulatório no ordenamento jurídico brasileiro, ao estabelecer parâmetros claros sobre coleta, tratamento, armazenamento e compartilhamento de informações pessoais no ambiente digital. Seu objetivo central é garantir a proteção dos direitos fundamentais de liberdade e privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2024). No contexto das plataformas digitais, a LGPD assume papel essencial, visto que estas atuam como mediadoras de vasto fluxo de dados sensíveis.

O ambiente digital se consolidou como espaço de interação, consumo e produção de informação, exigindo maior responsabilidade por parte das empresas de tecnologia. Segundo Doneda (2021), a proteção de dados não pode ser vista apenas como uma questão técnica ou de segurança, mas como dimensão essencial dos direitos fundamentais. Assim, as plataformas digitais devem estruturar políticas transparentes e mecanismos de controle que possibilitem aos usuários exercer efetivamente sua autodeterminação informativa.

O princípio do consentimento informado é um dos pilares da LGPD. Bioni (2019) destaca que o consentimento deve ser livre, informado e inequívoco, o que significa que não pode ser obtido de forma genérica ou por meio de cláusulas obscuras nos termos de uso. Essa exigência impõe às plataformas digitais o dever de redigir comunicações claras e acessíveis, eliminando a prática de autorizações implícitas ou camufladas em longos contratos de adesão.

Contudo, o consentimento, embora relevante, não é o único fundamento da proteção de dados. Fernandes e Nuzzi (2022) lembram que a LGPD também prevê outras bases legais para

o tratamento, como o cumprimento de obrigação legal, a execução de contrato ou o legítimo interesse do controlador. Isso demonstra que a lei busca equilibrar a autonomia do usuário com a necessidade prática das plataformas em gerenciar grandes volumes de dados para viabilizar seus serviços.

A LGPD brasileira adota uma disciplina próxima àquela prevista pela legislação europeia no que se refere aos dados pessoais sensíveis, ainda que o regime europeu imponha restrições mais rigorosas, em razão da busca por uma proteção mais efetiva dos direitos fundamentais e da liberdade individual.

O tratamento de dados pessoais sensíveis possui bases legais, embora semelhantes, diferentes do tratamento dos dados pessoais comuns. O consentimento para essa categoria especial também é diferente, porquanto deve ser de forma específica e destacada, sem prejuízo dos requisitos gerais para o consentimento (Maciel, 2019, p.37).

A Lei Geral de Proteção de Dados, em seu artigo 5º, incisos VI a IX, define os principais sujeitos envolvidos no tratamento de dados pessoais, que incluem o controlador e o operador. Além deles, a legislação também introduz a figura do encarregado, função inspirada no modelo europeu do GDPR (MATTOS *et al.*, 2019; LIMA, 2020).

Assim, a LGPD prevê quatro atores principais: o titular dos dados, o controlador, o operador e o encarregado. O titular corresponde a toda pessoa natural cujas informações sejam objeto de tratamento. Já o controlador e o operador, que podem ser tanto pessoas físicas quanto jurídicas, são responsáveis pelo tratamento: ao controlador cabe a tomada de decisões sobre as finalidades e meios de tratamento, enquanto ao operador compete a execução dessas atividades (SAID, 2020).

A LGPD define como papéis principais: Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Encarregado de dados: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da lei em todo o território nacional (Garcia, 2020, p.18).

Nesse contexto, a figura do controlador é responsável por tomar as principais decisões relacionadas ao tratamento de dados pessoais, enquanto ao operador cabe a execução prática desse tratamento conforme as diretrizes estabelecidas. O controlador define a finalidade da

coleta, os meios a serem utilizados, o tipo de dado que será tratado, o público-alvo da coleta, o período de armazenamento e os níveis de acesso autorizados. Por concentrar essas decisões, recai sobre ele a maior parte das responsabilidades previstas pela LGPD, incluindo a proteção dos dados e a adoção de medidas que assegurem os direitos dos titulares.

O operador, por sua vez, atua na execução das tarefas determinadas pelo controlador, limitando-se ao processamento dos dados conforme as finalidades previamente estabelecidas. Apesar de seguir as instruções do controlador, o operador possui autonomia técnica para definir os sistemas, métodos e ferramentas a serem utilizados no tratamento, abrangendo desde a coleta e armazenamento até a transferência e recuperação das informações. Ele deve zelar pela segurança dos dados em todas as etapas, sob pena de responder solidariamente pelos danos eventualmente causados aos titulares. Dessa forma, tanto controlador quanto operador podem ser responsabilizados pelos prejuízos decorrentes da atividade de tratamento, conforme dispõe a LGPD.

O dever de segurança também ocupa posição de destaque. Conforme dispõe o art. 46 da LGPD, os controladores e operadores devem adotar medidas técnicas e administrativas capazes de proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração e comunicação (Brasil, 2024). Para as plataformas digitais, isso se traduz em investimentos contínuos em tecnologia de criptografia, protocolos de segurança e governança corporativa em proteção de dados.

Nesse ponto, Manzato, Soares e Cugula (2024) enfatizam que a tutela dos direitos da personalidade nos contratos digitais é diretamente impactada pela forma como as plataformas tratam dados pessoais. Uma gestão inadequada pode acarretar danos morais e materiais, gerando o dever de indenizar. Dessa forma, a responsabilidade civil das plataformas está intrinsecamente ligada à observância dos princípios e regras da LGPD.

Outro aspecto relevante é a transparência. A LGPD determina que os titulares de dados tenham acesso facilitado a informações sobre o tratamento realizado, incluindo a finalidade, a forma e a duração do processamento. Segundo Fernandes e Nuzzi (2022), a transparência é condição essencial para que o titular exerça seus direitos de acesso, correção, portabilidade e eliminação de dados. Portanto, as plataformas digitais precisam criar canais eficazes de comunicação com os usuários.

A legislação também prevê mecanismos de responsabilização em caso de descumprimento. O art. 52 da LGPD estabelece sanções administrativas que vão desde advertências até multas de até 2% do faturamento da empresa, limitadas a cinquenta milhões

de reais por infração (Brasil, 2024). Tais penalidades reforçam o caráter coercitivo da norma e buscam estimular uma cultura de conformidade nas organizações digitais.

O impacto da LGPD nas plataformas digitais também se reflete na governança interna. Doneda (2021) aponta que a lei exige a criação de programas estruturados de proteção de dados, com a designação de encarregado (DPO – *Data Protection Officer*) responsável por interagir com os titulares e com a Autoridade Nacional de Proteção de Dados (ANPD). Esse mecanismo fortalece a *accountability* das empresas e cria uma ponte entre a sociedade civil e as corporações.

Além disso, a lei reforça a importância do princípio da minimização. Bioni (2019) explica que as plataformas devem coletar apenas os dados estritamente necessários para a finalidade declarada, evitando práticas abusivas de coleta massiva. Esse princípio se contrapõe ao modelo tradicional de exploração de dados, baseado na acumulação indiscriminada de informações para fins comerciais e de marketing.

A discussão sobre o dever de proteção de dados envolve, também, a perspectiva contratual. Manzato, Soares e Cugula (2024) assinalam que, nos contratos digitais, a proteção de dados pessoais deve ser considerada cláusula essencial, visto que está diretamente relacionada à dignidade e aos direitos da personalidade do contratante. O descumprimento desse dever pode configurar vício contratual e ensejar reparação.

A LGPD ainda consagra o direito à portabilidade dos dados, permitindo ao usuário transferir suas informações de uma plataforma para outra, sempre que tecnicamente viável (Brasil, 2024). Fernandes e Nuzzi (2022) entendem que essa medida promove maior concorrência entre as empresas digitais e amplia o poder de escolha do consumidor, reforçando a soberania informacional do titular.

Não se pode ignorar que o cumprimento da LGPD traz desafios técnicos e financeiros para as plataformas digitais, especialmente as de pequeno e médio porte. Doneda (2021) destaca que a adaptação requer investimentos em infraestrutura e treinamento de pessoal, mas tais custos são necessários para garantir a conformidade e evitar riscos reputacionais e jurídicos.

A lei também estabelece regras específicas para o tratamento de dados sensíveis, como origem racial, convicção religiosa, opinião política ou dados de saúde. O art. 11 da LGPD restringe severamente o uso dessas informações, exigindo consentimento expresso ou hipóteses legais excepcionais (Brasil, 2024). Bioni (2019) salienta que a proteção reforçada desses dados visa prevenir práticas discriminatórias no ambiente digital.

Outro elemento fundamental é a atuação da ANPD, órgão responsável por fiscalizar e regulamentar a aplicação da LGPD. Fernandes e Nuzzi (2022) ressaltam que a autoridade

exerce papel pedagógico e sancionatório, orientando empresas e cidadãos quanto às boas práticas em proteção de dados. Sua efetividade é condição essencial para consolidar a cultura de proteção no Brasil.

A internacionalização dos fluxos de dados é outro ponto de atenção. Plataformas digitais frequentemente transferem informações para servidores localizados em outros países. A LGPD, em seus arts. 33 a 36, estabelece requisitos rigorosos para a transferência internacional, exigindo garantias adequadas de proteção (Brasil, 2024). Doneda (2021) argumenta que essa previsão reforça a soberania nacional e protege os cidadãos de regimes jurídicos menos protetivos.

A responsabilização civil decorrente de incidentes de segurança também merece destaque. Manzato, Soares e Cugula (2024) observam que falhas como vazamento de dados ou ataques cibernéticos podem gerar danos coletivos, exigindo reparação ampla. Nesse cenário, a LGPD serve como parâmetro normativo para balizar a responsabilidade das plataformas e dos provedores de serviços digitais.

É importante considerar, ainda, o impacto da LGPD na relação de confiança entre usuários e plataformas. Fernandes e Nuzzi (2022) afirmam que o respeito à privacidade e aos direitos de dados fortalece a credibilidade das empresas, aumentando a adesão e fidelidade dos consumidores. Assim, a conformidade legal não é apenas obrigação, mas também vantagem competitiva no mercado digital.

Ao estabelecer padrões mínimos de governança e segurança, a LGPD promove um alinhamento do Brasil com outras legislações internacionais, como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR). Bioni (2019) observa que essa aproximação facilita o intercâmbio global e torna o mercado brasileiro mais atrativo para investimentos internacionais.

Por fim, a LGPD representa um avanço no reconhecimento da proteção de dados como direito fundamental, impondo às plataformas digitais o dever de respeitar a privacidade e a autodeterminação informativa dos usuários. Como enfatiza Doneda (2021), o desafio atual não é apenas jurídico, mas também cultural, demandando mudanças profundas na forma como a sociedade lida com informações pessoais. Assim, a efetividade da lei depende tanto da atuação estatal quanto da conscientização coletiva sobre a centralidade dos dados na era digital.

3.2 Liberdade de expressão *versus* proteção da privacidade

A relação entre liberdade de expressão e proteção da privacidade constitui um dos dilemas centrais do direito digital. Ambos são direitos fundamentais consagrados

constitucionalmente, mas que, em diversas situações, se apresentam em tensão. Como destacam Diniz *et al.* (2025), o ambiente digital ampliou exponencialmente as possibilidades de comunicação, mas também potencializou riscos de violação da privacidade, exigindo que o Poder Judiciário equilibre esses direitos de forma proporcional e razoável, evitando tanto censura quanto exposição abusiva de dados pessoais.

Nesse cenário, a LGPD desempenha papel relevante ao reforçar mecanismos de proteção da privacidade no tratamento de informações pessoais. Contudo, é necessário que tais medidas não impliquem em restrição indevida da liberdade de expressão. Para Siqueira e Fachin (2022), a legislação brasileira deve ser interpretada em consonância com a Constituição, garantindo que a tutela da privacidade não se converta em obstáculo à livre manifestação do pensamento, especialmente em plataformas digitais, onde a circulação de ideias constitui elemento essencial da democracia.

A jurisprudência brasileira, em especial do Superior Tribunal de Justiça (STJ), tem enfrentado casos em que esses direitos colidem, como em situações de remoção de conteúdos ofensivos ou na responsabilização de plataformas por publicações de terceiros. Conforme ressaltam Diniz *et al.* (2025), os tribunais têm buscado adotar a técnica da ponderação, reconhecendo que nenhum dos direitos é absoluto e que a solução depende da análise do caso concreto, considerando tanto a relevância da manifestação quanto a extensão da violação à intimidade.

O grande desafio reside na delimitação do que constitui abuso da liberdade de expressão. Siqueira e Fachin (2022) argumentam que a proteção da privacidade deve ser vista como instrumento de preservação da dignidade da pessoa humana, e não como mecanismo de supressão da crítica ou da circulação de informações de interesse público. Nesse sentido, cabe ao Judiciário diferenciar manifestações legítimas de opiniões das práticas ilícitas, como discurso de ódio, exposição indevida de dados sensíveis ou ataques à honra.

Portanto, a harmonização entre liberdade de expressão e privacidade no ambiente digital exige uma abordagem jurídica que valorize ambos os direitos em sua dimensão social e individual. Diniz *et al.* (2025) apontam que a solução passa pela aplicação de critérios de proporcionalidade e pela consolidação de uma cultura de responsabilidade digital. Assim, não se trata de privilegiar um direito em detrimento do outro, mas de buscar uma convivência equilibrada, capaz de proteger tanto a esfera pessoal quanto o espaço democrático de debate.

4 A JURISPRUDÊNCIA DO STJ E A RESPONSABILIDADE CIVIL POR

CONTEÚDOS DE USUÁRIOS

O avanço das tecnologias digitais e a expansão das plataformas de compartilhamento de informações trouxeram novos desafios ao Direito, especialmente no que se refere à responsabilização civil por conteúdos produzidos e divulgados por usuários. Nesse contexto, o Superior Tribunal de Justiça (STJ) tem desempenhado papel fundamental na interpretação e aplicação das normas jurídicas que buscam equilibrar a liberdade de expressão com a proteção da honra, da imagem, da privacidade e dos dados pessoais. A jurisprudência da Corte vem consolidando parâmetros importantes para delimitar a responsabilidade de provedores e usuários no ambiente digital.

A análise dos precedentes revela que a Corte tem buscado evitar tanto a imposição de uma censura prévia quanto a omissão diante de danos causados por manifestações abusivas. Em casos envolvendo conteúdos ofensivos, observa-se a construção de critérios para aferir quando e em que medida os provedores de internet devem ser responsabilizados pelos danos gerados, especialmente diante de pedidos de retirada de publicações.

Além disso, a questão dos dados pessoais e a disseminação de notícias falsas (*fake news*) ampliam ainda mais a complexidade da discussão. O STJ tem reconhecido que as plataformas digitais não podem se eximir completamente de sua função social, sendo necessário estabelecer mecanismos de controle e de atuação eficaz para coibir violações aos direitos fundamentais, sem comprometer a livre circulação de informações.

Essa seção, portanto, buscará examinar de forma detalhada dois aspectos centrais da jurisprudência do STJ sobre o tema: os casos de responsabilização civil por conteúdos ofensivos, nos quais a Corte delinea limites para a atuação das plataformas frente a manifestações abusivas; e a relação entre dados pessoais, *fake news* e a responsabilidade das plataformas, que envolve diretamente a proteção da privacidade, da honra e da integridade informacional no ambiente digital.

4.1 Casos de responsabilização civil por conteúdos ofensivos

A discussão sobre a responsabilização civil por conteúdos ofensivos publicados em plataformas digitais tem ocupado posição central no âmbito do Superior Tribunal de Justiça (STJ). A jurisprudência da Corte consolidou o entendimento de que não se aplica a responsabilidade objetiva aos provedores de conteúdo em relação a danos morais decorrentes de mensagens ofensivas postadas por usuários. Em decisão paradigmática, no REsp

1.308.830/RS, relatado pela Ministra Nancy Andrighi, a Terceira Turma firmou que tais danos não constituem risco inerente à atividade dos provedores, afastando a incidência do art. 927, parágrafo único, do Código Civil de 2002 (Brasil, 2002).

No entanto, a responsabilidade do provedor de conteúdo é de natureza subjetiva nos casos em que, após ser notificado sobre conteúdo ilícito — que fira a privacidade ou atente contra a honra e a imagem do indivíduo —, a empresa não adota medidas rápidas para remover a informação, passando, dessa forma, a responder solidariamente com o autor do dano pela reparação à vítima. Conforme podemos observar:

AGRAVO INTERNO NO RECURSO ESPECIAL. AÇÃO INDENIZATÓRIA. DANOS MORAIS. RESPONSABILIDADE CIVIL DE PROVEDOR DE INTERNET. OFENSAS INSERIDAS POR ANÔNIMO NO SITE DE RELACIONAMENTOS ORKUT. RETIRADA DE CONTEÚDO OFENSIVO APÓS A NOTIFICAÇÃO. INEXISTÊNCIA DE ATO ILÍCITO. PRECEDENTES. AGRAVO NÃO PROVIDO. 1. A jurisprudência desta Corte caminha no sentido de que: I) o dano moral decorrente de mensagens com conteúdo ofensivo inseridas no site pelo usuário não constitui risco inerente à atividade desenvolvida pelo provedor de conteúdo, pelo que não se lhe é aplicável a responsabilidade objetiva, prevista no art. 927, parágrafo único, do CC/2002; II) a fiscalização prévia dos conteúdos postados não é atividade intrínseca ao serviço prestado pelo provedor de conteúdo. 2. A responsabilidade civil do provedor de internet, em casos como este, é subjetiva, e considerando que não ficou caracterizada nenhuma conduta ilícita da ora agravada capaz de ensejar a sua responsabilização, pois a empresa retirou da internet as imagens/mensagens ofensivas em 3 (três) dias, assim que foi notificada, não merece reforma o acórdão recorrido. 3. Agravo interno desprovido. (AgInt no REsp 1507782/RS, Rel. Ministro RAUL ARAÚJO, QUARTA TURMA, julgado em 11/02/2020, DJe 03/03/2020)

No mesmo sentido, o STJ tem reiterado que a responsabilização dos provedores somente ocorre quando, após devidamente notificados por ordem judicial, deixam de retirar o conteúdo ofensivo. Essa posição busca equilibrar a liberdade de expressão com a necessidade de proteção aos direitos da personalidade, evitando a imposição de uma obrigação geral de monitoramento prévio, que poderia inviabilizar a própria dinâmica das plataformas digitais. Assim, a Corte privilegia a lógica de responsabilização subjetiva, condicionada à ciência inequívoca da ilicitude (REsp 1.308.830/RS, 2012).

No REsp 1.859.665/SC, o STJ enfrentou um caso em que uma empresa buscava a responsabilização do provedor pela veiculação de vídeo considerado difamatório. A decisão destacou que, ainda que a postagem possa afetar a imagem da sociedade empresária, a quebra indiscriminada de sigilo dos usuários que compartilharam o conteúdo não seria admissível sem a devida exposição de razões fundadas. Nesse contexto, prevaleceu a interpretação do art. 22 do Marco Civil da Internet (Lei nº 12.965/2014), que assegura a preservação da privacidade e do sigilo de dados, condicionando sua quebra à autorização judicial (Brasil, 2014).

RECURSO ESPECIAL. OBRIGAÇÃO DE FAZER C/C EXIBIÇÃO DE DOCUMENTOS. POSTAGEM DE VÍDEO CONTENDO INFORMAÇÕES ALEGADAMENTE FALSAS, PREJUDICIAIS À IMAGEM DA SOCIEDADE EMPRESÁRIA AUTORA, EM REDE SOCIAL. QUEBRA DO SIGILO DE TODOS OS USUÁRIOS QUE COMPARTILHARAM O CONTEÚDO POTENCIALMENTE DIFAMATÓRIO NA PLATAFORMA DO FACEBOOK. IMPOSSIBILIDADE. PLEITO SEM EXPOSIÇÃO DE FUNDADAS RAZÕES PARA A QUEBRA. MARCO CIVIL DA INTERNET (LEI N. 12.965/2014, ART. 22). PRESERVAÇÃO DA PRIVACIDADE E DO DIREITO AO SIGILO DE DADOS. 1. O Marco Civil da Internet (Lei n. 12.965/2014) estabelece que, na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 ano, nos termos do regulamento (art. 13); e o provedor de aplicações de internet, custodiar os respectivos registros de acesso a aplicações de internet pelo prazo de 6 meses (art. 15). 2. O propósito da norma foi criar instrumental que consiga, por autoridade constituída e precedida de autorização judicial, acessar os registros de conexão, rastreando e sancionando eventuais condutas ilícitas perpetradas por usuários da internet e inibindo, de alguma forma, a falsa noção de anonimato no uso das redes. Por outro lado, a Lei n. 12.965/2014 possui viés hermenêutico voltado ao zelo pela preservação da intimidade, da vida privada, da honra e da imagem do usuário (art. 23), com a previsão de cláusula de reserva judicial para qualquer quebra de sigilo. 3. Portanto, se é certo afirmar que o usuário das redes sociais pode livremente reivindicar seu direito fundamental de expressão, também é correto sustentar que a sua liberdade encontrará limites nos direitos da personalidade de outrem, sob pena de abuso em sua autonomia, já que nenhum direito é absoluto, por maior que seja a sua posição de preferência, especialmente se tratar-se de danos a outros direitos de elevada importância.

4. No caso, a autora requereu a suspensão imediata do vídeo disponibilizado em redes sociais no qual um homem, anonimamente, afirmava ter comprado um lanche que estaria contaminado com larvas nas dependências da sua empresa, não sendo tal notícia verdadeira, já que a refeição jamais fora adquirida no estabelecimento da requerente, que, em razão disso, foi afetada em seus negócios e em sua imagem. Além disso, requereu fosse a empresa de rede social obrigada a fornecer o IP de todos os responsáveis pelo compartilhamento do vídeo difamador. 5. Nos termos da Lei n. 12.965/2014 (art. 22), a parte interessada poderá pleitear ao juízo, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet. Para tanto, sob pena de admissibilidade, exige a norma que haja: I - fundados indícios da ocorrência do ilícito; II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III - período ao qual se referem os registros (parágrafo único). 6. É vedado ao provedor de aplicações de internet – em pedido genérico e coletivo, sem a especificação mínima de uma conduta ilícita realizada – fornecer dados, de forma indiscriminada, dos usuários que tenham compartilhado determinada postagem. 7. Na espécie, a recorrida não trouxe nenhum elemento, nem sequer descreveu indícios de ilicitude da conduta dos usuários que, por qualquer motivo, acabaram por apenas compartilhar o vídeo com conteúdo difamador, limitando-se a identificar a página do autor da postagem e de um ex-funcionário que também teria publicado o vídeo em seu perfil. 8. Assim, sopesados os direitos envolvidos e o risco potencial de violação de cada um deles, deve prevalecer a privacidade dos usuários. Não se pode subjugar o direito à privacidade a ponto de permitir a quebra indiscriminada do sigilo dos registros, com informações de foro íntimo dos usuários, tão somente pelo fato de terem compartilhado determinado vídeo que, depois se soube, era falso. 9. Recurso especial provido (BRASIL. Superior Tribunal de Justiça (STJ). REsp 1.859.665/SC. Rel. Min. Paulo de Tarso Sanseverino. 3ª Turma. Julgado em 10 mar. 2020).

O caso em análise também evidenciou a tensão entre a busca pela identificação de infratores e a salvaguarda de direitos fundamentais. O STJ enfatizou que, embora o Marco Civil tenha sido concebido como um instrumento para rastrear condutas ilícitas, ele igualmente se orienta pela proteção da intimidade e da vida privada dos usuários. Por isso, não basta a alegação genérica de ofensa: é necessário que o pleito de quebra de sigilo esteja devidamente fundamentado e justificado (REsp 1.859.665/SC, 2020).

Essa mesma linha de raciocínio aparece em decisões sobre a liberdade de expressão e seus limites. No AgInt no AREsp 685.720/SP, a Corte reafirmou que o direito de manifestar opiniões não é absoluto, sobretudo quando há violação à honra, à imagem e à dignidade de terceiros. Assim, as plataformas somente respondem se, após ordem judicial, mantiverem o conteúdo ofensivo disponível, reforçando o modelo de responsabilidade por omissão qualificada (STJ, 2015).

A jurisprudência também tem reforçado que o controle de conteúdo por parte dos provedores deve ser compatível com o respeito à autonomia dos usuários. O STJ entende que cabe ao Poder Judiciário, e não às plataformas, definir o que configura ofensa aos direitos da personalidade. Essa interpretação protege contra possíveis abusos de censura privada e garante que a liberdade de expressão continue sendo um dos pilares do ambiente digital, ainda que sujeito a limites legais e constitucionais (REsp 1.308.830/RS, 2012).

Contudo, há casos em que a responsabilidade dos provedores é afirmada de forma mais rigorosa, especialmente quando se verifica inércia diante de ordens judiciais claras. Nesses cenários, a omissão é considerada uma forma de conivência, o que enseja responsabilização solidária pelos danos ocasionados. Isso demonstra que o STJ busca impor às plataformas um dever de diligência, sem, contudo, convertê-las em censores prévios da internet (REsp 1.859.665/SC, 2020).

Outro ponto relevante é a distinção entre conteúdos gerados espontaneamente por usuários e aqueles impulsionados ou promovidos pelas próprias plataformas. Embora a jurisprudência ainda caminhe na consolidação dessa diferenciação, já se reconhece que a atividade da plataforma, quando ativa e voltada à divulgação de determinado conteúdo, pode atrair maior responsabilidade. Nesse caso, a lógica de neutralidade perde força, e a plataforma passa a ser vista como participante do ato ilícito (AgInt no AREsp 685.720/SP, 2015).

O Marco Civil da Internet ocupa papel central nessas decisões, servindo de parâmetro normativo para compatibilizar direitos fundamentais. Ao mesmo tempo em que garante a preservação da privacidade e do sigilo, também cria instrumentos para a responsabilização de condutas abusivas. O STJ tem utilizado seus dispositivos para evitar excessos tanto por parte

das vítimas, que buscam responsabilizações amplas, quanto das plataformas, que alegam neutralidade em todas as situações (BRASIL, 2014).

Portanto, os casos analisados demonstram o esforço do STJ em construir um equilíbrio entre liberdade de expressão e proteção da honra, da imagem e da privacidade. A jurisprudência, a partir de precedentes como o REsp 1.308.830/RS, o REsp 1.859.665/SC e o AgInt no AREsp 685.720/SP, estabelece parâmetros importantes para orientar a atuação de usuários, empresas e do próprio Judiciário. Trata-se de um campo em constante evolução, que reflete os desafios contemporâneos da sociedade da informação e a necessidade de interpretar o direito civil à luz das novas tecnologias.

4.2 Dados pessoais, *fake news* e a atuação das plataformas

A disseminação de *fake news* nas plataformas digitais representa um desafio contemporâneo para a proteção de dados pessoais e a preservação dos direitos fundamentais dos usuários. As informações falsas, frequentemente manipuladas com objetivos políticos ou econômicos, podem violar a privacidade e a imagem de indivíduos, bem como comprometer processos democráticos. Zanin e Ferreira (2025) destacam que a circulação desenfreada de conteúdos falsos exige das plataformas digitais a adoção de mecanismos de monitoramento e verificação, sem, no entanto, comprometer a liberdade de expressão.

As plataformas digitais atuam como intermediárias na propagação de informações, e a manipulação algorítmica intensifica o alcance de conteúdos falsos, tornando difícil a distinção entre usuários que compartilham por engano e aqueles que deliberadamente criam desinformação. Segundo Pinheiro e Costa (2025), os algoritmos das redes sociais podem priorizar conteúdos sensacionalistas, ampliando a viralização de *fake news* e, consequentemente, expondo dados pessoais de terceiros de forma involuntária ou indevida.

O Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD) oferecem parâmetros normativos para limitar os riscos associados à circulação de *fake news*, impondo deveres de guarda e proteção de dados aos provedores de serviços digitais. Borges (2025) observa que, apesar dos avanços normativos, ainda há incertezas quanto à extensão da responsabilidade civil das plataformas frente à viralização de conteúdos ilícitos, especialmente no que se refere à obrigação de remoção imediata de informações que violem direitos de personalidade.

Em situações práticas, os provedores de aplicações digitais devem agir prontamente após a identificação de *fake news* que envolvam dados pessoais, evitando a perpetuação de

danos a terceiros. A jurisprudência brasileira tem enfatizado que a responsabilidade subjetiva recai sobre a plataforma quando esta, mesmo notificada, não adota medidas eficazes para impedir a disseminação de conteúdos prejudiciais (Zanin; Ferreira, 2025). Esse posicionamento busca equilibrar a liberdade de expressão com a proteção da privacidade e da integridade de dados pessoais.

Além do monitoramento de conteúdo, as plataformas precisam investir em mecanismos de rastreamento e autenticação de informações, garantindo transparência e confiabilidade no fluxo de dados. Pinheiro e Costa (2025) reforçam que a atuação proativa das plataformas é essencial não apenas para proteger direitos individuais, mas também para resguardar a credibilidade do processo democrático, que pode ser gravemente afetado pela propagação de notícias falsas e manipulação de dados sensíveis.

Portanto, a atuação das plataformas digitais em casos de *fake news* envolve a implementação de medidas técnicas e jurídicas que conciliam a proteção de dados pessoais, a preservação da privacidade e a liberdade de expressão. A responsabilidade civil surge como instrumento para coibir abusos, exigir diligência e garantir que os usuários sejam amparados juridicamente contra danos causados por conteúdos ilícitos, em consonância com o Marco Civil da Internet e a LGPD (Borges, 2025).

Nessa toada, a problemática é eminentemente atual e multifacetada. Diante disso, é imperiosa a necessidade de ressignificar o aparato jurídico no intuito de criar regras visando o fortalecimento de mecanismos de fiscalização, inclusive, de governança, para a garantia da segurança jurídica em ambientes digitais.

5 CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo desta pesquisa permitiu compreender que a responsabilidade civil das plataformas digitais é uma questão multifacetada, que exige conciliar direitos fundamentais, como a liberdade de expressão, com a proteção da privacidade e dos dados pessoais dos usuários. Observou-se que, embora a responsabilidade objetiva não se aplique de forma ampla aos provedores de serviços digitais, a responsabilidade subjetiva se mostra essencial para coibir abusos e garantir a reparação de danos decorrentes de conteúdos ilícitos ou ofensivos.

A Lei Geral de Proteção de Dados (LGPD) e o Marco Civil da Internet surgem como instrumentos fundamentais para balizar a atuação das plataformas, impondo deveres claros de guarda, tratamento e proteção de dados, bem como limites à circulação de informações que

possam prejudicar terceiros. Essas normas conferem segurança jurídica e estabelecem parâmetros para que a responsabilização ocorra de forma equilibrada, evitando tanto a omissão das plataformas quanto a censura excessiva de conteúdos.

A revisão da jurisprudência do Superior Tribunal de Justiça evidenciou que o entendimento consolidado privilegia a responsabilidade subjetiva do provedor, condicionada à notificação prévia sobre o conteúdo ilícito e à inércia injustificada em retirá-lo do ar. Casos recentes demonstram que o STJ busca proteger direitos da personalidade sem restringir indevidamente a liberdade de expressão, reforçando a necessidade de uma atuação diligente e fundamentada das plataformas diante de conteúdos ofensivos, *fake news* ou violações de privacidade.

Além disso, a pesquisa ressaltou que a atuação das plataformas digitais deve ser pautada por princípios de transparência, governança responsável e diligência na moderação de conteúdos. A implementação de mecanismos técnicos e administrativos para rastrear e remover informações prejudiciais é imprescindível para reduzir riscos aos usuários e assegurar a integridade do ambiente digital. Nesse sentido, a responsabilização civil funciona como instrumento de incentivo à boa governança e à proteção dos direitos fundamentais.

Conclui-se, portanto, que a regulação da responsabilidade civil das plataformas digitais é um campo em evolução, demandando constante atualização legislativa e interpretação jurisprudencial para acompanhar as inovações tecnológicas. A pesquisa evidencia que a harmonização entre liberdade de expressão, proteção da privacidade e responsabilização por conteúdos ilícitos é possível, mas exige cuidado na aplicação das normas e na definição de limites claros para o dever de diligência das plataformas.

Finalmente, a investigação realizada reforça a importância do equilíbrio entre inovação tecnológica e direitos fundamentais. A atuação responsável das plataformas digitais, combinada com a aplicação adequada da legislação e a jurisprudência do STJ, contribui para um ambiente virtual mais seguro, ético e juridicamente sustentável, garantindo a proteção de indivíduos e promovendo a confiança na utilização de serviços digitais no Brasil.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Barbara Jhessyka; SOMBRA, Maria Clara; DO CARMO AZEVEDO, Delner. A RESPONSABILIDADE DAS PLATAFORMAS DIGITAIS PELOS CONTEÚDOS PATROCINADOS: DESAFIOS E PERSPECTIVAS NO DIREITO DO CONSUMIDOR. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 11, n. 4, p. 1155-1170, 2025. Disponível em: <https://periodicorease.pro.br/rease/article/view/18686>. Acesso em: 19 set. 2025.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Editora Forense, 2019.

BORGES, Gustavo Silveira. Propostas para o aperfeiçoamento da tese do STF sobre o Marco Civil da Internet à luz da responsabilidade civil: entre o avanço e a incerteza. **Revista IBERC**, v. 8, n. 2, p. 178-194, 2025. Disponível em: <https://revista.iber.org.br/iber/article/view/358/291>. Acesso em: 19 set. 2025.

BRASIL. **Lei Geral de Proteção de Dados Pessoais**: Lei nº 13.709/2018. Brasília, DF: Senado Federal, 2024. 47 p. Edição atualizada até junho de 2024. ISBN 978-65-5676-500-6.

BRASIL. Código Civil. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 21 set. 2025.

BRASIL. Superior Tribunal de Justiça (STJ). **REsp 1.308.830/RS**. Rel. Min. Nancy Andrighi. 3ª Turma. Julgado em 08 maio 2012. DJe 19 jun. 2012. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=124852901&num_registro=202000208006&data=20210420&tipo=5&formato=PDFAcesso em: 21 set. 2025.

BRASIL. Superior Tribunal de Justiça (STJ). **REsp 1.859.665/SC**. Rel. Min. Paulo de Tarso Sanseverino. 3ª Turma. Julgado em 10 mar. 2020. Disponível em: <https://processo.stj.jus.br/processo/pesquisa/?aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&termo=REsp%201859665>. Acesso em: 21 set. 2025.

BRASIL. Superior Tribunal de Justiça (STJ). **AgInt no AREsp 685.720/SP**. Rel. Min. Luis Felipe Salomão. 4ª Turma. Julgado em 03 mar. 2015. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=101922885&num_registro=201500662632&data=20201016&tipo=91&formato=PDF. Acesso em: 20 set. 2025.

CHIARINI, Tulio *et al.* **Plataformas digitais: mapeamento semissistemático e interdisciplinar do conhecimento produzido nas universidades brasileiras**. Texto para Discussão, 2023. DISPONÍVEL EM: <https://repositorio.ipea.gov.br/server/api/core/bitstreams/4c20f7d7-63d3-4b51-837f-04788a946ed0/content>. Acesso em: 20 set. 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. rev. e atual. Rio de Janeiro: Forense, 2021.

DIAS, Daniel Pires Novais et al. Plataformas no Marco Civil da Internet: a necessidade de uma responsabilidade progressiva baseada em riscos. **Civilistica. com**, v. 12, n. 3, p. 1-24, 2023. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/931>. Acesso em: 19 set. 2025.

FERNANDES, Marcelo Eloy; NUZZI, Ana Paula Eloy. Fundamentos da Lei Geral de Proteção de Dados (LGPD): uma revisão narrativa. **Research, Society and Development**, v.

11, n. 12, p. e310111234247-e310111234247, 2022. Disponível em:
<https://rsdjournal.org/index.php/rsd/article/view/34247>. Acesso: 20 set. 2025.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil**, v. 3: responsabilidade civil. 18. ed. São Paulo: Saraiva Educação, 2020.

GONÇALVES, Victor Hugo Pereira. **Marco civil da internet comentado** / Victor Hugo Pereira Gonçalves. – 1. ed. – São Paulo: Atlas, 2017.

MACIEL, Rafael. **Manual Prático sobre a Lei geral de Proteção de Dados pessoais**: Atualizada com a Medida Provisória nº 869/18. Goiânia: RM Digital Education. 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados comentada** [livro eletrônico]/coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. --2. ed. -- São Paulo: Thomson Reuters Brasil, 2019.

MARQUES, Claudia Lima et al. **10 anos marco civil da internet** [recurso eletrônico] : avaliando impactos e desafios / Camila Fernandes Pantuzo ... [recurso eletrônico] ; coordenado por Claudia Lima Marques, Guilherme Magalhães Martins, Fernando Rodrigues Martins. - Indaiatuba, SP : Editora Foco, 2024.

MANZATO, Welington Junior Jorge; SOARES, Marcelo Negri; CUGULA, Jarbas Rodrigues Gomes. Lei geral de proteção de dados e a importância da tutela dos direitos da personalidade nos contratos digitais. **Boletim de Conjuntura (BOCA)**, v. 18, n. 54, p. 621-646, 2024. Disponível em: <https://revista.ioles.com.br/boca/index.php/revista/article/view/5124>. Acesso em: 16 set. 2025.

MELO, Nehemias Domingos de. **Lições de direito civil** [recurso eletrônico] : Obrigações e Responsabilidade Civil / Nehemias Domingos de Melo. - 6. ed. - Indaiatuba, SP : Editora Foco, 2025.

OLIVEIRA, Luanna Kelly Arrais de; DE SOUSA, Deisy Sanglard. RESPONSABILIDADE CIVIL POR ATOS ILÍCITOS E ABUSOS DOS USUÁRIOS DO INSTAGRAM NO BRASIL: A LINHA ENTRE A LIBERDADE DE EXPRESSÃO E OS ABUSOS CONTRA OS DIREITOS DE PERSONALIDADE. **LUMEN ET VIRTUS**, v. 16, n. 47, p. 3892-3904, 2025. Disponível em: <https://periodicos.newsciencepubl.com/LEV/article/view/4571>. Acesso em: 19 set. 2025.

PINHEIRO, Weider Silva et al. A PROTEÇÃO DE DADOS PESSOAIS NAS RELAÇÕES CONTRATUAIS PRIVADAS: LIMITES E POSSIBILIDADES DA LGPD. **Revista DCS**, v. 22, n. 80, p. e2975-e2975, 2025. Disponível em:
<https://ojs.revistadcs.com/index.php/revista/article/view/2875>. Acesso em: 15 set. 2025.

PINHEIRO, Camilla; COSTA, Edwaldo. AS FAKE NEWS SOBRE O PL DAS FAKE NEWS: MANIPULAÇÃO ALGORÍTMICA NO DEBATE SOBRE REGULAÇÃO DAS PLATAFORMAS DIGITAIS NO BRASIL. **ARACÊ**, v. 7, n. 6, p. 30432-30455, 2025. Disponível em: <https://periodicos.newsciencepubl.com/arace/article/view/5730>. Acesso em: 19 set. 2025.

RIZZARDO, Arnaldo. **Responsabilidade civil** / Arnaldo Rizzardo. 8. ed. Rio de Janeiro: Forense, 2019.

SIQUEIRA, Dirceu Pereira; FACHIN, Zulmar. Política, direitos da personalidade e a proteção da liberdade de expressão na LGPD. **REVISTA DA FACULDADE DE DIREITO DA UFMG**, v. 80, p. 51-68, 2022. Disponível em: <https://web.direito.ufmg.br/revista/index.php/revista/article/view/2144>. Acesso em: 20 set. 2025.

ZANIN, Gabriela; FERREIRA, Rafael Fonseca. Fake News, Processo Democrático e o Papel das Plataformas Digitais. **Pensar - Revista de Ciências Jurídicas**, v. 30, p. 1-13, 2025. Disponível em: <https://ojs.unifor.br/rpen/article/view/15953>. Acesso em: 20 set. 2025.