

UNIVERSIDADE FEDERAL DE OURO PRETO

Escola de Direito, Turismo e Museologia

Departamento de Direito

Arthur de Araújo Braga Ferreira

O DEVER DE DILIGÊNCIA NO COMBATE À DESINFORMAÇÃO DIGITAL

Investigação sobre o papel de usuários, administradores de plataformas e desenvolvedores no controle da disseminação de fake news

Ouro Preto - MG

2026

ARTHUR DE ARAÚJO BRAGA FERREIRA

O DEVER DE DILIGÊNCIA NO COMBATE À DESINFORMAÇÃO DIGITAL

Investigação sobre o papel de usuários, administradores de plataformas e desenvolvedores no controle da disseminação de fake news

Monografia apresentada ao Curso de Direito da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de Bacharel em Direito

Área de concentração: Direito Civil

Orientadora: Juliana Evangelista de Almeida

Ouro Preto - MG

2026



FOLHA DE APROVAÇÃO

Arthur de Araújo Braga Ferreira

O DEVER DE DILIGÊNCIA NO COMBATE À DESINFORMAÇÃO DIGITAL Investigação sobre o papel de usuários, administradores de plataformas e desenvolvedores no controle da disseminação de fake news

Monografia apresentada ao Curso de Direito da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de Bacharel em Direito

Aprovada em 03 de março de 2026

Membros da banca

Doutora - Juliana Evangelista de Almeida - Orientador(a) Universidade Federal de Ouro Preto
Doutra - Beatriz Schettini - Universidade Federal de Ouro Preto
Graduado - Elísio Hermenegildo da Silva Júnior - Universidade Federal de Ouro Preto

Juliana Evangelista de Almeida, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 05 de março de 2026



Documento assinado eletronicamente por **Juliana Evangelista de Almeida, PROFESSOR DE MAGISTERIO SUPERIOR**, em 05/03/2026, às 14:32, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1069978** e o código CRC **1BEDE210**.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus por ter me capacitado, dado discernimento e colocado pessoas em minha vida que mudaram o caminho da minha trajetória, possibilitando-me chegar tão longe. Ao meu pai, que, mesmo sem saber ler e escrever, me inspirou a buscar um futuro melhor por meio da educação. Às minhas mães, pelo apoio e carinho incondicionais, sendo mais do que fundamentais à minha formação. À Universidade Federal de Ouro Preto, pela educação pública, humanizada e de qualidade. Aos meus amigos de vida e ouro-pretanos, reconheço minha sorte por ter cruzado caminhos e compartilhado momentos extraordinários. À República Adega, por ter me acolhido como casa e família, possibilitando meu crescimento como pessoa. Por fim, agradeço aos professores do curso de Direito pela dedicação e pelos grandes ensinamentos. Agradeço, em especial, à Juliana, pelos auxílios, pela paciência e pela leveza na condução da orientação.

RESUMO

A desinformação digital deixou de ser apenas um problema comunicacional e passou a produzir consequências jurídicas relevantes, como violações à honra e à privacidade, prejuízos ao debate público e riscos à integridade de processos democráticos. No ambiente online, conteúdos falsos se disseminam com rapidez, grande alcance e apoio de mecanismos de recomendação algorítmica, o que amplia o potencial de dano e dificulta sua contenção. Diante desse cenário, o presente trabalho analisa como o dever de diligência pode orientar, no direito brasileiro, uma responsabilização adequada no combate à desinformação, considerando que usuários, plataformas digitais e desenvolvedores ocupam posições distintas no ecossistema informacional e dispõem de capacidades diferentes de prevenção e controle. A pesquisa adota método jurídico-dogmático, com análise de legislação, doutrina e jurisprudência, partindo dos arts. 186 e 927 do Código Civil e dialogando com o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais e o debate travado no Supremo Tribunal Federal acerca do art. 19 do MCI (Tema 987 da Repercussão Geral), além de parâmetros utilizados no enfrentamento da desinformação eleitoral. Como resultado, o estudo sistematiza critérios para a aplicação do dever de diligência no ambiente digital, como a previsibilidade do dano, a posição e a capacidade técnica do agente, o nexo de causalidade, o regime de responsabilidade e a proporcionalidade conforme a gravidade da ilicitude. Conclui-se que a responsabilização deve ser graduada: usuários, em regra, respondem por culpa e devem adotar cautela mínima ao divulgar conteúdos claramente falsos ou lesivos; plataformas assumem deveres mais intensos, em razão do controle sobre mecanismos de visibilidade, recomendação e monetização; e desenvolvedores atuam predominantemente em um plano preventivo e estrutural, com limites atuais à responsabilização direta e necessidade de avanço regulatório em governança tecnológica. O trabalho sustenta que o dever de diligência, aplicado de forma proporcional e compatível com os direitos fundamentais, permite enfrentar riscos informacionais ampliados sem ruptura com os fundamentos tradicionais da responsabilidade civil.

Palavras-chave: desinformação digital; dever de diligência; responsabilidade civil; plataformas digitais; governança tecnológica.

ABSTRACT

Digital misinformation has ceased to be merely a communication problem and has come to produce significant legal consequences, such as violations of reputation and privacy, harm to public debate, and risks to the integrity of democratic processes. In online environments, false content spreads rapidly, reaches wide audiences, and is often supported by algorithmic recommendation mechanisms, which increases the potential for harm and makes its containment more difficult. In this context, this study analyzes how the duty of diligence can guide, under Brazilian law, an appropriate framework of liability to address misinformation, considering that users, digital platforms, and developers occupy distinct positions within the informational ecosystem and possess different capacities for prevention and control. The research adopts a legal-dogmatic method, based on the analysis of legislation, legal scholarship, and case law, drawing from Articles 186 and 927 of the Brazilian Civil Code and engaging with the Internet Civil Framework, the General Data Protection Law, and the debate before the Brazilian Supreme Court concerning Article 19 of the Internet Civil Framework (Topic 987 of General Repercussion), as well as standards applied in the context of electoral misinformation. As a result, the study systematizes criteria for applying the duty of diligence in the digital environment, including harm foreseeability, the position and technical capacity of the actor, causation, the applicable liability regime, and proportionality according to the gravity of the unlawfulness. It concludes that liability should be graduated: users are generally subject to fault-based liability and must exercise minimum caution when disseminating content that is clearly false or harmful; platforms assume more demanding duties due to their control over visibility, recommendation, and monetization mechanisms; and developers operate predominantly at a preventive and structural level, with current limits to direct liability and a need for regulatory advancement in technology governance. The study argues that the duty of diligence, when applied proportionally and in a manner compatible with fundamental rights, enables the addressing of amplified informational risks without departing from the traditional foundations of civil liability.

Keywords: digital misinformation; duty of diligence; civil liability; online platforms; technology governance.

SUMÁRIO

1 INTRODUÇÃO.....	6
2 A DESINFORMAÇÃO DIGITAL COMO PROBLEMA JURÍDICO E O PAPEL DOS ATORES DIGITAIS.....	7
2.1 A desinformação como fenômeno jurídico e social.....	8
2.2 Mapeamento dos atores digitais e seus papéis.....	10
2.2.1 Usuários: o dever de cautela na comunicação.....	10
2.2.2 Plataformas digitais: intermediárias e curadoras de informação.....	11
2.2.3 Desenvolvedores de tecnologia: a dimensão estruturante da diligência.....	11
2.3 A interdependência dos agentes e a necessidade do dever de diligência.....	12
3 O DEVER DE DILIGÊNCIA NO DIREITO BRASILEIRO E SUA TRANSPOSIÇÃO PARA O AMBIENTE DIGITAL.....	13
3.1 O dever de diligência na responsabilidade civil brasileira.....	14
3.2 O dever de diligência no Marco Civil da Internet.....	16
3.3 Interseções com a Lei Geral de Proteção de Dados Pessoais (LGPD).....	18
3.3.1 Prevenção e gestão de riscos como fundamentos estruturantes.....	18
3.3.2 Responsabilização, prestação de contas e governança.....	19
3.3.3 O impacto da LGPD na circulação de informações e nos riscos de desinformação.....	19
3.4 O debate no STF sobre o art. 19 do MCI (Tema 987 da Repercussão Geral).....	20
3.5 Critérios jurídicos para a aplicação digital do dever de diligência.....	21
3.5.1 Previsibilidade do dano como critério de diligência digital.....	22
3.5.2 Posição e capacidade técnica do agente.....	23
3.5.3 Nexo de causalidade no ambiente digital.....	24
3.5.4 Natureza da responsabilidade (objetiva x subjetiva) em cada situação.....	25
3.5.5 Proporcionalidade e gravidade da ilicitude.....	26
4 APLICAÇÃO DIFERENCIADA DO DEVER DE DILIGÊNCIA ENTRE OS ATORES DIGITAIS.....	27
4.1 Aplicação dos critérios de diligência aos usuários.....	28
4.2 Aplicação dos critérios de diligência às plataformas digitais.....	30
4.3 Aplicação dos critérios de diligência aos desenvolvedores e sistemas automatizados	32
4.4 Modelo integrado de corresponsabilidade no ecossistema informacional.....	33
5 CONCLUSÃO.....	35
REFERÊNCIAS.....	38

1 INTRODUÇÃO

A desinformação digital consolidou-se como um dos principais desafios contemporâneos enfrentados pelas democracias constitucionais e pelo Direito. A expansão das redes sociais e das plataformas digitais transformou profundamente a circulação de informações, conferindo a conteúdos falsos, enganosos ou manipulados um potencial ampliado de alcance e impacto. Nesse contexto, a desinformação passou a produzir efeitos jurídicos relevantes, como a violação de direitos da personalidade, a manipulação da opinião pública e o enfraquecimento da confiança nas instituições democráticas, exigindo do Direito respostas compatíveis com a complexidade do ambiente informacional contemporâneo.

Nesse cenário, o Direito é chamado a enfrentar um problema que desafia categorias tradicionais da responsabilidade civil. A identificação do agente causador do dano, a delimitação do nexo de causalidade e a aferição da culpa tornam-se mais complexas em um ambiente marcado por múltiplos intermediários, decisões automatizadas e interações descentralizadas. Ainda assim, o ordenamento jurídico brasileiro dispõe de instrumentos capazes de dialogar com essa realidade, especialmente a partir da noção de dever de diligência, extraída dos fundamentos clássicos da responsabilidade civil e reinterpretada à luz das especificidades do meio digital.

A partir dos arts. 186 e 927 do Código Civil, é possível identificar a existência de um dever geral de cuidado que serve de fundamento para a análise da responsabilidade por danos informacionais. Embora concebidos em um contexto pré-digital, esses dispositivos oferecem base normativa suficiente para a reflexão sobre o dever de diligência no ambiente digital, tema que será desenvolvido ao longo do trabalho.

Essa adaptação tem sido progressivamente reconhecida no plano normativo e jurisprudencial. O Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais, ainda que não tratem diretamente da desinformação, estabelecem parâmetros relevantes de cuidado, prevenção e responsabilização no ambiente digital. Da mesma forma, decisões recentes do Supremo Tribunal Federal e do Tribunal Superior Eleitoral indicam uma tendência de reconhecimento de deveres mínimos de diligência por parte de agentes que exercem influência significativa sobre a circulação de informações, especialmente em situações de grave ilicitude ou risco a direitos fundamentais.

Diante desse quadro, o presente trabalho tem como objetivo analisar a desinformação digital a partir da perspectiva do dever de diligência no Direito brasileiro, examinando como esse dever pode ser aplicado de forma diferenciada aos principais atores do ecossistema informacional. Parte-se da premissa de que usuários, plataformas digitais e desenvolvedores

ocupam posições distintas na cadeia informacional e dispõem de capacidades diversas de controle e prevenção de danos, o que impede a adoção de um modelo uniforme de responsabilização.

A pesquisa adota método jurídico-dogmático, com análise normativa, doutrinária e jurisprudencial, além de diálogo com referências internacionais relevantes, como o DSA da União Europeia. Busca-se, assim, construir um modelo interpretativo que preserve a coerência dos fundamentos tradicionais da responsabilidade civil, ao mesmo tempo em que ofereça respostas proporcionais e constitucionalmente adequadas aos riscos informacionais amplificados pela tecnologia.

Para alcançar esse objetivo, o trabalho estrutura-se da seguinte forma: o Capítulo 2 examina a desinformação como problema jurídico e apresenta o papel desempenhado pelos diferentes atores digitais; o Capítulo 3 analisa o dever de diligência no Direito brasileiro e seus critérios de aplicação no ambiente digital; o Capítulo 4 aplica esses critérios de maneira diferenciada a usuários, plataformas e desenvolvedores, culminando em uma leitura integrada da corresponsabilidade no ecossistema informacional; por fim, a conclusão sistematiza os principais achados da pesquisa e aponta limites e perspectivas futuras para o enfrentamento jurídico da desinformação digital.

2 A DESINFORMAÇÃO DIGITAL COMO PROBLEMA JURÍDICO E O PAPEL DOS ATORES DIGITAIS

A desinformação digital apresenta-se como um fenômeno que transcende o campo da comunicação social e assume relevância jurídica própria, ao produzir impactos concretos sobre direitos fundamentais, instituições democráticas e relações privadas. A automação dos fluxos informacionais e o papel central assumido pelas plataformas digitais ampliaram de forma significativa a circulação de conteúdos falsos ou manipulados, o que exige do Direito respostas capazes de ir além de condutas individuais e considerar também as estruturas que organizam esse ambiente informacional.

Este capítulo tem por objetivo examinar a desinformação como problema jurídico e identificar os principais atores envolvidos em sua disseminação. Parte-se da premissa de que a desinformação decorre da interação entre usuários, plataformas digitais e estruturas tecnológicas, cujas posições na cadeia informacional são desiguais e, por isso, exigem critérios distintos de análise jurídica.

Com base nesse enquadramento, o capítulo desenvolve a caracterização jurídica da desinformação, o mapeamento dos atores digitais e a análise de sua interdependência,

preparando o terreno teórico para a aplicação do dever de diligência como eixo estruturante da responsabilidade no ambiente digital.

2.1 A desinformação como fenômeno jurídico e social

A desinformação digital consolidou-se como um dos maiores desafios contemporâneos aos sistemas democráticos e ao Direito. A dinâmica acelerada das redes sociais, aliada aos mecanismos de recomendação algorítmica, torna a circulação de conteúdos falsos ou manipulados mais rápida, mais massiva e mais difícil de conter. O resultado é que informações imprecisas, antes vistas como problema essencialmente comunicacional, passaram a produzir efeitos jurídicos concretos: violam a honra, afetam a privacidade, desestabilizam processos eleitorais e corroem a confiança pública em instituições democráticas. Por isso, a desinformação deixou de ser um fenômeno periférico. Ela passou a exigir respostas jurídicas estruturadas, capazes de equilibrar liberdade de expressão, deveres de cuidado e responsabilidade civil no ambiente digital.

A literatura recente mostra que a desinformação está inserida em um cenário mais amplo de crise da esfera pública e de fragilização da confiança social. Em estudo sobre práticas comunicacionais contemporâneas, Mendonça et al. (2023) analisam como as fake news têm sido utilizadas como parte de um repertório de ação política marcado por forte carga emocional, mobilização identitária e produção de antagonismos. Nesse contexto, o desafio jurídico não se limita a verificar a veracidade dos conteúdos, mas envolve compreender como informações enganosas moldam percepções públicas, distorcem processos deliberativos e criam ambiente propício à manipulação e polarização.

Do ponto de vista jurídico, a desinformação pode configurar violação de deveres gerais de cautela e de boa-fé objetiva. Aquele que contribui para a propagação de conteúdos falsos, causando dano a outrem, pode enquadrar-se nas hipóteses dos arts. 186 e 927 do Código Civil. O primeiro define como ato ilícito a conduta negligente ou imprudente que provoque dano; o art. 927 estabelece o dever de indenizar, e seu parágrafo único admite responsabilidade objetiva quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para terceiros. Embora elaborados em um contexto pré-digital, esses dispositivos comportam interpretação que abrange danos informacionais, especialmente quando a conduta envolve previsibilidade de lesão, amplificação indevida ou desrespeito a direitos da personalidade. Como destaca Maria Helena Diniz (2024), o dever jurídico de diligência impõe ao agente o cuidado necessário para evitar danos previsíveis a terceiros, ainda que a conduta se desenvolva em ambientes distintos do espaço físico

tradicional. A autora enfatiza que a culpa, manifestada na negligência, imprudência ou imperícia, permanece parâmetro central da responsabilidade civil, inclusive em contextos tecnologicamente mediados, nos quais a circulação de informações potencializa riscos e amplia o alcance dos danos.

No âmbito institucional, medidas normativas recentes reforçam o reconhecimento jurídico da desinformação. A Resolução TSE nº 23.714/2022 (BRASIL, 2022) regulamentou mecanismos de enfrentamento à desinformação eleitoral, como remoção célere de conteúdos sabidamente falsos, desmonetização de páginas reincidentes e cooperação com plataformas digitais. A norma parte de um pressuposto claro: a integridade do processo eleitoral depende de um ecossistema informacional minimamente confiável, e a circulação massiva de informações falsas constitui ameaça concreta à democracia.

O mesmo movimento aparece no Supremo Tribunal Federal, especialmente com o julgamento do Tema 987 da Repercussão Geral (RE 1.037.396/SC) (BRASIL, 2025), que discutiu a constitucionalidade do art. 19 do Marco Civil da Internet. Embora tenha preservado, como regra geral, o modelo de responsabilização mediante ordem judicial específica, o STF reconheceu que as plataformas têm deveres de diligência, especialmente em situações de grave ilicitude envolvendo discurso de ódio, violência ou direitos de crianças e adolescentes. A Corte aproximou o ordenamento brasileiro de modelos internacionais que combinam liberdade de expressão com transparência, prevenção e prestação de contas por parte dos intermediários digitais.

Nesse cenário, o debate legislativo também avança. O Projeto de Lei nº 2.630/2020 (BRASIL, 2020), conhecido como “PL das Fake News”, propõe deveres de transparência algorítmica, rastreabilidade proporcional de mensagens, políticas mínimas de moderação e auditorias externas. Entretanto, apesar de buscar estabelecer um marco regulatório mais claro, o projeto enfrenta resistência significativa da sociedade. A consulta pública disponibilizada pela Câmara dos Deputados revela esse cenário de controvérsia: mais de 353 mil participantes manifestaram apoio ao PL, enquanto aproximadamente 424 mil votaram contra sua aprovação, indicando que a maior parte dos cidadãos que se engajaram no processo vê a proposta com cautela. Essa rejeição não corresponde a uma resistência ao combate à desinformação, mas reflete preocupações legítimas com eventuais riscos à liberdade de expressão, à privacidade e à possibilidade de que mecanismos como a rastreabilidade de mensagens produzam efeitos indesejados, como vigilância excessiva ou autocensura. Além disso, parte da crítica recai sobre a amplitude das obrigações previstas e sobre a percepção de que algumas medidas podem delegar às plataformas um poder de moderação elevado, sem

critérios suficientemente claros. Essas preocupações ajudam a explicar por que a regulação da desinformação permanece tema sensível e de intensa disputa pública, exigindo cautela e análise técnica rigorosa na construção de qualquer solução legislativa.

A comparação internacional mostra convergência. O DSA (Regulamento UE 2022/2065) impõe obrigações escalonadas às plataformas — avaliações de risco sistêmico, medidas de mitigação, transparência dos algoritmos e mecanismos de contestação de decisões automatizadas. O Digital Services Act (Regulamento (UE) 2022/2065, doravante DSA) não criminaliza a desinformação, mas constrói um modelo robusto de responsabilização procedimental, centrado no dever de diligência. Assim, a desinformação deve ser entendida como fenômeno multifacetado que exige a atuação coordenada dos atores que compõem o ecossistema digital. Ao longo deste trabalho, o dever de diligência servirá como eixo estruturante para delimitar as obrigações de cada agente e propor um modelo de responsabilidade proporcional e constitucionalmente adequado.

2.2 Mapeamento dos atores digitais e seus papéis

O ecossistema digital é composto por uma rede complexa e interdependente de agentes que influenciam direta ou indiretamente o fluxo de informações. A compreensão jurídica da desinformação exige identificar esses atores, analisar seu papel e determinar os deveres que lhes são impostos pelo ordenamento jurídico. Usuários, plataformas e desenvolvedores não ocupam a mesma posição na cadeia informacional e, portanto, não podem ser responsabilizados segundo critérios uniformes. A solução adequada passa por uma lógica de responsabilidade graduada, orientada pelo dever de diligência.

2.2.1 Usuários: o dever de cautela na comunicação

Os usuários são o ponto de partida da circulação de informação: publicam, comentam, compartilham e impulsionam conteúdos em redes sociais e aplicativos de mensagens. Embora muitas vezes considerado “elo fraco” da cadeia, sua atuação está submetida aos limites gerais do direito, especialmente aos arts. 186 e 927 do Código Civil. O compartilhamento deliberado de conteúdos falsos, difamatórios ou manifestamente inverídicos pode configurar ato ilícito civil e, em certos casos, ilícito penal.

Ao contrário da percepção comum, o anonimato absoluto não é assegurado juridicamente. Procedimentos de identificação baseados em logs, endereços IP e requisições judiciais permitem responsabilizar usuários que utilizam a internet para causar danos. A

Resolução TSE nº 23.714/2022 reforça essa lógica ao prever diligências específicas para localizar responsáveis por disseminação de desinformação eleitoral.

O dever de diligência do usuário decorre da boa-fé objetiva: exige-se um padrão mínimo de cuidado, verificar origem, plausibilidade e contexto da informação antes de compartilhá-la. Isso não significa transformar erros comuns em culpa jurídica, mas reconhecer que pode haver culpa quando o usuário, diante das circunstâncias, tinha condições razoáveis de perceber a falsidade ou o potencial lesivo do conteúdo.

2.2.2 Plataformas digitais: intermediárias e curadoras de informação

As plataformas digitais ocupam uma posição distinta: além de hospedar conteúdos de terceiros, organizam o ambiente informacional por meio de sistemas de moderação e algoritmos de recomendação. Isso lhes confere um poder significativo sobre o que se torna visível, relevante ou viral.

O art. 19 do Marco Civil da Internet adotou, originalmente, um modelo de responsabilidade reativa: as plataformas só respondem civilmente se descumprirem ordem judicial específica que determine a remoção de conteúdo. O julgamento do STF no Tema 987 (RE 1.037.396/SC) (BRASIL, 2025), porém, ajustou esse paradigma, reconhecendo que intermediários digitais possuem obrigações mínimas de cuidado, especialmente quando expostos a violações graves de direitos fundamentais.

Nos últimos anos, decisões do TSE reforçaram essa tendência, impondo remoção rápida de desinformação eleitoral, desmonetização de perfis reincidentes e medidas para impedir reiteraões. Essas decisões indicam que a diligência esperada das plataformas não se limita ao cumprimento de ordens judiciais, mas envolve a adoção de procedimentos internos razoáveis para prevenir danos sistêmicos.

2.2.3 Desenvolvedores de tecnologia: a dimensão estruturante da diligência

Desenvolvedores de sistemas e algoritmos influenciam diretamente a circulação de informações. A forma como modelos de recomendação são projetados, priorizando engajamento, tempo de visualização ou interação, afeta a probabilidade de disseminação de conteúdos enganosos. A LGPD reforça uma lógica de prevenção e segurança (art. 6º e art. 46), que, embora não nomeada como ‘privacy by design’, aproxima-se de uma exigência de governança e mitigação de riscos desde a concepção.

Uma leitura contemporânea desse enfoque preventivo permite discutir, no plano teórico e regulatório, a adoção de práticas de ‘integridade desde a concepção’ (integrity by

design), voltadas a reduzir riscos previsíveis de amplificação desproporcional de desinformação. Trata-se, contudo, de proposta ainda em construção, sem positividade específica no ordenamento brasileiro

2.3 A interdependência dos agentes e a necessidade do dever de diligência

A desinformação digital não se origina de um único agente, nem pode ser compreendida a partir de uma relação linear entre emissor e destinatário. Trata-se de um fenômeno sistêmico, cuja dinâmica decorre da interação contínua entre usuários, plataformas digitais e desenvolvedores de tecnologias que estruturam o ambiente informacional. Cada um desses atores interfere, de maneira distinta, na produção, moderação, priorização e circulação de conteúdos, o que torna a propagação de informações falsas um processo distribuído e difícil de controlar de forma isolada.

Esse caráter relacional é evidenciado por estudos recentes sobre o ecossistema comunicacional contemporâneo. Pesquisas de Mendonça et al. (2023) mostram que a desinformação tende a se espalhar em redes altamente conectadas, nas quais o comportamento dos usuários se combina com mecanismos de visibilidade definidos pelas plataformas. Não é apenas o conteúdo em si que determina seu alcance, mas a forma como algoritmos priorizam determinadas interações, replicam padrões de engajamento e favorecem mensagens emocionalmente intensas. Assim, a viralização de conteúdos enganosos resulta da combinação entre ações individuais e estruturas tecnológicas.

O reconhecimento dessa complexidade aparece também em iniciativas institucionais. A Resolução TSE nº 23.714/2022, por exemplo, parte da premissa de que o enfrentamento à desinformação eleitoral depende da atuação coordenada entre autoridades públicas e plataformas digitais, prevendo medidas de cooperação, canais de comunicação direta e procedimentos voltados à remoção célere de conteúdos sabidamente falsos. A norma não atribui responsabilidade única a nenhum agente, mas admite que a circulação de informações enganosas decorre de múltiplos fatores e exige esforços articulados.

O Supremo Tribunal Federal, ao analisar o Tema 987 (RE 1.037.396/SC) (BRASIL, 2025), também reconheceu a necessidade de compreender a desinformação dentro de uma lógica sistêmica. Embora o julgamento tenha se concentrado na constitucionalidade do art. 19 do Marco Civil da Internet, diversos votos destacaram que o ambiente digital atual envolve interações complexas entre usuários, intermediários e sistemas automatizados, e que essa estrutura influencia diretamente a forma como conteúdos ilícitos se disseminam. Trata-se de

um reconhecimento institucional de que o fenômeno não pode ser reduzido a relações bilaterais tradicionais.

No plano internacional, o DSA (Regulamento UE 2022/2065) reforça essa percepção ao prever obrigações graduais de avaliação e mitigação de riscos sistêmicos associados à circulação de conteúdos, incluindo a desinformação. O DSA (UNIÃO EUROPEIA, 2022) parte da constatação empírica de que determinados agentes possuem maior capacidade técnica e estrutural de influenciar o fluxo informacional, razão pela qual identifica a necessidade de mecanismos de cooperação e transparência entre os diferentes participantes do ecossistema digital.

A partir desses elementos, é possível afirmar que a desinformação digital se desenvolve dentro de uma estrutura interdependente, que envolve comportamentos individuais, escolhas de design tecnológico e políticas adotadas pelas plataformas. Essa constatação não implica atribuição prévia de responsabilidade a qualquer ator, mas evidencia que o fenômeno é complexo, distribuído e dificilmente solucionável por medidas isoladas. A compreensão adequada dessa dinâmica é fundamental para que, em momento posterior, o debate jurídico possa considerar de forma realista a atuação dos diversos agentes envolvidos na circulação de conteúdos.

3 O DEVER DE DILIGÊNCIA NO DIREITO BRASILEIRO E SUA TRANSPOSIÇÃO PARA O AMBIENTE DIGITAL

O enfrentamento jurídico da desinformação digital exige, antes de tudo, a compreensão dos fundamentos da responsabilidade civil no direito brasileiro. Embora o debate contemporâneo frequentemente destaque plataformas digitais, algoritmos e redes sociais, a análise não pode se desvincular das categorias tradicionais que estruturam o dever de cuidado e a obrigação de reparar danos. É a partir desses institutos consolidados que se torna possível avaliar, de maneira coerente, como o Direito responde aos danos informacionais produzidos no ambiente digital. Assim, a adaptação do dever de diligência às novas dinâmicas comunicacionais não pressupõe a criação de novos modelos jurídicos, mas a releitura de conceitos já existentes diante de riscos ampliados pela tecnologia.

Parte-se da compreensão de que o direito civil brasileiro já dispõe de instrumentos aptos a enfrentar danos decorrentes da circulação de informações no ambiente digital. A proposta deste capítulo não é introduzir novas categorias jurídicas, mas demonstrar como institutos tradicionais podem ser reinterpretados diante das transformações tecnológicas contemporâneas. Para isso, analisa-se inicialmente o dever de diligência na responsabilidade

civil clássica, identificando seus elementos estruturantes. Em seguida, examina-se a forma como esse dever é projetado no Marco Civil da Internet e na Lei Geral de Proteção de Dados Pessoais, diplomas que incorporam expectativas objetivas de cuidado no ambiente digital. Na sequência, aborda-se o debate travado no Supremo Tribunal Federal acerca do art. 19 do MCI, destacando seus impactos sobre a compreensão da diligência das plataformas. Por fim, o capítulo sistematiza critérios jurídicos que permitem aplicar o dever de diligência às dinâmicas digitais de forma proporcional, coerente com o direito civil e sensível às especificidades técnicas do ecossistema informacional.

3.1 O dever de diligência na responsabilidade civil brasileira

Antes de falar em plataformas, algoritmos ou redes sociais, é preciso voltar o olhar para a base: como o direito civil brasileiro entende o dever de diligência? É a partir dessa estrutura tradicional, que já existe há décadas, que se torna possível adaptar o raciocínio para o ambiente digital e para a desinformação. O ponto de partida está nos arts. 186 e 927 do Código Civil. O art. 186 define o ato ilícito como a conduta (ação ou omissão) culposa, por negligência, imprudência ou imperícia, que viola direito e causa dano a outrem. Nesse sentido, extrai-se desse artigo que cabe responsabilidade civil nos atos que envolverem culpa, dano e nexo de causalidade. Já o art. 927 impõe o dever de indenizar tanto nas hipóteses de culpa quanto, em determinados casos, independentemente dela, quando a atividade normalmente desenvolvida pelo autor do dano implicar risco para terceiros. Nesse desenho, o ordenamento projeta sobre todos os sujeitos um dever geral de não lesar: cada pessoa deve conduzir-se com um padrão mínimo de cuidado para não causar danos a outras.

A doutrina civilista ajuda a esclarecer o que se entende, na prática, por dever de diligência. Maria Helena Diniz (2024) explica que a responsabilidade civil não se funda, necessariamente, na obtenção de um resultado, mas na forma como o agente se comporta diante da situação concreta. O que o Direito avalia é se foram adotados os cuidados, a prudência e a atenção que razoavelmente se esperavam, considerando as circunstâncias, as informações disponíveis e os riscos envolvidos. Assim, a culpa não decorre automaticamente da ocorrência do dano, mas da omissão de precauções exigíveis ou da adoção de uma conduta pouco diligente. Trata-se de um critério objetivo de análise: não se investiga o que o agente pensou ou quis, mas se ele agiu conforme o padrão de cuidado juridicamente esperado (DINIZ, 2024).

Sérgio Cavalieri Filho (2023), ao tratar do elemento culpa na responsabilidade civil, reforça essa ideia de objetivação. Para ele, a culpa é aferida pela comparação entre a conduta

concreta do agente e um modelo de comportamento socialmente exigível, levando em conta as circunstâncias de tempo, lugar e o nível de risco da atividade. Em atividades em que o risco é maior – transporte, serviços médicos, produtos perigosos, grandes operações empresariais – a expectativa de diligência também se eleva. Esse raciocínio prepara o terreno para enxergar certas atividades digitais, notadamente as que envolvem tratamento massivo de dados e curadoria de informação, como atividades de risco relevante, nas quais o dever de cuidado é mais intenso.

Outro eixo indispensável do dever de diligência é a boa-fé objetiva, positivada pelo Código Civil em diversos dispositivos e consolidada pela doutrina como verdadeiro padrão ético-jurídico de conduta. Pablo Stolze Gagliano e Rodolfo Pamplona Filho conceituam a boa-fé objetiva como um modelo normativo que impõe deveres de lealdade, cooperação, proteção e informação, independentemente da intenção subjetiva das partes (GAGLIANO; PAMPLONA FILHO, 2025). A partir dessa compreensão, Judith Martins-Costa demonstra que a boa-fé não se limita a orientar a interpretação dos negócios jurídicos, mas atua como fonte de deveres laterais ou anexos, que não integram o núcleo da prestação principal, mas decorrem da confiança e da expectativa legítima criadas na relação jurídica (MARTINS-COSTA, 2021). Esses deveres, como o de informar adequadamente, cooperar para a realização do vínculo e evitar comportamentos contraditórios, funcionam como instrumentos concretos de diligência e têm sido reiteradamente reconhecidos pela jurisprudência do Superior Tribunal de Justiça, sobretudo em situações em que a conduta omissiva ou descuidada de um agente frustra a confiança legitimamente depositada pelo outro.

Esse movimento de expansão da boa-fé objetiva é especialmente relevante para o ambiente digital por dois motivos centrais. Primeiro, porque grande parte das interações em redes sociais, aplicativos e plataformas depende de algum grau de confiança, seja entre usuários, seja entre usuários e os provedores de serviços. Segundo, porque a lógica de funcionamento da desinformação se apoia justamente nessa confiança: conteúdos falsos ou distorcidos circulam com aparência de credibilidade, muitas vezes impulsionados por quem compartilha ou pelo próprio design das plataformas. Nesse cenário, o dever de diligência comunicacional surge como um desdobramento concreto da boa-fé objetiva: aquele que divulga ou replica informações que sabia, ou tinha condições razoáveis de saber, serem falsas ou potencialmente danosas atua de forma incompatível com o padrão de comportamento esperado no ambiente informacional digital, comprometendo a confiança mínima necessária para que ele funcione de maneira segura e íntegra.

A partir desse quadro, torna-se evidente que o próprio direito civil já fornece instrumentos suficientes para enfrentar danos decorrentes da desinformação, ainda que não empregue a expressão “dever de diligência digital”. A articulação entre o dever geral de não lesar (arts. 186 e 927), o padrão objetivo de cuidado e os deveres anexos da boa-fé permite enquadrar como culposa e, em determinadas situações, até como atividade de risco a conduta de quem, no ambiente digital, contribui para a amplificação de danos informacionais previsíveis. O desafio contemporâneo, portanto, não está em criar uma nova categoria jurídica, mas em reinterpretar institutos consolidados diante de um cenário em que alcance, velocidade e irreversibilidade das mensagens ampliam de forma qualitativamente distinta a gravidade do dano.

Assim, o dever de diligência mostra-se plenamente compatível com os desafios impostos pelo ambiente digital. Os institutos clássicos da responsabilidade civil, como a culpa, o padrão objetivo de cuidado e a boa-fé objetiva, oferecem critérios consistentes para a avaliação de condutas que resultam em danos informacionais, sobretudo quando associados ao alcance, à velocidade e ao potencial de amplificação característicos da comunicação online. Esses parâmetros demonstram que o direito civil brasileiro já dispõe de bases normativas suficientes para enfrentar situações de desinformação, ainda que não utilize expressamente a noção de “diligência digital”. Todavia, a aplicação desses fundamentos não se dá de forma abstrata ou dissociada do contexto tecnológico. Ao contrário, eles são progressivamente concretizados por diplomas legais que regulam diretamente o funcionamento da internet e o tratamento de dados pessoais. Nesse sentido, torna-se necessário avançar da construção civilista geral para a análise dos marcos normativos específicos que estruturam o ambiente digital no Brasil. É nesse ponto que se inserem o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais, os quais incorporam expectativas objetivas de cuidado e traduzem o dever de diligência em obrigações jurídicas ajustadas às particularidades do ecossistema informacional contemporâneo.

3.2 O dever de diligência no Marco Civil da Internet

O Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) não tratam diretamente da desinformação, mas oferecem parâmetros normativos que projetam expectativas objetivas de cuidado no ambiente digital. Esses diplomas partem da premissa de que a atuação de usuários, provedores de aplicação e

agentes de tratamento influencia de maneira relevante a circulação de informações, o que afasta a ideia de que o ambiente digital seria um espaço destituído de relevância jurídica.

No Marco Civil da Internet, essa dimensão aparece sobretudo em seus deveres procedimentais. A disciplina da guarda de registros, os direitos de informação e transparência assegurados ao usuário e o regime de responsabilidade condicionado à atuação do provedor revelam que intermediários digitais devem exercer um padrão mínimo de cautela. Embora o art. 19 estabeleça a necessidade de ordem judicial específica para fins de responsabilização civil, o sistema normativo evidencia que plataformas não são agentes meramente passivos, mas participantes estruturais do ambiente informacional, sujeitos a deveres proporcionais ao impacto de sua atuação.

A Lei Geral de Proteção de Dados Pessoais introduz no ordenamento brasileiro um modelo de responsabilidade civil fortemente orientado à prevenção e à gestão de riscos, que dialoga diretamente com a noção de dever de diligência. Nos termos do art. 42 da LGPD, o controlador ou o operador que, no exercício da atividade de tratamento de dados pessoais, causar dano patrimonial, moral, individual ou coletivo, em violação à legislação, está obrigado a repará-lo. A norma deixa claro que a responsabilidade não se limita a falhas pontuais, mas decorre da própria organização da atividade de tratamento, reforçando a ideia de que agentes que operam fluxos informacionais assumem deveres jurídicos proporcionais aos riscos que criam.

Esse dever é densificado pelo art. 44, ao estabelecer que o tratamento será considerado irregular não apenas quando violar formalmente a lei, mas também quando não oferecer a segurança que o titular pode legitimamente esperar, consideradas as circunstâncias do caso, os riscos razoavelmente previsíveis e as técnicas disponíveis à época. Trata-se de critério objetivo, que aproxima a LGPD do padrão civilista de aferição da culpa por violação do dever de cuidado, deslocando o foco da intenção subjetiva para a adequação da conduta diante dos riscos inerentes à atividade.

O art. 46, por sua vez, funciona como concretização técnica desse dever, ao exigir a adoção de medidas de segurança aptas a evitar acessos não autorizados, usos ilícitos ou tratamentos inadequados. A leitura conjunta desses dispositivos revela que a LGPD não institui apenas obrigações formais, mas um verdadeiro dever jurídico de diligência informacional, cujo descumprimento pode gerar responsabilização sempre que o agente deixa de adotar medidas compatíveis com os riscos previsíveis de sua atuação. Embora a lei não

tenha como objeto direto o combate à desinformação, seus parâmetros de responsabilidade incidem sobre estruturas tecnológicas que influenciam decisivamente a circulação e a amplificação de conteúdos, especialmente quando baseadas em tratamento massivo de dados pessoais.

3.3 Interseções com a Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) introduziu um modelo regulatório voltado à prevenção, à gestão de riscos e à responsabilização ativa dos agentes que realizam tratamento de dados. Embora não tenha sido elaborada com foco específico no combate à desinformação, sua estrutura normativa incide sobre elementos centrais que possibilitam a rápida disseminação de conteúdos falsos no ambiente digital. O tratamento massivo de dados pessoais, especialmente aqueles utilizados para elaborar perfis, segmentar públicos e personalizar recomendações, influencia de maneira decisiva a visibilidade, a velocidade e a persistência de determinadas informações. Ao limitar juridicamente esse tratamento, a LGPD afeta, ainda que de forma indireta, a dinâmica que sustenta a circulação de conteúdos enganosos.

3.3.1 Prevenção e gestão de riscos como fundamentos estruturantes

A LGPD consagra um modelo de responsabilidade orientado à prevenção. O art. 6º estabelece princípios como segurança, prevenção, responsabilização e demonstração de conformidade, que exigem a antecipação de riscos e a adoção de medidas adequadas antes que danos possam ocorrer. O art. 46 reforça essa lógica ao determinar a implementação de medidas técnicas e administrativas capazes de proteger dados pessoais contra acessos não autorizados e contra situações acidentais de perda, alteração ou divulgação indevida.

Esse conjunto normativo desloca o centro de gravidade para uma responsabilidade de caráter preventivo. O agente deve planejar, monitorar, registrar e revisar continuamente suas práticas. Trata-se de um modelo que se aproxima da noção civilista de diligência, mas incorpora uma dimensão organizacional própria de atividades altamente complexas e baseadas em fluxos contínuos de dados. No tema da desinformação, essa racionalidade preventiva adquire especial importância, pois muitos dos danos informacionais decorrem de escolhas estruturais das plataformas, como seus critérios de recomendação, seus mecanismos de priorização de conteúdo e a organização dos fluxos de circulação.

3.3.2 Responsabilização, prestação de contas e governança

Além da prevenção, a LGPD institui o princípio da responsabilização e prestação de contas, segundo o qual os agentes de tratamento não apenas devem cumprir a legislação, mas precisam demonstrar, de maneira concreta e documentada, que suas práticas são compatíveis com os parâmetros legais. Isso estabelece um modelo de responsabilidade ativa, que exige acompanhamento contínuo de riscos, revisões metodológicas, avaliação de impactos e justificativas transparentes quanto às decisões tomadas no tratamento de dados.

Essa lógica aproxima a LGPD de uma compreensão ampliada do dever de diligência. No ambiente digital, em que decisões automatizadas podem atingir milhões de usuários, a simples adoção de medidas pontuais é insuficiente. A legislação demanda uma postura constante de supervisão e governança, para garantir que práticas tecnológicas — como algoritmos de recomendação, sistemas de classificação ou mecanismos de priorização — não ampliem riscos informacionais previsíveis ou resultem na intensificação de conteúdos enganosos.

3.3.3 O impacto da LGPD na circulação de informações e nos riscos de desinformação

Outro ponto de interseção entre a LGPD e o tema da desinformação está no regime jurídico da tomada de decisão automatizada e do perfilhamento, previsto no art. 20. Esses mecanismos definem quais conteúdos cada usuário visualiza, em qual ordem e com qual intensidade, influenciando diretamente a experiência informacional individual. Quando utilizados de forma opaca ou sem avaliação adequada dos riscos, os sistemas automatizados podem reforçar vieses, amplificar conteúdos falsos e aumentar a vulnerabilidade de determinados grupos.

A lógica de segmentação comporta riscos próprios. Técnicas de micro direcionamento, comuns em campanhas políticas, estratégias publicitárias e conteúdos relacionados à saúde, permitem que certos grupos sejam expostos a mensagens falsas de maneira altamente direcionada, sem possibilidade de contestação pública. Nesse cenário, os princípios da finalidade, necessidade e minimização funcionam como limites jurídicos essenciais, impedindo que dados pessoais sejam utilizados de forma excessiva, desproporcional ou destinada a práticas que ampliem artificialmente o alcance de conteúdos enganosos.

Por fim, a LGPD demonstra que a proteção de dados não se limita à tutela da privacidade individual. Ela influencia diretamente a organização do ambiente informacional. Exigências de transparência, documentação e controle reduzem a opacidade de sistemas de recomendação e classificações automatizadas, dificultando que práticas tecnológicas reforcem

vulnerabilidades informacionais. Ao estabelecer padrões mínimos de governança e permitir maior auditabilidade de processos algorítmicos, a LGPD contribui para mitigar as condições que favorecem a disseminação de desinformação e reforça, de maneira indireta, o dever de diligência no tratamento e na circulação de informações.

3.4 O debate no STF sobre o art. 19 do MCI (Tema 987 da Repercussão Geral)

Desde sua formulação, o art. 19 do MCI estabeleceu um modelo de responsabilidade civil que exige que haja uma ordem judicial para que ocorra a remoção de conteúdos ilícitos propagados no meio digital. De modo objetivo, os provedores de aplicações somente poderiam ser responsabilizados civilmente em caso de descumprimento de prazo e limites estabelecidos por decisão judicial que determinasse a retirada do conteúdo. Essa disposição buscou afastar um dever geral de monitoramento, preservando a liberdade de expressão e evitando que as plataformas agissem arbitrariamente sobre a permanência de determinados temas na internet. Embora esse equilíbrio tenha sido adequado ao contexto de 2014, sua aplicação prática passou a ser questionada diante da evolução tecnológica das plataformas digitais. Em coluna publicada na *Folha de S. Paulo*, Ronaldo Lemos (2023), um dos idealizadores do Marco Civil, destaca que o art. 19 foi concebido para responder a um ambiente menos automatizado e menos estruturado por sistemas algorítmicos, razão pela qual pode apresentar limitações quando confrontado com a escala, a velocidade e o alcance sistêmico que hoje caracterizam a circulação de conteúdos online. Essa crítica não defende a superação do regime, mas explicita tensões que se tornaram evidentes no debate constitucional levado ao Supremo Tribunal Federal.

Foi nesse cenário que o STF, ao julgar o Tema 987 (RE 1.037.396/SC) (BRASIL, 2025), examinou a compatibilidade do art. 19 com a Constituição em um contexto marcado pela crescente centralidade das plataformas digitais. De um lado, argumentava-se que a exigência de ordem judicial individualizada era essencial para evitar remoções excessivas e garantir que a liberdade de expressão permanecesse protegida contra decisões privadas baseadas em critérios opacos. De outro, ressaltava-se que, em situações de grave ilicitude, a necessidade de aguardar decisão judicial poderia tornar a tutela de direitos fundamentais ineficaz, dada a rapidez com que conteúdos ilícitos se replicam em ambientes algorítmicos.

Para fundamentar essa posição, o STF interpretou o art. 19 em diálogo com parâmetros constitucionais específicos, como a liberdade de expressão (art. 5º, IV e IX), a proteção da honra e da privacidade (art. 5º, X), a garantia de acesso à Justiça (art. 5º, XXXV) e a proteção integral de crianças e adolescentes (art. 227). Essa leitura foi complementada por normas

infraconstitucionais, como os arts. 186 e 927 do Código Civil, que consagram o dever geral de não lesar, e pela Resolução TSE nº 23.714/2022, que já impunha medidas imediatas em casos de desinformação eleitoral grave. Ao afirmar que o art. 19 deve ser aplicado de maneira sistemática e constitucionalmente orientada, o Supremo reforçou que esse dispositivo não confere imunidade ampla aos intermediários, mas deve ser interpretado de modo a compatibilizar a liberdade de expressão com a necessidade de prevenir danos informacionais que se propagam com rapidez e alcançam ampla escala.

Outro ponto ressaltado pelo STF diz respeito à distinção entre *controle editorial* e *dever de cuidado*. A Corte esclareceu que exigir que plataformas mantenham mecanismos básicos de resposta a denúncias, rotinas de verificação e protocolos de prevenção não as transforma em editoras de conteúdo nem implica censura privada. Trata-se de impor um padrão mínimo de atuação diante de riscos previsíveis, sem que isso autorize a seleção de conteúdos com base em critérios ideológicos ou preferências particulares. Essa diferenciação, presente em votos de diversos ministros, reforça que o regime do art. 19 pode conviver com expectativas proporcionais de diligência, desde que mantida a autonomia comunicacional dos usuários.

Por fim, o STF reconheceu que o modelo do art. 19 não é plenamente eficaz para lidar com situações de ilicitude flagrante, nas quais o dano é imediato e sua permanência na rede amplia gravemente a violação de direitos fundamentais. Em casos como pornografia infantil, incitação direta à violência, golpes reiterados ou violações envolvendo crianças e adolescentes, a exigência de ordem judicial prévia mostra-se incompatível com a urgência da proteção. Nesses cenários, plataformas têm o dever jurídico de agir prontamente, sob pena de contribuírem para a perpetuação do dano. Essa compreensão não revoga o regime original, mas introduz uma flexibilização necessária para adequá-lo às características do ecossistema digital contemporâneo e à velocidade com que certos conteúdos ilícitos se espalham.

3.5 Critérios jurídicos para a aplicação digital do dever de diligência

A adaptação do dever de diligência ao ambiente digital exige uma abordagem que considere tanto os fundamentos clássicos da responsabilidade civil quanto as especificidades técnicas que moldam a circulação de informações online. A velocidade de propagação, a automatização de fluxos e a capacidade de amplificação dos algoritmos criam um contexto em que o potencial de dano se altera de maneira qualitativa. Por isso, a aferição da diligência não se limita à análise subjetiva das intenções do agente: depende também da compreensão das

arquiteturas tecnológicas que influenciam o alcance, a visibilidade e a replicação de conteúdos.

Nesse cenário, torna-se necessário identificar critérios que orientem quando a atuação de um agente, seja usuário, plataforma ou desenvolvedor, deve ser considerada adequada ou insuficiente para prevenir danos informacionais previsíveis. Esses critérios devem possibilitar avaliações proporcionais, compatíveis com a complexidade tecnológica e coerentes com a estrutura normativa do direito civil brasileiro. É sobre essa base que se organizam os cinco parâmetros analisados a seguir.

3.5.1 Previsibilidade do dano como critério de diligência digital

A previsibilidade do dano constitui o ponto de partida para a avaliação da diligência. Segundo os arts. 186 e 927 do Código Civil, responde quem podia, de modo razoável, antecipar que sua conduta criaria risco relevante a terceiros. No ambiente digital, essa previsão envolve não apenas o conteúdo divulgado, mas também o modo como as plataformas estruturam sua circulação, mecanismos de recomendação, replicação automática e priorização de engajamento aumentam a probabilidade de que certas informações gerem efeitos rápidos e amplos.

A dinâmica própria das plataformas, marcada por sistemas de recomendação, priorização automática e compartilhamento instantâneo, faz com que determinados conteúdos tenham um potencial muito maior de causar danos em curto espaço de tempo. Com isso, condutas que no ambiente offline produziram risco mínimo passam, no meio digital, a gerar impactos significativamente mais amplos e, sobretudo, plenamente previsíveis. A previsibilidade, nesse cenário, deixa de depender da percepção subjetiva do agente e passa a ser aferida segundo um padrão objetivo que considera o funcionamento real do ecossistema informacional. Quem compartilha, impulsiona ou hospeda um conteúdo sabe, ou deveria saber, que ele pode atingir milhares de pessoas em poucos minutos.

Esse entendimento encontra respaldo em decisões recentes. O Tribunal Superior Eleitoral, ao aplicar a Resolução nº 23.714/2022, reconhece que a circulação acelerada de conteúdos sabidamente falsos torna o dano eleitoral não apenas possível, mas altamente previsível, motivo pelo qual admite medidas céleres como remoção e desmonetização. De forma convergente, o Supremo Tribunal Federal, no julgamento do Tema 987 (RE 1.037.396/SC) (BRASIL, 2025), afirmou que as plataformas digitais são capazes de antecipar riscos decorrentes da operação de sistemas de recomendação e de ambientes com elevado

grau de viralização, especialmente quando envolvem violações graves de direitos fundamentais.

Dessa forma, o primeiro critério para a incidência do dever de diligência digital é a avaliação objetiva da previsibilidade do dano. Sempre que a dinâmica tecnológica indicar, de forma clara, que determinado conteúdo pode gerar lesões rápidas, amplas ou irreversíveis, como ocorre em temas sensíveis relacionados à violência, saúde pública, proteção de crianças e adolescentes ou processos eleitorais, surge para o agente o dever jurídico de adotar cuidados proporcionais para prevenir ou mitigar o dano. Trata-se de adaptação coerente dos institutos clássicos da responsabilidade civil às particularidades da comunicação digital, fundada na ideia de que ninguém pode se eximir da responsabilidade quando os riscos são facilmente identificáveis e tecnicamente compreensíveis.

3.5.2 Posição e capacidade técnica do agente

A posição ocupada pelo agente na cadeia informacional influencia diretamente o grau de diligência que se espera de sua atuação. O direito civil sempre reconheceu que o dever de cuidado se intensifica à medida que aumenta a capacidade técnica do agente ou o risco inerente à atividade. Sérgio Cavalieri Filho (2023) explica que a culpa consiste na violação de um dever objetivo de cuidado que o agente podia conhecer e observar. Esse dever é medido a partir de padrões socialmente razoáveis e, em atividades complexas ou especializadas, leva em conta o conhecimento técnico exigível do profissional.

Transposto para o ambiente digital, esse raciocínio significa que diferentes agentes têm deveres distintos. Usuários comuns operam com alcance e impacto reduzidos, razão pela qual o principal cuidado exigido é verificar minimamente a plausibilidade e a origem das informações que compartilham. Já plataformas de grande porte e desenvolvedores de sistemas automatizados controlam aspectos estruturais da circulação informacional. Por exercerem atividades que influenciam de forma ampla e contínua o ambiente digital, espera-se deles um nível mais elevado de precaução e de mecanismos internos capazes de evitar danos previsíveis. Em síntese, a posição e a capacidade técnica do agente calibram o padrão de cuidado exigível: quanto maior o controle sobre mecanismos de alcance, priorização e monetização, maior a expectativa de diligência e de adoção de medidas internas compatíveis com esse poder de organização do fluxo informacional.

Esse critério permite calibrar o dever de diligência digital conforme a posição ocupada pelo agente na cadeia informacional. Não se trata de instaurar uma responsabilidade automática para quem ocupa posições de maior impacto no ecossistema informacional, mas

de reconhecer que a aferição da culpa e do dever de cuidado deve considerar o tipo de atividade desenvolvida, o grau de risco que ela gera e o controle efetivo exercido sobre a circulação de conteúdos. Esse enfoque permite construir um modelo de responsabilização proporcional, coerente com os fundamentos da responsabilidade civil e sensível às assimetrias reais do ambiente digital.

3.5.3 Nexos de causalidade no ambiente digital

A análise do nexo de causalidade permanece elemento indispensável da responsabilidade civil, inclusive no contexto digital. Como sublinha Maria Helena Diniz (2024) ao tratar da fixação das perdas e danos, somente podem ser indenizados os prejuízos que constituam efeito direto e imediato da conduta ilícita (art. 403 do Código Civil). A autora ressalta, ainda, que a dificuldade de estabelecer o nexo causal não autoriza sua dispensa, posição reforçada pelo Enunciado n. 659 da IX Jornada de Direito Civil (CONSELHO DA JUSTIÇA FEDERAL, 2022), segundo o qual a complexidade fática não afasta a necessidade de examinar o vínculo causal entre a conduta e o dano. Esse entendimento é central para distinguir situações em que o prejuízo decorre efetivamente da atuação do agente daquelas em que resulta de fatores alheios à sua esfera de responsabilidade.

No ambiente digital, entretanto, a identificação desse vínculo torna-se mais complexa. A circulação de informações ocorre de forma rápida, descentralizada e potencializada por mecanismos de recomendação, o que fragmenta a cadeia causal e pode envolver diversos agentes. Esse cenário amplia o desafio probatório, mas não modifica o parâmetro jurídico: é necessário demonstrar que o dano decorre da conduta do agente de maneira direta, imediata ou, ao menos, segundo um nexo lógico e previsível. A aferição causal deve considerar as particularidades tecnológicas, como viralização, replicação automática e direcionamento de conteúdo, sem, contudo, transformar tais elementos em justificativa para afastar a responsabilidade.

A doutrina de Diniz (2024) também destaca que são indenizáveis não apenas danos emergentes, mas também lucros cessantes, desde que demonstrados com base em probabilidade objetiva e critérios de razoabilidade. Tal raciocínio permite reconhecer, no ambiente digital, hipóteses em que a atuação ilícita resulta na perda de oportunidades concretas, configurando a chamada perda da chance, desde que seja possível demonstrar que a chance existia e que sua frustração decorreu do comportamento lesivo. Assim, mesmo danos que se manifestam em fluxos informacionais fluidos podem ser juridicamente atribuídos ao agente quando demonstrado o nexo necessário entre conduta e resultado.

Dessa forma, a análise do nexo causal no ambiente digital exige atenção às particularidades tecnológicas, mas não altera o fundamento jurídico tradicional: é necessário demonstrar que a conduta contribuiu de maneira relevante para o resultado danoso, segundo critérios objetivos de previsibilidade. A fragmentação da cadeia informacional e a multiplicidade de agentes não dispensam a verificação causal; apenas tornam sua aferição mais cuidadosa. O direito civil continua a exigir vínculo lógico e adequado entre comportamento e dano, ainda que adaptado às dinâmicas próprias da circulação online.

3.5.4 Natureza da responsabilidade (objetiva x subjetiva) em cada situação

A definição sobre qual regime de responsabilidade se aplica aos agentes do ambiente digital, subjetivo ou objetivo, é ponto central para a adequada delimitação do dever de diligência. O direito civil brasileiro adota, como regra, a responsabilidade subjetiva, fundada na culpa (arts. 186 e 927, caput, do Código Civil). Somente em hipóteses excepcionais o ordenamento autoriza a responsabilidade objetiva, seja por previsão legal expressa, seja quando a atividade normalmente desenvolvida pelo agente implicar risco especial para terceiros (art. 927, parágrafo único).

No contexto da desinformação, a responsabilidade subjetiva permanece como parâmetro predominante. A avaliação da conduta, nesse modelo, exige examinar se o agente, seja usuário, plataforma ou desenvolvedor, violou o dever objetivo de cuidado, isto é, se deixou de adotar medidas razoáveis para evitar danos que eram previsíveis e evitáveis. Para os usuários, isso significa verificar se houve negligência ao compartilhar conteúdos manifestamente falsos ou potencialmente danosos. Para plataformas, a aferição envolve critérios mais complexos, como a existência de protocolos mínimos de resposta, mecanismos de detecção de ilícitos reiterados e capacidade técnica de mitigação de riscos informacionais.

A responsabilidade objetiva, por sua vez, tem incidência mais restrita. Não há, no direito brasileiro, previsão legal que estabeleça, de maneira geral, responsabilidade objetiva das plataformas de internet pela circulação de conteúdo de terceiros. Tampouco existe entendimento jurisprudencial consolidado de que a atividade típica dessas empresas — organizar fluxos informacionais, operar sistemas algorítmicos e hospedar conteúdos — constitua, por si só, atividade de risco especial nos termos do art. 927, parágrafo único. Apesar de discussões acadêmicas sobre a possibilidade de enquadramento das plataformas como desempenhando atividade de risco, o Supremo Tribunal Federal e o Superior Tribunal de Justiça ainda não adotaram essa interpretação de maneira firme e generalizável.

O Código de Defesa do Consumidor pode, em situações específicas, atrair a responsabilidade objetiva, especialmente quando há relação jurídica direta entre usuário e plataforma que se enquadra como serviço de consumo. Contudo, mesmo nessa hipótese, a responsabilização costuma recair sobre falhas do serviço (como defeitos de segurança, ausência de informações ou descumprimento contratual), e não sobre o conteúdo gerado por terceiros, cuja análise permanece submetida ao modelo de responsabilidade subjetiva.

Diante desse cenário, conclui-se que a aplicação do dever de diligência no ambiente digital deve ser orientada, como regra, pelo regime subjetivo, com graus diferenciados de exigência conforme a posição do agente na cadeia informacional e sua capacidade técnica de prever e mitigar riscos. A responsabilização objetiva permanece excepcional, restrita a hipóteses legalmente previstas ou a situações em que, após amadurecimento jurisprudencial, eventualmente se reconheça que determinadas operações tecnológicas constituem efetiva atividade de risco especial — o que, até o momento, não se consolidou no ordenamento brasileiro.

3.5.5 Proporcionalidade e gravidade da ilicitude

A aplicação do dever de diligência no ambiente digital demanda avaliar a intensidade do risco associado a cada situação concreta. O Código Civil, ao estabelecer a responsabilidade baseada na previsibilidade do dano e no dever de cuidado (arts. 186 e 927), fornece o ponto de partida para essa análise. No meio digital, contudo, o risco não depende apenas do conteúdo em si: sua velocidade de propagação, o alcance potencial e o impacto sobre grupos vulneráveis podem alterar substancialmente a gravidade da lesão. No campo do tratamento de dados, essa lógica de adequação e necessidade aparece expressamente nos princípios da LGPD (art. 6º, II e III), que exigem compatibilidade entre finalidade, meios e extensão da medida adotada. Embora a LGPD não regule a desinformação em si, seus princípios ajudam a estruturar, por analogia metodológica, uma noção de intervenção proporcional no ambiente digital.

A proporcionalidade funciona, nesse cenário, como critério de ajuste entre o risco existente e a atuação esperada do agente. Quando a probabilidade de dano é elevada, por exemplo, em situações envolvendo dados sensíveis, golpes financeiros, manipulação de informação eleitoral ou conteúdos que possam afetar a saúde pública, exige-se um nível maior de precaução. Já em contextos em que o risco previsível é limitado, a intervenção deve ser restrita ao necessário, evitando impactos desproporcionais sobre a liberdade de expressão e sobre o funcionamento das plataformas.

A gravidade da ilicitude também influencia o dever de cuidado. Quando há violação evidente de direitos fundamentais, especialmente no que diz respeito à proteção da dignidade, da infância, da integridade física ou da regularidade dos processos democráticos, espera-se que o agente adote medidas mais incisivas para impedir que o dano se consolide ou se amplifique. A rapidez com que informações circulam online torna essa atuação particularmente relevante.

A conjugação entre proporcionalidade e gravidade da ilicitude permite modular o dever de diligência conforme as características do caso concreto, preservando o equilíbrio entre proteção contra danos informacionais e respeito às liberdades comunicacionais. Trata-se de um critério flexível, que não substitui os fundamentos da responsabilidade civil, mas complementa sua aplicação na realidade tecnológica contemporânea.

A partir desses cinco critérios (previsibilidade do dano, posição e capacidade técnica do agente, nexo de causalidade, natureza da responsabilidade aplicável e proporcionalidade em relação à gravidade da ilicitude) é possível construir um modelo coerente de diligência digital. Eles permitem avaliar, com base no direito civil brasileiro, o que se espera de cada agente no ecossistema informacional e fornecem parâmetros objetivos para distinguir condutas diligentes de condutas negligentes em ambientes tecnológicos complexos. Esses critérios servirão, no capítulo seguinte, para examinar como o dever de diligência se aplica de maneira diferenciada a usuários, plataformas e desenvolvedores, conforme suas funções e capacidades específicas.

4 APLICAÇÃO DIFERENCIADA DO DEVER DE DILIGÊNCIA ENTRE OS ATORES DIGITAIS

A consolidação do dever de diligência como parâmetro jurídico para o enfrentamento da desinformação exige, nesta etapa do trabalho, a sua aplicação concreta aos diferentes atores que compõem o ecossistema digital. Após a delimitação dos fundamentos teóricos da responsabilidade civil e a identificação dos critérios jurídicos relevantes para a aferição da diligência no ambiente online, torna-se necessário examinar como esses parâmetros se manifestam de maneira distinta conforme a posição ocupada por cada agente na cadeia informacional.

Parte-se do reconhecimento de que usuários, plataformas digitais e desenvolvedores exercem papéis assimétricos na produção, organização e circulação de informações. Essa assimetria reflete diferenças significativas quanto ao grau de controle sobre os fluxos

informacionais, à capacidade técnica de prever riscos e à possibilidade concreta de intervir para evitar ou mitigar danos. Por essa razão, a aplicação do dever de diligência não pode ocorrer de forma uniforme ou abstrata, sob pena de desconsiderar as particularidades funcionais e tecnológicas que caracterizam cada agente.

O objetivo deste capítulo é, portanto, analisar como os critérios de diligência anteriormente desenvolvidos: previsibilidade do dano, posição e capacidade técnica do agente, nexo de causalidade, natureza da responsabilidade e proporcionalidade em relação à gravidade da ilicitude, incidem de maneira diferenciada sobre usuários, plataformas digitais e desenvolvedores. Busca-se demonstrar que a responsabilidade civil no ambiente digital deve ser calibrada conforme as capacidades reais de atuação de cada sujeito, evitando tanto a banalização da culpa quanto a criação de regimes de responsabilização excessivos ou incompatíveis com os fundamentos do direito civil brasileiro.

Essa abordagem permite enfrentar a desinformação de forma juridicamente consistente, reconhecendo a complexidade do fenômeno e preservando a coerência dogmática do sistema. Ao aplicar o dever de diligência de maneira graduada e contextualizada, o capítulo oferece um modelo analítico capaz de distinguir condutas juridicamente relevantes daquelas que, embora inseridas no ecossistema informacional, não podem ser legitimamente convertidas em deveres indenizatórios.

Dessa forma, o enfrentamento jurídico da desinformação exige a articulação dos deveres de diligência em diferentes níveis, de acordo com as funções exercidas por cada agente no ecossistema digital. A aplicação diferenciada desses critérios permite calibrar a responsabilidade civil conforme a capacidade real de controle, de previsão de riscos e de intervenção de cada ator, preservando tanto a proteção de direitos fundamentais quanto a coerência dogmática do direito civil brasileiro. É a partir dessa lógica que se passa à análise concreta da atuação de usuários, plataformas digitais e desenvolvedores, examinando-se, em cada caso, os contornos jurídicos do dever de diligência.

4.1 Aplicação dos critérios de diligência aos usuários

A análise inicia-se pelos usuários, que ocupam a posição mais elementar na cadeia informacional e constituem o ponto inicial da circulação de conteúdos no ambiente digital. Embora não detenham controle estrutural sobre os mecanismos de visibilidade e amplificação,

sua atuação não é juridicamente neutra. O compartilhamento de informações, sobretudo em redes sociais, produz efeitos que podem alcançar grande número de destinatários, razão pela qual o ordenamento jurídico impõe aos usuários um dever mínimo de cuidado compatível com sua posição e com os riscos previsíveis de sua conduta.

A responsabilidade dos usuários na circulação de informações digitais permanece fundada, via de regra, no regime subjetivo previsto nos arts. 186 e 927 do Código Civil. Isso significa que a responsabilização depende da demonstração de uma conduta negligente, imprudente ou imperita, isto é, da violação do dever objetivo de cuidado exigível de qualquer pessoa razoável. No ambiente digital, esse dever traduz-se na obrigação mínima de verificar a plausibilidade, a origem e o potencial dano de um conteúdo antes de produzi-lo ou compartilhá-lo. Trata-se de um padrão básico de diligência, compatível com a posição do usuário na cadeia informacional e com sua capacidade limitada de controle sobre a dinâmica tecnológica das plataformas.

A jurisprudência brasileira já reconheceu que, mesmo na ausência de intenção específica de causar prejuízo, o compartilhamento irrefletido de informações pode configurar conduta culposa quando o conteúdo apresenta sinais evidentes de falsidade ou manifesta aptidão para gerar dano. Nessas hipóteses, a dinâmica própria das redes sociais, marcada por ampla difusão e rápida replicação, torna o resultado lesivo previsível, ainda que não desejado pelo agente. A aferição da negligência, portanto, recai sobre aquilo que o usuário podia e devia saber ao interagir com determinado conteúdo, em consonância com os critérios de previsibilidade do dano e de proporcionalidade desenvolvidos no capítulo anterior.

Essa lógica fica clara em casos concretos analisados pelo Poder Judiciário. Um exemplo expressivo é o julgado do Tribunal de Justiça de Minas Gerais que tratou da divulgação não autorizada de fotografias íntimas em redes sociais (TJMG, Apelação Cível nº 1.0000.24.507120-4/001, j. 04.09.2025). Na hipótese, o usuário divulgou imagens privadas de sua ex-companheira, ocasionando ampla exposição e violação direta à honra e à intimidade. O Tribunal reconheceu que, em situações dessa natureza, o dano moral é presumido (*in re ipsa*), pois a lesão aos direitos da personalidade constitui consequência imediata e logicamente previsível da conduta. A decisão reforça que a responsabilidade civil do usuário decorre não apenas da ação voluntária, mas da previsibilidade objetiva do dano em um ambiente informacional que potencializa seus efeitos.

Além disso, o mesmo Tribunal enfrentou situação diretamente relacionada à circulação de informações falsas, ao julgar a Apelação Cível nº 1.0000.25.437086-9/001. No caso, a usuária de rede social imputou publicamente à autora a prática de crime, apresentando a

acusação como fato verdadeiro, sem qualquer comprovação. A Corte afastou a alegação de exercício regular da liberdade de expressão, destacando que a atribuição categórica de fato criminoso não se confunde com opinião ou crítica e impõe ao emissor um dever reforçado de cautela. Considerou-se que a divulgação em redes sociais amplia significativamente o alcance e os efeitos da conduta, tornando previsíveis os danos à honra e à dignidade da vítima. O Tribunal reconheceu o nexo causal entre a postagem e o prejuízo sofrido, afastando a tese de rompimento causal pela atuação de terceiros, e concluiu que a ausência de diligência mínima na verificação da veracidade da informação caracteriza ato ilícito, nos termos dos arts. 186 e 927 do Código Civil.

Em ambos os precedentes, observa-se que a atuação do usuário é avaliada não apenas pelo conteúdo veiculado, mas pelo risco inerente à sua disseminação no meio digital. A análise do dever de cuidado e do nexo causal adapta-se às particularidades tecnológicas do ambiente online, no qual a replicação é rápida, descontrolada e capaz de produzir efeitos amplos em curto espaço de tempo. Os casos demonstram, assim, que o dever de diligência mínima do usuário constitui parâmetro juridicamente exigível e que sua violação, quando associada a danos previsíveis, enseja responsabilidade civil.

4.2 Aplicação dos critérios de diligência às plataformas digitais

A atuação das plataformas digitais ocupa posição central no debate contemporâneo sobre o dever de diligência no ambiente informacional. Diferentemente dos usuários individuais, essas empresas exercem controle técnico relevante sobre a organização, a visibilidade e a circulação dos conteúdos, o que lhes confere capacidade concreta de influenciar a propagação de informações ilícitas ou danosas. Por essa razão, a análise de sua responsabilidade não pode ser reduzida à lógica da neutralidade absoluta dos intermediários.

Nesse sentido, a decisão proferida pelo Supremo Tribunal Federal no Agravo Regimental no Inquérito nº 4.923/DF (BRASIL, 2024a) oferece importante parâmetro para a compreensão do dever de diligência aplicável às plataformas. Ao examinar a utilização reiterada de ambientes digitais para a prática de ilícitos e para a difusão de conteúdos que atentavam contra a ordem democrática, a Corte deslocou o foco do julgamento do conteúdo isolado para a conduta das plataformas enquanto organizadoras do fluxo informacional. O STF assentou que a liberdade de expressão não pode ser invocada como escudo para práticas ilícitas nem impede a adoção de medidas destinadas a interromper a continuidade de condutas abusivas no ambiente digital. Conforme registrado no voto condutor, a Constituição não protege o uso das redes como instrumentos para a violação de direitos fundamentais ou para a

subversão da ordem constitucional. A decisão também deixa claro que o dever de diligência das plataformas não se confunde com censura prévia nem com a atribuição automática de responsabilidade pelo conteúdo produzido por terceiros. O que se exige é a adoção de medidas proporcionais e tecnicamente viáveis quando houver utilização reiterada da infraestrutura digital para a prática de ilícitos. Nessa perspectiva, providências como suspensão de perfis, bloqueio de canais e desmonetização não são compreendidas como controle editorial, mas como respostas legítimas diante da previsibilidade do dano e da gravidade da conduta.

Além do precedente judicial, é útil registrar a forma como o próprio STF comunicou publicamente medidas recentes de esforços relacionadas ao cumprimento de ordens judiciais por plataformas, como elemento contextual do debate. Esse entendimento foi posteriormente concretizado de forma expressiva em decisão amplamente divulgada, na qual o ministro Alexandre de Moraes, no âmbito da Petição nº 12.404/DF (BRASIL, 2024), determinou a suspensão integral do funcionamento da plataforma X (antigo Twitter) em todo o território nacional, até o cumprimento de ordens judiciais previamente descumpridas, o pagamento das multas impostas e a indicação de representante legal no país. A medida, de natureza excepcional, foi fundamentada na constatação de descumprimento reiterado de decisões do STF, bem como na tentativa deliberada da empresa de se furtar à jurisdição brasileira, inclusive com o encerramento de sua representação nacional. Segundo o relator, o Supremo Tribunal Federal esgotou previamente as vias menos gravosas, concedendo oportunidades sucessivas para que a plataforma adequasse sua conduta. Apenas diante da persistência do comportamento ilícito e da inviabilização prática da fiscalização judicial é que se adotou a suspensão temporária do serviço. A decisão também envolveu a atuação coordenada da Agência Nacional de Telecomunicações (Anatel), bem como a intimação de empresas responsáveis por sistemas operacionais e lojas de aplicativos, evidenciando que a medida não se dirigiu ao conteúdo isolado, mas à estrutura operacional que permitia a reiteração das ilicitudes.

Esse episódio ilustra de forma concreta a compreensão já delineada no Agravo Regimental no Inquérito nº 4.923/DF (BRASIL, 2024a): o dever de diligência das plataformas não se esgota na remoção pontual de conteúdos específicos, podendo abranger, em situações extremas, a interrupção de estruturas digitais que viabilizam a continuidade de práticas ilícitas. A responsabilização, nesse contexto, não decorre da mera existência de conteúdo de terceiros, mas da omissão relevante diante de riscos graves, previsíveis e reiterados, associados ao modo de funcionamento da própria plataforma.

Assim, tanto o Agravo Regimental quanto a decisão que determinou a suspensão do X contribuem para a consolidação de um modelo intermediário de responsabilização das plataformas digitais. O STF afasta simultaneamente a neutralidade absoluta e a responsabilização automática, afirmando que a atuação diligente deve ser avaliada à luz da previsibilidade do dano, da gravidade da ilicitude e do controle efetivo exercido sobre os mecanismos de circulação informacional. Trata-se de compreensão que se harmoniza com os critérios desenvolvidos no capítulo anterior e oferece base sólida para a análise da responsabilidade das plataformas no enfrentamento da desinformação.

4.3 Aplicação dos critérios de diligência aos desenvolvedores e sistemas automatizados

A inclusão dos desenvolvedores no debate sobre desinformação digital deve ser feita com especial cautela. Diferentemente dos usuários e das plataformas, esses agentes não atuam diretamente na produção, no compartilhamento ou na moderação de conteúdos específicos. Sua atividade consiste, em regra, na criação de softwares, algoritmos e arquiteturas técnicas que serão posteriormente utilizados por terceiros. Por essa razão, a responsabilização civil direta dos desenvolvedores por danos decorrentes da circulação de desinformação mostra-se, no estado atual do direito brasileiro, juridicamente excepcional e pouco provável.

A criação de um sistema tecnológico, por si só, não se confunde com a prática de um ato ilícito nem com a decisão concreta de difundir informações falsas. O vínculo entre o desenvolvimento do software e o dano final é mediado por múltiplos fatores posteriores, como o uso que plataformas fazem da tecnologia, as escolhas de moderação adotadas e o comportamento dos usuários. Essa fragmentação enfraquece o nexo de causalidade exigido pela responsabilidade civil clássica e impõe limites dogmáticos à imputação direta de dever de indenizar aos desenvolvedores. Essa constatação, contudo, não significa que o papel dos desenvolvedores seja irrelevante para a compreensão do fenômeno da desinformação. As decisões técnicas tomadas nas fases iniciais de desenvolvimento exercem influência significativa sobre o funcionamento dos ambientes digitais. Critérios de recomendação, métricas de engajamento, formas de ranqueamento e mecanismos de automação não são escolhas neutras: elas condicionam a visibilidade dos conteúdos, a velocidade de circulação das informações e a possibilidade de amplificação de mensagens enganosas. Assim, ainda que os desenvolvedores não controlem conteúdos específicos, a estrutura que projetam pode tornar determinados padrões de disseminação mais prováveis. Do ponto de vista jurídico, essa influência estrutural não autoriza a transposição automática do dever de diligência para um regime de responsabilidade civil direta. O que se identifica com maior clareza é a existência

de um campo preventivo e normativo ainda pouco explorado, situado entre o desenvolvimento técnico e a responsabilização tradicional. Trata-se de um espaço no qual as escolhas de design impactam riscos informacionais relevantes, mas não encontram correspondência clara em deveres jurídicos específicos voltados aos desenvolvedores no ordenamento brasileiro.

A legislação vigente confirma esse limite. A Lei Geral de Proteção de Dados Pessoais, embora consagre princípios como prevenção, segurança e responsabilização, direciona suas obrigações principalmente aos agentes que decidem sobre a finalidade e os meios do tratamento de dados, o que, na prática, recai sobre controladores e plataformas. Não há, no plano interno, um regime normativo que imponha deveres específicos de contenção da desinformação ou de mitigação de riscos informacionais diretamente aos desenvolvedores de software. Essa ausência revela uma lacuna relevante. O direito reconhece que arquiteturas digitais influenciam comportamentos e ampliam riscos, mas ainda não dispõe de instrumentos claros para traduzir essa influência em deveres jurídicos proporcionais e operacionais para quem projeta essas tecnologias. O resultado é um descompasso entre a relevância técnica das decisões de desenvolvimento e sua consideração jurídica, especialmente no campo da desinformação.

Dessa forma, o papel dos desenvolvedores no presente estudo não é o de potenciais réus centrais da responsabilidade civil, mas o de agentes cuja atuação evidencia os limites do modelo tradicional de imputação de danos diante da complexidade tecnológica. Reconhecer essa lacuna não enfraquece a análise jurídica; ao contrário, contribui para uma compreensão mais realista do dever de diligência no ambiente digital e aponta para a necessidade de debates futuros sobre governança tecnológica, prevenção de riscos e regulação estrutural da circulação informacional.

4.4 Modelo integrado de corresponsabilidade no ecossistema informacional

A análise do dever de diligência no ambiente digital evidencia que a circulação de informações não pode ser compreendida a partir de condutas isoladas. O fenômeno da desinformação surge de uma dinâmica complexa, na qual interagem usuários, plataformas digitais e estruturas tecnológicas subjacentes. Cada um desses agentes ocupa posição distinta na cadeia informacional e dispõe de diferentes graus de controle sobre a produção, a organização e a difusão dos conteúdos. Por essa razão, a aplicação do dever de diligência exige uma abordagem que considere essas assimetrias funcionais, sem perder de vista os critérios clássicos da responsabilidade civil.

Os usuários, conforme examinado no tópico 4.1, permanecem sujeitos ao regime subjetivo de responsabilização, fundado na culpa. O dever que lhes incumbe é compatível com sua posição limitada no ecossistema digital e traduz-se na exigência de verificação mínima da plausibilidade, da origem e do potencial lesivo das informações compartilhadas. A responsabilidade individual decorre da previsibilidade do dano e da violação do dever objetivo de cuidado, especialmente quando o conteúdo apresenta sinais evidentes de falsidade ou aptidão para causar prejuízos relevantes.

As plataformas digitais, por sua vez, assumem papel estruturalmente distinto. Como analisado no tópico 4.2, essas empresas exercem controle técnico significativo sobre mecanismos de visibilidade, recomendação, monetização e amplificação de conteúdos. Essa posição singular justifica a imposição de um dever de diligência mais intenso, avaliado à luz da previsibilidade do dano, da gravidade da ilicitude e do controle efetivo exercido sobre os fluxos informacionais. A jurisprudência constitucional recente, especialmente no âmbito do Supremo Tribunal Federal, afasta tanto a ideia de neutralidade absoluta quanto a de responsabilização automática, reconhecendo que a omissão diante de condutas ilícitas reiteradas pode adquirir relevância jurídica.

No que se refere aos desenvolvedores, conforme discutido no tópico 4.3, a imputação direta de responsabilidade civil encontra limites dogmáticos relevantes. A criação de softwares, algoritmos ou arquiteturas digitais não se confunde com a decisão concreta de difundir determinado conteúdo ilícito. A atuação desses agentes situa-se, predominantemente, em um plano estrutural e preventivo, cuja relevância jurídica se manifesta mais no campo da governança tecnológica e da avaliação de riscos do que na responsabilização reparatória. A ausência de previsão legal específica e a dificuldade de estabelecer nexo causal direto reforçam a necessidade de cautela na imputação de deveres indenizatórios a esses sujeitos.

Nesse contexto, não se propõe a criação de um modelo autônomo de responsabilidade civil, tampouco a introdução de uma nova categoria dogmática. O que se extrai da análise desenvolvida é uma leitura integrada dos deveres de diligência já existentes no ordenamento jurídico, aplicada às particularidades do ambiente digital. A consideração conjunta da atuação de usuários, plataformas e desenvolvedores permite compreender que o dever de cuidado não se manifesta de forma homogênea entre todos os agentes, nem pode ser atribuído indistintamente. Trata-se de uma construção interpretativa, fundada nos critérios clássicos da responsabilidade civil, como previsibilidade do dano, controle da conduta e risco da atividade, adaptados à complexidade do ecossistema informacional contemporâneo. Essa abordagem integrada evita soluções simplificadoras e preserva a coerência do direito civil. Ao mesmo

tempo, permite responder de forma mais precisa aos desafios impostos pela desinformação, reconhecendo que nem toda contribuição causal gera dever de indenizar, mas que a omissão diante de riscos evidentes e controláveis pode assumir relevância jurídica. O dever de diligência, assim compreendido, funciona como instrumento de calibração da responsabilidade, ajustando-a às capacidades reais de cada agente e às circunstâncias concretas do caso. Dessa forma, o enfrentamento jurídico da desinformação exige a articulação dos deveres de diligência em diferentes níveis, sem romper com os fundamentos tradicionais da responsabilidade civil. A integração desses critérios oferece um caminho dogmaticamente consistente para lidar com riscos informacionais amplificados pela tecnologia, preservando tanto a proteção de direitos fundamentais quanto a segurança jurídica necessária à atuação dos diversos agentes no ambiente digital.

5 CONCLUSÃO

A desinformação digital consolidou-se, ao longo deste trabalho, como um fenômeno jurídico complexo, que não pode ser adequadamente enfrentado a partir de soluções simplificadoras ou de modelos tradicionais aplicados de forma mecânica. A análise desenvolvida demonstrou que a circulação de informações no ambiente digital altera qualitativamente o risco de dano, em razão da velocidade, do alcance e da capacidade de amplificação proporcionados pelas plataformas e pelos sistemas automatizados. Diante desse cenário, o Direito é chamado não a criar categorias inteiramente novas, mas a reinterpretar institutos consolidados da responsabilidade civil à luz das especificidades tecnológicas contemporâneas.

Partindo da caracterização da desinformação como problema jurídico social, o trabalho evidenciou que seus efeitos ultrapassam o plano comunicacional e incidem diretamente sobre direitos fundamentais, processos democráticos e relações privadas. A análise do papel desempenhado por usuários, plataformas digitais e desenvolvedores permitiu demonstrar que a disseminação de informações falsas não resulta de uma única conduta isolada, mas de uma dinâmica interdependente, estruturada por decisões individuais, arquiteturas tecnológicas e modelos de organização informacional. Esse diagnóstico permitiu enquadrar a desinformação como fenômeno sistêmico, no qual responsabilidades não se distribuem de forma uniforme, mas se graduam conforme a posição ocupada e a capacidade real de influência de cada agente sobre os fluxos informacionais.

No plano dogmático, o estudo demonstrou que o direito civil brasileiro já dispõe de fundamentos normativos suficientes para enfrentar danos informacionais, especialmente a

partir dos arts. 186 e 927 do Código Civil, da boa-fé objetiva e do dever geral de não lesar. A contribuição central consistiu em demonstrar que o dever de diligência, tradicionalmente aplicado a atividades físicas e relações interpessoais clássicas, pode ser transposto de forma coerente para o ambiente digital, desde que observados critérios objetivos e proporcionais. A análise da doutrina civilista confirmou que a culpa não se confunde com intenção subjetiva, mas com a violação de um padrão de cuidado socialmente exigível, cuja intensidade varia conforme o risco da atividade e a posição ocupada pelo agente.

Essa base teórica foi densificada pela análise dos marcos normativos específicos do ambiente digital. O Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais revelam uma clara incorporação de expectativas objetivas de cuidado, prevenção e gestão de riscos, ainda que não tratem diretamente da desinformação. O debate constitucional travado no Supremo Tribunal Federal, especialmente no julgamento do Tema 987 da Repercussão Geral, confirmou que o art. 19 do MCI não pode ser interpretado como cláusula de imunidade ampla das plataformas, mas deve ser aplicado de maneira sistemática e constitucionalmente orientada, compatibilizando a liberdade de expressão com a proteção de direitos fundamentais diante de ilícitos graves e previsíveis.

A sistematização dos critérios jurídicos para a aplicação digital do dever de diligência representou um dos principais aportes do trabalho. A previsibilidade do dano, a posição e a capacidade técnica do agente, o nexo de causalidade, a natureza da responsabilidade aplicável e a proporcionalidade em relação à gravidade da ilicitude mostraram-se parâmetros aptos a orientar decisões jurídicas sem romper com a estrutura clássica da responsabilidade civil. Esses critérios permitem distinguir condutas meramente inseridas no ecossistema informacional daquelas que, por omissão relevante ou atuação negligente, contribuem de forma juridicamente significativa para a produção ou amplificação de danos.

A aplicação diferenciada desses parâmetros aos diversos atores digitais reforçou a necessidade de uma responsabilização calibrada. Os usuários permanecem sujeitos ao regime subjetivo, com dever de cautela compatível com sua posição limitada, especialmente quando o dano é previsível e decorre da divulgação de conteúdos manifestamente falsos ou lesivos. As plataformas digitais, por exercerem controle estrutural sobre os fluxos informacionais, assumem deveres mais intensos de diligência, avaliados à luz da previsibilidade do dano, da gravidade da ilicitude e do controle efetivo que detêm sobre mecanismos de visibilidade, recomendação e monetização. Já os desenvolvedores situam-se, predominantemente, em um plano preventivo e estrutural, cuja relevância jurídica ainda encontra limites dogmáticos

claros no ordenamento brasileiro, revelando uma lacuna regulatória que demanda reflexão futura, especialmente no campo da governança tecnológica.

Ao final, o trabalho demonstrou que o enfrentamento jurídico da desinformação não exige a criação de um regime autônomo de responsabilidade civil, tampouco a adoção de soluções maximalistas que comprometam a liberdade de expressão ou a segurança jurídica. O dever de diligência, compreendido como padrão objetivo de cuidado ajustado às capacidades reais de cada agente, oferece um instrumento dogmaticamente consistente para lidar com os riscos informacionais amplificados pela tecnologia. Trata-se de um critério de calibração da responsabilidade, capaz de preservar os fundamentos clássicos do direito civil e, ao mesmo tempo, responder de forma adequada às transformações do ambiente digital.

Nesse sentido, a contribuição deste trabalho consiste em demonstrar que o direito civil brasileiro, quando interpretado de maneira sistemática e sensível ao contexto tecnológico, possui condições de enfrentar os desafios impostos pela desinformação sem ruptura com sua tradição dogmática. O dever de diligência emerge, assim, como eixo central para a construção de respostas jurídicas proporcionais, constitucionais e compatíveis com a complexidade do ecossistema informacional contemporâneo, abrindo caminho para futuras reflexões normativas e jurisprudenciais sobre a governança da informação na sociedade digital.

REFERÊNCIAS

BRASIL. **Código Civil**. Lei nº 10.406, de 10 de janeiro de 2002. *Diário Oficial da União*: seção 1, Brasília, DF, 11 jan. 2002.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. *Diário Oficial da União*: seção 1, Brasília, DF, 5 out. 1988.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. Senado Federal. Projeto de Lei nº 2.630, de 2020. Estabelece a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. 2020. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/141944>. Acesso em: 16 nov. 2025.

BRASIL. Supremo Tribunal Federal. Agravo regimental no Inquérito n. 4.923/DF. Relator: Alexandre de Moraes. Julgado em 30 set. 2024.

BRASIL. Supremo Tribunal Federal. Petição n. 12.404/DF. Relator: Alexandre de Moraes. Julgado em 30 ago. 2024.

BRASIL. Supremo Tribunal Federal. Recurso extraordinário n. 1.037.396/SC (Tema 987 da Repercussão Geral). Relator: Dias Toffoli. Julgado em 26 jun. 2025.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.714, de 20 de outubro de 2022. Dispõe sobre o enfrentamento à desinformação no processo eleitoral. *Diário Oficial da União*: seção 1, Brasília, DF, 21 out. 2022.

MINAS GERAIS. Tribunal de Justiça de Minas Gerais. Apelação Cível n. 1.0000.24.507120-4/001. Relator: Newton Teixeira Carvalho. Julgado em 4 set. 2025.

MINAS GERAIS. Tribunal de Justiça de Minas Gerais. Apelação Cível n. 1.0000.25.437086-9/001. Relatora: Eveline Felix. Julgado em 9 dez. 2025.

CAVALIERI FILHO, Sérgio. *Programa de responsabilidade civil*. 16. ed. São Paulo: Atlas, 2023.

CONSELHO DA JUSTIÇA FEDERAL (Brasil). Centro de Estudos Judiciários. *IX Jornada de Direito Civil: enunciados aprovados*. Brasília, DF: CJF/CEJ, 2022. Disponível em: <https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf>. Acesso em: 13 nov. 2025.

DINIZ, Maria Helena. *Curso de direito civil brasileiro: responsabilidade civil*. 38. ed. São Paulo: Saraiva, 2024.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. *Novo curso de direito civil: parte geral*. 27. ed. São Paulo: Saraiva, 2025.

LEMOS, Ronaldo. Mudar Marco Civil da Internet ameaça liberdade de expressão. Folha de S.Paulo, São Paulo, 12 mar. 2023. Disponível em: <https://www1.folha.uol.com.br/ilustrissima/2023/03/mudar-marco-civil-da-internet-ameaca-liberdade-de-expressao.shtml>. Acesso em: 15 nov. 2025.

MARTINS-COSTA, Judith. *A boa-fé no direito privado: critérios para sua aplicação*. 3. ed. São Paulo: Grupo GEN, 2021.

MENDONÇA, Ricardo Fabrino; FREITAS, Viviane Gonçalves; AGGIO, Camilo de Oliveira; SANTOS, Nina Fernandes dos. Fake news e o repertório contemporâneo de ação política. *Dados – Revista de Ciências Sociais*, Rio de Janeiro, v. 66, n. 2, e20200213, 2023. DOI: 10.1590/dados.2023.66.2.301.

UNIÃO EUROPEIA. Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais). *Jornal Oficial da União Europeia*, L 277, 27 out. 2022, p. 1. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX%3A32022R2065>. Acesso em: 20 nov. 2025.