**UNIVERSIDADE FEDERAL DE SERGIPE**
**PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA**
**PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO**

LUCAS RIBEIRO DE FARIA

# **CONECTADOS E DIVIDIDOS:** o risco das redes sociais algorítmicas e a resposta do direito brasileiro para os agentes digitais

São Cristóvão/SE
2026

Lucas Ribeiro de Faria

**CONECTADOS E DIVIDIDOS:** o risco das redes sociais algorítmicas e a resposta do direito brasileiro para os agentes digitais

Dissertação apresentada como requisito parcial de exame de defesa no Programa de Pós-Graduação em Direito da Universidade Federal de Sergipe (PRODIR/UFS), para a obtenção do título de Mestre em Direito.

Área: Teoria da Constituição e Constitucionalização do Direito
Linha de Pesquisa: Constitucionalização dos Direito e Cidadania.

Orientador: Professor Doutor Lucas Gonçalves da Silva.

São Cristóvão/SE
2026

Lucas Ribeiro de Faria

**CONECTADOS E DIVIDIDOS:** o risco das redes sociais algorítmicas e a resposta do direito brasileiro para os agentes digitais

**Banca Examinadora**

_____

Prof. Dr. Lucas Gonçalves da Silva – Orientador
Universidade Federal de Sergipe – UFS

_____

Prof. Dr. Henrique Ribeiro Cardoso – Membro Interno
Universidade Federal de Sergipe – UFS

_____

Prof. Dr. Liton Lanes Pilau Sobrinho – Membro Externo
Universidade do Vale do Itajaí – UNIVALI

São Cristóvão/SE
23/01/2026

Assim como dediquei meu trabalho de conclusão de curso da graduação em direito à minha irmã Karolina, também lhe dedico essa dissertação de mestrado. Que sirva para lhe mostrar que tudo é possível, contanto que feito com amor e dedicação. Confio plenamente em você. Sei que será feliz e que terá sucesso nas escolhas que fizer. Sempre estarei ao seu lado com amor de irmão mais velho.

**RESUMO**

A presente dissertação investiga os impactos sociais, jurídicos e informacionais das redes digitais contemporâneas, com foco na atuação dos algoritmos e na responsabilidade jurídica dos agentes digitais. Partindo da hipótese de que a hiperconectividade impulsionada por redes sociais algorítmicas tem promovido a fragmentação social, a polarização política e a desinformação, o trabalho propõe um exame crítico das bases legais vigentes, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados, apontando seus limites e avanços. A pesquisa também analisa o papel dos influenciadores digitais como novos mediadores simbólicos na sociedade digital, destacando sua capacidade de moldar comportamentos, influenciar decisões e propagar conteúdos, inclusive prejudiciais. A metodologia adotada é qualitativa, de base bibliográfica e normativa, com análise crítica interdisciplinar de teorias da comunicação, do direito constitucional e da tecnologia. Ao final, propõe-se uma releitura constitucional da regulação das plataformas, visando harmonizar liberdade de expressão, proteção de dados e responsabilidade civil e penal. O estudo conclui que a responsabilização efetiva dos agentes digitais e a regulação dos algoritmos são medidas imprescindíveis para a preservação dos direitos fundamentais e da democracia no ambiente virtual.

**Palavras-chave:** Redes sociais; Algoritmos; Influenciadores digitais; Responsabilidade Jurídica; Direito digital.

***ABSTRACT***

*This dissertation investigates the social, legal, and informational impacts of contemporary digital networks, focusing on the role of algorithms and the legal responsibility of digital agents. Based on the hypothesis that algorithmic-driven hyperconnectivity fosters social fragmentation, political polarization, and misinformation, this research critically examines Brazil's current legal framework, including the Internet Civil Framework and the General Data Protection Law, identifying both its limitations and strengths. The study also explores the role of digital influencers as new symbolic mediators in the digital society, highlighting their capacity to shape behaviors, influence decision-making, and disseminate potentially harmful content. The methodology is qualitative, based on bibliographic and normative analysis, adopting an interdisciplinary approach from communication theory, constitutional law, and technology. The research proposes a constitutional reinterpretation of platform regulation, aiming to harmonize freedom of expression, data protection, and civil and criminal liability. It concludes that the effective accountability of digital actors and the regulation of algorithms are essential measures for safeguarding fundamental rights and democratic values in the digital environment.*

***Keywords:*** *Social networks; Algorithms; Digital influencers; Legal Accountability; Digital law.*

# SUMÁRIO

## INTRODUÇÃO

Este trabalho nasceu com a inquietação acerca do uso da *internet* na atualidade. Sem dúvidas existiu uma revolução tecnológica que se agudizou no Século XXI, considerando o avanço da tecnologia. Dispositivos superinteligentes, ferramentas virtuais com ultra velocidade em praticamente todos os escopos do saber humano e novas formas de relacionamentos sociais dominam o mundo moderno e se tornam cada vez mais acessíveis, principalmente através do aparelho celular que está na palma da mão.

Enquanto poucas mudanças são perceptíveis ao longo dos séculos anteriores, as mudanças nas tecnologias e na organização do tecido social que ocorreram a partir da Revolução Industrial são perceptivelmente mais rápidas, o que demonstra uma quebra de padrão em relação ao tempo que a humanidade tinha para se adaptar psicologicamente e socialmente a alterações tão drásticas.

É dizer: enquanto a humanidade caminhava lentamente com a adaptação das pouquíssimas novidades entre os Séculos XI e XII, por exemplo, as mudanças entre os Séculos XIX e XX e, principalmente, entre os Séculos XX e XXI são tão rápidas e extremas que não é possível afirmar com o grau de certeza necessário que a humanidade está preparada para acompanhá-las.

O problema pode ser analisado, o que é o escopo desse trabalho, principalmente, através do uso da *internet*, que surgiu no século passado e redesenhou as relações sociais.

Portanto, existem dúvidas que merecem, ao menos, uma tentativa de resposta. É necessário investigar: como a *internet* surgiu e transformou as relações sociais; quais os impactos que são causados nas relações jurídicas; como os algoritmos utilizados, criados e regidos por empresas direcionadas pela lógica do capital, impactam as interações entre pessoas; qual papel as redes sociais e influenciadores digitais exercem nesse processo; como o direito internacional e o direito brasileiro estão lidando com a questão; de que forma eventuais problemas podem ser sanados ou minimamente prevenidos, especialmente a partir de uma releitura constitucional que equilibre a liberdade de expressão e os direitos de personalidade.

Com esse intento, o presente trabalho foi dividido em três capítulos mais abrangentes. O primeiro capítulo preocupou-se em tratar do surgimento da *internet*, da sua evolução e da forma que influenciou na hiperconectividade social. Traçando

um panorama, especialmente, sobre o surgimento das redes sociais e de uma nova categoria profissional (influenciadores digitais), foi explorada a forma que os algoritmos e que a inteligência artificial são criados e operados para explorar a lógica do engajamento e dos números (curtidas, comentários, compartilhamentos, salvamentos e visualizações), de maneira que seja maximizada a lógica do lucro pelas empresas que atuam como agentes digitais – plataformas moderadoras de conteúdo.

O segundo capítulo ocupou-se com o conceito de sociedade de risco digital e, especialmente, da maneira abrangente que o direito vem se adequando à nova realidade. Foi objeto de estudo o Marco Civil da *Internet* (inclusive com sua recente reinterpretação operada pelo Supremo Tribunal Federal, no julgamento dos Temas 987 e 533). Além disso, buscou-se delimitar como o direito brasileiro regula os dados que trafegam na *internet* através da Lei Geral de Proteção de Dados (LGPD). Também foram delimitadas as situações que envolvem os discursos de *fake news*, de ódio e de polarização política, à luz, especialmente, do caso julgado no STF que culminou na suspensão temporária da Rede Social X (antigo *Twitter*). Em arremate, foram trazidas perspectivas regulatórias internacionais acerca do uso da *internet*, para a finalidade de estudo comparado.

O terceiro capítulo, por fim, ocupou-se com a tutela jurídica, especificamente, dos agentes digitais no direito brasileiro. As maiores áreas jurídicas foram trabalhadas de forma breve, já que o objetivo é traçar um panorama geral da regulação da *internet* no Brasil. Foram explorados, ainda que de forma mais sucinta: a responsabilização cível; a responsabilização em relações de consumo; a proteção jurídica de menores de idade e de idosos, enquanto grupos de hipervulnerabilidade digital; a responsabilização criminal; e a tutela jurídica do direito brasileiro no contexto das eleições digitais.

A metodologia adotada no presente trabalho tem escopo qualitativo, com o objetivo de entender contextos sociais, culturais e individuais através de análise bibliográfica, normativa e de julgados, especialmente oriundos do Supremo Tribunal Federal, que digam respeito aos temas abordados. A orientação é voltada a uma análise interdisciplinar que envolve as áreas aplicáveis do conhecimento humano, especialmente acerca da tecnologia, da comunicação social e do direito.

A conclusão do trabalho orienta-se pela absoluta impossibilidade de a evolução legislativa e jurisprudencial acompanhar as transformações sociais ocorridas na *internet.* Corolário, conclui-se que não é prudente depositar toda a confiança em um

sistema, através da aplicação do direito, voltado a corrigir problemas que surgiram, mas sim impor aos agentes digitais, especialmente aos provedores de conexões e de serviços representados por grandes empresas, a obrigação de evitar, prevenir ou mitigar o aparecimento de situações jurídicas que violem direitos individuais em nome de uma suposta liberdade de expressão irrestrita.

# 1 A EVOLUÇÃO DA INTERNET E A HIPERCONECTIVIDADE SOCIAL

A *internet* revolucionou a forma de se relacionar no mundo moderno, especialmente a partir do final do Século XIX. O mundo digital globalizado passa por severas alterações das estruturas econômicas e sociais através do uso da inteligência artificial, da robótica avançada, do *data science*, das *fintechs*, do uso das redes sociais e das mais diversas ferramentas digitais (Magrani, 2018).

Segundo Rosa (2012), o surgimento da internet remonta um conjunto de ideias e desenvolvimentos tecnológicos ligado ao projeto ARPANET, implementado no ano de 1969. O projeto, influenciado por teóricos como Joseph Licklider, defendia uma espécie de interação simbiótica entre humanos e computadores, conforme ideias prévias de Nobert Wiener sobre cibernética e comunicação.

O ARPANET, como parte integrante da rede da Agência de Investigação de Projetos dos Estados Unidos, surgiu durante uma disputa de domínio da geopolítica mundial com a extinta União Soviética. Foi criado como reação ao Projeto *Sputnik* (URSS), ou seja, a rede mundial de computadores tem em seu nascimento um contexto bélico da Guerra Fria, entre os anos de 1947 a 1991 (Abreu, 2009).

O ARPANET foi a primeira rede de computadores capaz de utilizar comutação de pacotes, com a comunicação direta entre máquinas geograficamente distantes, com o objetivo inicial de compartilhar recursos computacionais (Rosa, 2012).

Desde então, o surgimento da *internet* mudou a estrutura de comunicação dos veículos em massa. Se anteriormente era falado em comunicação de “um para todos”, através da *internet,* a comunicação passou a ser do tipo “todos para todos” (Lemos e Lévy, 2010). A comunicação dos veículos tradicionais, enquanto era classificada como “massiva”, deu lugar à comunicação “pós-massiva” do ambiente digital.

Nesse sentido, o surgimento da *internet* é comparável, por alguns, ao surgimento da escrita. As opções de utilização das ferramentas, de avanços tecnológicos, de hiperconectividade, são infinitas[1].

O acesso à *internet* ainda não é completamente democratizado, considerando

[1] Levy (1996, p. 41) ensina que “Considerar o computador apenas como um instrumento a mais para produzir textos, sons, ou imagens sobre suporte fixo (papel, película, fita magnética) equivale a negar sua fecundidade propriamente cultural, ou seja, o aparecimento de novos gêneros ligados à interatividade”. O computador *lato sensu*, hoje, conceito também aplicável a aparelhos móveis (celulares, por exemplo, verdadeiros microcomputadores), é um dispositivo com possibilidades praticamente infinitas de interações interpessoais e de manipulação de dados digitais.

que 50% dos lares no Brasil não tinham acesso à *internet* banda larga, de acordo com a pesquisa TIC Domicílios (Magrani, 2018). Esse acesso, entretanto, vem crescendo, considerando mesma pesquisa realizada em 2024, concluindo que o número de usuários da *internet* no Brasil chegou a 166 milhões de pessoas, equivalente a 89% da população (G1, 2024).

Com o acesso e o uso de ferramentas – como computadores e celulares – cada vez mais comum, vive-se uma sociedade em estado de hiperconectividade, onde todos precisam estar *online* a todo tempo, com suas informações pessoais e profissionais armazenadas e coletadas pelas tecnologias disponíveis.

Nessa realidade, a hiperconectividade pode ser definida como um estado permanente de disponibilidade dos indivíduos para se comunicar a qualquer momento. É ininterrupta, ansiolítica, imediata, nas comunicações entre indivíduos chamadas de pessoa para pessoa (*person-to-person*, ou P2P, na sigla em inglês), nas comunicações de pessoas com máquinas ou entre as próprias máquinas[2].

A hiperconectividade, sem dúvidas, em razão do fluxo contínuo de dados, gera profunda transformação nas relações humanas e no próprio conceito de produtividade. A sociedade hiper conectada está constantemente buscando desempenho. Nas sociedades disciplinares do passado, o controle era exercido por instâncias externas, diferentemente das sociedades atuais, com indivíduos que se auto exploram em máxima eficiência (Hansen, 2022).

A dinâmica da hiperconectividade leva a população a constante exaustão crônica, o descanso é impossível e a cobrança por produtividade é internalizada. As fronteiras entre o trabalho e a vida pessoal são diluídas para ampliar a sensação de cansaço e esvaziamento existencial (Hansen, 2022).

Tais comportamentos geram uma sensação ansiolítica mais exacerbada, com uma perda na capacidade de reflexão profunda. Significa que as pessoas, mesmo que não trabalhem ou não sejam produtivas, sentem a necessidade de manutenção da hiperconectividade, com acesso frequente a aparelhos digitais, entretanto, sem

---

[2] “O termo hiperconectividade foi cunhado inicialmente para descrever o estado de disponibilidade dos indivíduos para se comunicar a qual quer momento e tem desdobramentos importantes. Podemos citar alguns: o estado em que as pessoas estão conectadas a todo momento (*always-on*); a possibilidade de estar prontamente acessível (*readily accessible*); a riqueza de informações; a interatividade; o armazenamento ininterrupto de dados (*always recording*). O termo hiperconectividade está hoje atrelado às comunicações entre indivíduos (*person-to-person*, P2P), indivíduos e máquina (*human-to-machine, H2M*) e entre máquinas (*machine-to-machine*, M2M) valendo-se, para tanto, de diferentes meios de comunicação. Há, nesse contexto, um fluxo contínuo de informações e massiva produção de dados” (Magrani, 2018, p. 21).

considerar efetivamente o papel psíquico, profissional ou financeiro da conduta.

A hiperconectividade não redefine somente a forma de comunicação, mas a própria percepção da realidade. Os ambientes físico e digital se confundem. As tecnologias são mais que simples ferramentas, mas forças que remodelam nossa identidade e as interações sociais. Os dados são abundantes, e não escassos. As informações são imediatas. A sobrecarga cognitiva se opera através da dependência de algoritmos e sistemas automatizados que minam a autonomia e a autorreflexão humana (Souza, 2021).

O estado social de hiperconectividade gera desafios diversos, uma espécie de responsabilidade epistêmica. O problema gera discussões sobre governança de dados acerca da coleta e do controle de dados pessoais, aprofundamento de desigualdades, redução da capacidade intelectual humana e dependência psicológica de ferramentas digitais (Souza, 2021).

Não se ignora que a sociedade hiper conectada viabiliza uma democratização do acesso às informações. Todavia, o problema surge quando a promoção de conhecimento dá lugar à desinformação e à superficialidade. As redes sociais adquirem especial relevo nesse sentido, com o vício nos dispositivos tecnológicos que viabilizam a liberação constante de dopamina e que reforçam um papel social de constante validação, com estímulo de comportamentos narcisistas e prejuízo de relações interpessoais autênticas (Bürger, 2014).

A sociedade digital que está conectada através da globalização é mais suscetível a linchamentos virtuais, violação de direitos de personalidade e disseminação de *fake news*, trazendo a necessidade de pensar e adotar estratégias de filtragem e gerenciamento de informações. É legítima a preocupação sobre o impacto social da hiperconectividade, sob pena de perpetuar uma geração sobrecarregada de dados, mas vazia de sabedoria, incapaz de lidar com os desafios complexos do mundo real (Bürger, 2014).

Um aspecto que não deve ser ignorado é que as camadas sociais são heterogêneas. A hiperconectividade atinge, em especial, os mais jovens (adolescentes e crianças) e até idosos, grupos tratados pela doutrina como em estado de hipervulnerabilidade – seja pela falta de experiência e desenvolvimento mental, como os mais jovens, seja pelo cansaço da mente velha e desgastada que tem dificuldades de se adaptar à dinâmica da sociedade digital moderna.

É nesse cenário de *internet* cada vez mais democratizada, com

hiperconectividade e sem o necessário discernimento mental, que as redes sociais adquirem especial relevo com a presença de influenciadores digitais, pessoas sem um necessário filtro de responsabilidade social ou capacidade em alguma matéria de utilidade pública que contam, por vezes, com dezenas ou até centenas de milhões de seguidores que acompanham o conteúdo produzido.

## 1.1 A ascensão das redes sociais

As redes sociais, não obstante sejam frequentemente associadas ao ambiente digital contemporâneo, relacionam-se de forma profunda com a evolução da humanidade. O que hoje é tratado de forma virtualizada, na verdade, é uma necessidade existente desde as primeiras comunidades humanas de organização em redes baseadas em laços de parentesco, território ou interesses comuns, essenciais para a sobrevivência e para o desenvolvimento sociocultural (Souza, Quandt, 2008).

O nascimento[3] das redes sociais é associado ao ano de 1994, quando foi lançado na rede mundial de computadores o *GeoCities*. Tratava-se de serviço que fornecia recursos para que as pessoas criassem suas próprias páginas na *internet*.

A análise científica contemporânea dessas estruturas de organização social conta com um campo multidisciplinar, incorporando contribuições da sociologia, da psicologia e até da matemática. A metodologia conhecida como *Social Network Analysis*, por exemplo, viabiliza a formalização gráfica e quantitativa das interações humanas, transformando conceitos abstratos em modelos testáveis para compreender padrões de disseminação de informações, mobilidade demográfica e até dinâmicas de poder, questões que influenciam diretamente nas relações humanas, inclusive na utilização de redes sociais (Souza, Quandt, 2008).

As redes sociais ultrapassaram as limitações geográficas e temporais com o advento da *internet*. Hoje, possuem escala global instantânea. As Tecnologias de Informação e Comunicação reconfiguram a própria morfologia social e substituem hierarquias tradicionais por estruturas descentralizadas. Os atores dentro das redes podem ser medidos através da densidade (proporção de conexões existentes que

[3] “O ano de 1994 marca a quebra de paradigmas e mostra ao mundo os primeiros traços das redes sociais com o lançamento do *GeoCities*. O conceito desse serviço era fornecer recursos para que as pessoas pudessem criar suas próprias páginas na *web*, sendo categorizadas de acordo com a sua localização. Ele chegou a ter 38 milhões de usuários, foi adquirido pela *Yahoo!* Cinco anos depois e foi fechado em 2009” (Daquino, 2012, p. 1).

reflete o grau de coesão de uma comunidade) e através da centralidade (nós críticos para o fluxo de informações). O fato é que foi amplificada a capacidade humana de se organizar, com a introdução de novas assimetrias de poder, quando indivíduos ou instituições em posições estratégicas passaram a controlar a disseminação de ideias e recursos (Souza, Quandt, 2008).

Na sociedade das redes digitais, é difícil estabelecer fronteiras claras. As informações são fluidas e multiníveis. As análises da utilização das redes sociais também revelam fenômenos como o surgimento de indivíduos com conexões semelhantes e influências distintas. Trata-se de atores que ocupam “pontes” entre subgrupos, também chamados de *brokers*, que detêm vantagens competitivas porque controlam o acesso a informações não redundantes. Essa linha de raciocínio ajuda a entender, por exemplo, o surgimento de influenciadores digitais e a propagação de inovações (Souza, Quandt, 2008).

Como a descoberta de tecnologia, mesmo que a mais rudimentar, sempre acompanhou a evolução humana, a *internet*, especialmente em sua fase colaborativa, alterou os paradigmas da comunicação ao permitir que usuários comuns se tornassem produtores ativos de conteúdo. O *Twitter,* por exemplo, pioneiro das redes sociais e lançado em 2006, estabeleceu inicialmente o padrão de mensagens curtas (até 140 caracteres) como nova forma de interação digital através dos chamados *microblogs* (Rufino, Tabosa, Nunes, 2009).

No início dos *microblogs*, como o *Twitter*, outras concorrentes foram lançadas, hoje praticamente desconhecidos, a exemplo de *Cocoloop, Meme, Tumblr, Minixr, Jaiku* e *Plurk*. Esses concorrentes tentaram incorporar avançados recursos como compartilhamento direto de mídia e geolocalização, entretanto, não suficientes para quebrar a hegemonia do *Twitter*, cuja popularidade tinha fundamento minimalista e permaneceu até o surgimento de outras redes sociais, como *Facebook* e *Instagram* (Rufino, Tabosa, Nunes, 2009).

Em salto temporal para o início do ano de 2025, as maiores redes sociais do mundo eram: *Facebook*, com 2.74 bilhões de usuários; *Youtube*, com 2.5 bilhões de usuários; *WhatsApp*, com 2 bilhões de usuários; *WeChat*, com 1.31 bilhões de usuários e; *TikTok*, com 1.05 bilhões de usuários (*Dreamgrow,* 2025).

Foi no surgimento dos *microblogs* que começaram a se alterar as ferramentas e estratégias das empresas e celebridades em relação ao *marketing* digital. Foram nos *microblogs* os casos pioneiros de utilização corporativa para divulgação de

produtos e promoções, assim como para a utilização de artistas com a finalidade de gerenciamento de imagem e interação direta com fãs. Quando um empreendimento adota essas novas mídias, pode fazê-lo com sucesso ou com fracasso, de acordo com o engajamento e as estratégias de comunicação organizacional (Rufino, Tabosa, Nunes, 2009).

Uma relação interessante[4] pode ser feita entre tecnologia e redes sociais. As redes sociais conectam pessoas em razão de um interesse comum, ou seja, sua razão de existir não está propriamente na existência da tecnologia, mas sim na necessidade de relações humanas. A tecnologia, através das redes sociais, surge apenas como agente facilitador na criação e compartilhamento de conteúdo.

Voltando os olhos ao *Instagram,* onde se concentra a maior parte dos influenciadores digitais que atuam no Brasil, a rede social adota um *design* multimodal, com elementos como barra de rolagem infinita e algoritmos de curadoria de conteúdo que operam como sofisticados mecanismos de captura e regulação da atenção (Hissa, 2023).

É no *Instagram* que os brasileiros passam a maior parte do seu tempo *online*. A rede social conta com estratégias de arquitetura da informação que estimulam um ambiente de consumo contínuo, de forma que a organicidade aparente do *feed* (tela inicial que concentra as publicações de quem o usuário segue) esconde uma engenharia precisa de estímulos sensoriais (Hissa, 2023).

O *Instagram* combina imagens, vídeos, textos curtos e elementos interativos para produzir um fluxo ininterrupto, quando a transição entre conteúdos díspares (de publicidades a postagens pessoais) ocorre sem qualquer atrito cognitivo, favorecendo a permanência prolongada na plataforma (Hissa, 2023).

Estudos sugerem que o *Instagram* é capaz de reconfigurar as capacidades cognitivas dos usuários, especialmente em relação ao tempo de atenção e ao processamento de informações. Os estímulos fragmentados e os saltos temáticos

---

[4] “Se por um lado, redes sociais relacionam-se a pessoas conectadas em função de um interesse comum, mídias sociais associam-se a conteúdos (textos, imagem, vídeo etc.) gerados e compartilhados pelas pessoas nas redes sociais. Dessa forma, tanto redes sociais como mídias sociais, em sua essência, não têm nada a ver com tecnologia, mas com pessoas e conexões humanas. A tecnologia apenas facilita e favorece a interação das pessoas e a criação e compartilhamento de conteúdos por elas. Assim, as redes sociais, como o *Facebook*, por exemplo, são plataformas que possibilitam, facilitam e potencializam a conexão de pessoas com outras pessoas, ampliando o alcance das redes sociais pessoais, e ferramentas de armazenamento e compartilhamento que alavancam o volume de mídias sociais criadas pelas pessoas. Assim, um site de redes sociais *on-line* é apenas uma plataforma tecnológica que favorece a atuação das pessoas para interagir e compartilhar conteúdos em suas redes sociais” (Martha Gabriel, 2010, p. 202).

abruptos característicos da rolagem infinita comprometem a formação de processos mentais profundos, como a reflexão crítica e a análise contextualizada (Hissa, 2023).

Outros efeitos perversos e observáveis são a proliferação de *fake news* e a severa polarização política. Contextos sociais observáveis no Brasil possibilitam tempos de extrema divisão da população entre candidatos de pleitos eleitorais, com agressões verbais e, por vezes, físicas. As informações equivocadas são disseminadas em detrimento dos dados factíveis, demonstrando a capacidade da homofilia (tendência humana a buscar afinidades) de criação de bolhas ideológicas herméticas, onde visões dissidentes são sistematicamente excluídas. Esse cenário, além de gerar uma ameaça ao embate democrático, causa um risco social de comprometimento de valores sociais fundamentais (Kaufman, Santaella, 2020).

Diante do aumento da utilização de redes sociais, foram alteradas drasticamente as estratégias de *marketing*, com a migração de marcas dos investimentos publicitários tradicionais para as plataformas virtuais, na expectativa de aumentar o poder de persuasão orgânica a públicos específicos. Na rede digital atual, ter atenção e tempo de visualização significa ter penetração propagandística. Percebe-se uma notável tensão entre a autenticidade do conteúdo e a comercialização no fenômeno das "*publiposts*", ou postagens pagas, quando conteúdos patrocinados são mimetizados como recomendações pessoais, afastando as fronteiras entre a publicidade e a opinião genuína do influenciador (Silva, Tessarolo, 2016).

O fenômeno do uso exacerbado das redes sociais altera profundamente as noções de celebridade, sucesso e capital social, especialmente nas gerações mais jovens. Influenciadores atingiram a capacidade de rivalizar com estrelas de televisão, podendo mobilizar fãs para uma causa ou ideologia específica. A nova hierarquia de influência, construída fora dos canais tradicionais, reflete uma mudança geracional nos valores e aspirações. A capacidade de produzir conteúdo viral e cultivar uma personalidade digital são mais relevantes que conquistas em campos do saber ou da convivência humana já estabelecidos, podendo causar a banalização do conhecimento técnico e específico ou uma pressão constante por performar uma vida perfeita (Silva, Tessarolo, 2016).

As redes sociais reestruturam as dinâmicas sociais e subjetivas. O público jovem, especialmente, constantemente é estimulado a expor a vida íntima em espaços públicos digitais, transformando práticas antes privadas em conteúdos

compartilháveis. É criada uma sociedade do espetáculo, na medida em que a construção identitária passa a ser mediada pela validação alheia através de curtidas e comentários. Por outro lado, esses jovens recebem grandes estímulos nas interações humanos, desenvolvendo uma habilidade multitarefa para gerenciar diversos fluxos comunicacionais simultaneamente, o que altera profundamente suas bases cognitivas e comunicacionais (Bordignon, Bonamigo, 2017).

Desta forma, as redes sociais ampliam as possibilidades de conexão, entretanto, fragilizam vínculos presenciais. A facilidade da comunicação digital, muitas vezes, substitui encontros face a face, esvaziando a qualidade das interações. As relações de amizade se tornam mais superficiais e permeadas por interações episódicas e performáticas. Conflitos interpessoais são transferidos da vida real para o ambiente digital, através de discussões em mensagens e comentários (Bordignon, Bonamigo, 2017).

As redes sociais na era da *internet* geram dois movimentos aparentemente contraditórios: homogeneização e singularização. As redes sociais uniformizam comportamentos, criam padrões de consumo, de linguagem e de autoapresentação que os jovens tendem a seguir. Entretanto, também abrem espaços para expressões individuais e experimentações identitárias que acabam desafiando as normas sociais tradicionais (Bordignon, Bonamigo, 2017). Significa dizer que esse fenômeno revela a natureza complexa das redes como dispositivos de subjetivação, capazes tanto de reproduzir lógicas hegemônicas quanto de fomentar resistências.

Em suma, as redes sociais, apesar de frequentemente vistas como fenômeno exclusivo da era digital, se revelam como extensão contemporânea de uma necessidade humana ancestral: a conexão em rede, antes limitada por critérios geográficos ou sociais, hoje potencializada em escala global.

Se, de um lado, a *internet* democratizou a produção de conteúdo, de outro, sua arquitetura atual opera sob a lógica da captura de atenção por meio de algoritmos que personalizam experiências, ao mesmo tempo que isolam os usuários em bolhas informacionais.

Essa dinâmica gera profundos paradoxos: a conectividade ocorre sem a verdadeira pluralidade, os estímulos cognitivos fragmentados comprometem a reflexão crítica e as relações sociais são reconfiguradas com o enfraquecimento de vínculos presenciais em favor de interações performáticas.

No campo político, a homofilia e a viralização de desinformação aumentam as

polarizações e conflitos sociais, enquanto a ascensão de influenciadores digitais redefine os conceitos de fama, capital social e sucesso, priorizando imagem sobre substância.

Todavia, as redes sociais virtuais mantêm um duplo caráter: homogeneízam comportamentos e abrem espaços para singularidades e resistências. A compreensão do fenômeno exige o reconhecimento de sua natureza multifacetada, já que ao mesmo tempo que são ferramentas de relacionamentos e empoderamento com promessa de conexões universais, são também responsáveis pela fragmentação de sentidos e mercantilização da atenção.

O futuro das redes sociais depende não apenas da evolução tecnológica, mas também de como a sociedade vai negociar com os valores éticos, democráticos e fraternos em meio a tantas informações difusas.

## 1.2 Os influenciadores digitais na *internet* contemporânea

Qualquer pessoa na era da *internet* tem a capacidade de criar conteúdo audiovisual, compartilhando para seus seguidores ou para pessoas que acessem seu perfil nas redes. Diversos nichos de produção de conteúdo, com diferentes formatos (texto, vídeo, áudio), são compartilhados diariamente, com interações através de curtidas, comentários ou compartilhamentos.

Os sujeitos que se destacam através de alcance e audiência em plataformas como *blogs*, *websites* e, recentemente, redes sociais, são os novos mediadores de informação e podem ser reconhecidos socialmente como especialistas em áreas específicas.

Trata-se de pessoas com grande quantidade de seguidores que ganham confiança da audiência através de autoidentificação ou admiração dos seguidores que, diversas vezes, relacionam-se profissionalmente e comercialmente com a estrutura do mercado de consumo, através de publicidade de produtos e serviços mediante remuneração atrelada ao nível de engajamento[5].

[5] “Caracterizados por uma quantidade significante de seguidores, personalidade de marca e relações comerciais com patrocinadores os influenciadores constroem uma relação de confiança com suas audiências. Eles são um tipo de celebridade da internet, tendo em vista suas habilidades de atrair e manter um público considerável através da produção de conteúdo. Para a autora, eles constroem uma reputação positiva por meio de narrativas pessoais e cotidianas, nas quais publicidades para produtos e serviços podem estar sobrepostas” (Ribeiro, 2021, p. 272).

Nesse contexto, a ascensão de influenciadores digitais constitui uma das transformações mais significativas no ecossistema de redes sociais contemporâneas. Esses agentes midiáticos são responsáveis por reconfigurar as dinâmicas de produção, consumo e validação de conteúdo, distinguindo-se dos meios de comunicação tradicionais. O contexto de cibercultura surge com a liberação do polo de emissão da informação e com a reconfiguração de formatos midiáticos, viabilizando que indivíduos comuns galguem o *status* de celebridades e formadores de opinião, sem a mediação das estruturas tradicionais de mídia (Silva, Tessarolo, 2016).

A *internet* democratizou o acesso virtual, trazendo vasto universo tecnológico. Existe um inegável avanço na maneira como as comunicações são realizadas através de plataformas interativas. As mudanças na comunicação tornaram o conhecimento mais difuso e facilitaram a disseminação de informações de maneiras síncrona e assíncrona.

Com a difusão de redes sociais, as pessoas podem compartilhar suas opiniões e experiências de maneira autônoma. A grande quantidade de informações e o impacto das redes sociais ao influenciar muitas pessoas revelaram-se como terreno fértil para o surgimento de personalidades *online*, denominadas "influenciadores digitais" (do inglês, *"digital influencer"*). Essas pessoas têm um grande poder para atrair o público mediante produção de conteúdo publicado nas redes sociais. Suas publicações tornam-se extremamente populares e compartilhadas, com inegável alcance e impacto, influenciando milhões ou bilhões de pessoas. Como o nome indica, os influenciadores digitais têm a capacidade de afetar as ações e escolhas daqueles que os seguem, já que são também conhecidos como influenciadores de opinião (Soares, 2024).

O surgimento dessa nova categoria digital, capaz de fomentar discussões e influenciar decisões, atraiu o patrocínio de marcas e empresas que compõem o mercado. Apesar de qualquer pessoa, ao menos em teoria, poder criar conteúdo (contanto que tenha acesso às tecnologias digitais), os que ganham maior visibilidade são os que obtêm maiores patrocínios e recursos financeiros, reproduzindo ou ditando padrões culturais ou padrões estéticos dominantes (Ribeiro, 2021).

Esse fenômeno revela uma profunda transformação na economia da atenção e nos processos de construção de valor simbólico. As celebridades tradicionais, por exemplo, possuem sua autoridade derivada da associação de veículos de mídia consolidades com conquistas em campos específicos, como cinema ou esportes. Os

influenciadores digitais, por outro lado, constroem sua relevância a partir da intimidade e da aparente autenticidade das interações cotidianas com os seguidores, além das métricas de engajamento (Silva, Tessarolo, 2016).

Entretanto, a aparente democratização da mídia através dos influenciadores digitais esconde profundas contradições. Embora portem-se como “gente como a gente”, operam dentro de uma lógica comercial cada vez mais profissionalizada e distante da espontaneidade que alegam apresentar. A aparente linguagem coloquial, o aparente estilo “caseiro” de produção de conteúdo, na verdade, são estratégias cuidadosamente elaboradas para aumentar o engajamento e a identificação emocional com o público (Silva, Tessarolo, 2016).

A atuação dos influenciadores insere-se em contexto mais amplo de integração de plataformas digitais em setores econômicos diversos e nas esferas da vida cotidiana. A profissão começou a se institucionalizar com os *blogs* do final dos anos 1990, expandindo-se posteriormente para redes sociais como *YouTube, Facebook, Instagram, Twitter,* entre outras. No Brasil, somente a partir de 2015, essa categoria de “blogueiros” passou a ser designada como “influenciadores digitais” nos discursos midiáticos e sociais (Ribeiro, 2021).

A literatura costuma abordar influenciadores digitais concentrando-se nas perspectivas de estudos sobre as celebridades ou sobre trabalho digital. Contudo, nessa abordagem, a ênfase costuma recair sobre o papel dos influenciadores ao moldar suas audiências, construir visibilidade nas plataformas e operar dentro de um mercado de influência (Ribeiro, 2021). A figura do influenciador é o agente ativo que utiliza as tecnologias digitais para produzir “influência” através de um conteúdo personalizado e performance nas plataformas, calcada especialmente em alcance e engajamento (visualizações, compartilhamentos, salvamentos e curtidas) das publicações feitas no ambiente onde os usuários interagem.

Um assunto relevante e que será melhor desenvolvido nesse trabalho, em razão da influência dos formadores de opinião, é a regulamentação do conteúdo gerado e compartilhado, podendo ser citado como exemplo a divulgação de jogos de azar que impacta a sociedade de forma significativa, tema que enfrenta atualmente desafios éticos e regulatórios significativos (Soares, 2024).

É evidente que os influenciadores digitais ocupam uma posição central nas dinâmicas de comunicação da era digital, atuando como novos mediadores simbólicos entre marcas, discursos e públicos diversos. A *internet* possibilitou a democratização

da produção de conteúdo, todavia, a lógica do engajamento, da monetização e da profissionalização da atividade faz emergir uma seletividade que perpetua desigualdades e impõe desafios éticos e regulatórios.

### 1.3 Os algoritmos e a inteligência artificial na *internet*

Como visto, o avanço da tecnologia faz parte do Século XXI. Com a popularização do acesso à *internet*, hoje mundialmente estabelecida, todos têm acesso a uma infinidade de informações nos dispositivos eletrônicos. O seu uso está integrado ao cotidiano do ser humano que, no afã de resolver problemas existentes ou imaginados, utiliza da sua criatividade para desenvolver novas ferramentas de produtividade, formas de lazer, armas de guerra, técnicas de manejo agrícola, tecnologias de informática, dentre outras áreas.

No bojo das tecnologias criadas surge a Inteligência Artificial - IA, espécie de algoritmo senciente que, através de programação, consegue simular uma consciência pensante, com o objetivo primordial de ajudar nas tarefas humanas.

Segundo Russel (2013, p. 25), ao citar outros autores renomados da área, é possível extrair as seguintes definições de inteligência artificial:

> "O novo e interessante esforço para fazer os computadores pensarem (...) máquinas com mentes, no sentido total e literal." (Haugeland, 1985)
> "[Automatização de] atividades que associamos ao pensamento humano, atividades como a tomada de decisões, a resolução de problemas, o aprendizado..." (Bellman, 1978)
> "O estudo das faculdades mentais pelo uso de modelos computacionais." (Charniak e McDermott, 1985)
> "O estudo das computações que tornam possível perceber, raciocinar e agir." (Winston, 1992)
> Agindo como seres humanos agindo racionalmente "A arte de criar máquinas que executam funções que exigem inteligência quando executadas por pessoas." (Kurzweil, 1990)
> "O estudo de como os computadores podem fazer tarefas que hoje são melhor desempenhadas pelas pessoas." (Rich and Knight, 1991)
> "Inteligência Computacional é o estudo do projeto de agentes inteligentes." (Poole et al., 1998)." (Nilsson, 1998)

Trata-se a inteligência artificial (IA) de um dos mais notáveis avanços tecnológicos do século XXI, surgindo como uma ferramenta programada para simular a capacidade de pensar, atuando em atividades que exigem raciocínio, aprendizagem e tomada de decisões (Russel, 2013).

Dentre as definições possíveis de IA, é possível extrair do compilado de

Russel (2013), ao citar outros importantes autores da área, que a inteligência artificial é o campo de estudo e desenvolvimento de sistemas computacionais projetados para realizar tarefas que exigem inteligência, quando executadas por seres humanos. As máquinas, com “mentes”, no sentido figurado, são capazes de automatizar atividades associadas ao pensamento humano, como a tomada de decisões e a resolução de problemas e o aprendizado, através do uso de modelos computacionais que simulam as faculdades mentais. Entrementes, os algoritmos tornam-se capazes de perceber, raciocinar e agir, assumindo a identidade de programações que são inteligentes, agem racionalmente e desempenham funções cognitivas de forma eficaz, às vezes superando os humanos em determinadas tarefas.

Portanto, a IA moderna não é somente treinada com conteúdo pré-existente, mas possui a capacidade de gerar novas conexões entre conteúdos através de mecanismos de aprendizado e dedução lógica, através da concatenação de informações.

As máquinas dotadas de IA são capazes de simular a cognição do ser humano através de algoritmos que operam com base em modelos computacionais, simulando comportamentos inteligentes. Dessa forma, nascem com o objetivo de auxiliar nas tarefas humanas através da execução de comandos e do processamento de informações, passando por novos aprendizados e tomando decisões de maneira autônoma, dentro dos limites programados (Russel, 2013).

É seguro afirmar que as inteligências artificiais, além do avanço possibilitado pela atividade humana, também se aperfeiçoam à medida que são utilizadas, já que os algoritmos, programações básicas em código, não só viabilizam a inteligência artificial como a otimiza a cada novo erro por ela produzida (Lessa, Cabral, Silvestre, 2020).

Nesse contexto, para definir a existência de uma inteligência artificial, é possível aplicar o “Teste de Turing”, proposto por Alan Turing em 1950, sendo que o computador (aqui, conceito empregado de forma ampla) deve passar por uma série de indagações realizadas por um examinador humano que, após as respostas, não deve ser capaz de saber se foram geradas por um ser humano ou por uma inteligência artificial (Russel, 2013).

O avanço da inteligência artificial contemporânea, entretanto, permite muito mais do que a geração espontânea de textos. Os mecanismos já são capazes de reconhecer objetos, realizar conversas fluidas que emulam a experiência humana,

gerar imagens complexas e até vídeos ultrarrealistas.

Sendo ferramentas dotadas de tamanho poder, não apenas de processamento de informação, mas, principalmente, de criação de informação, os algoritmos integrados às redes sociais ficam cada vez mais inteligentes, absorvendo informações, conectando-as e corrigindo os próprios erros, o que gera uma profunda alteração na forma de utilizar e perceber o espaço digital.

Os algoritmos funcionam nas redes sociais com caráter preditivo e não ideológico. Os sistemas de *deep learning* baseados em redes neurais analisam padrões de comportamento para personalizar conteúdos, entretanto, sem intencionalidade política inerente. Os algoritmos classificam informações com base em relevância calculada por métricas como tempo de interação e histórico de engajamento, sendo que os vieses existentes derivam de dados de treinamento enviesados (Kaufman, Santaella, 2020).

Isso porque os algoritmos operam sob a lógica da personalização e do impulsionamento de conteúdo. O usuário vê conteúdo semelhante àquele que mais o prende em tempo de tela. Ou seja: se o usuário de rede social passa mais tempo olhando vídeos com animais, o algoritmo necessariamente entregará conteúdo semelhante (vídeos de animais). O problema surge quando o conteúdo visualizado diz respeito a desinformação, a ilícitos ou a condutas moralmente reprováveis, situação em que o algoritmo entregará conteúdo negativo semelhante, favorecendo a criação de verdadeiras “bolhas” informacionais que reforçam um mau comportamento e a ignorância de outras perspectivas sobre um mesmo assunto[6].

Esse processo de aceitação passiva dos conteúdos sugeridos pelos algoritmos ocorre em razão da fadiga mental dos usuários, sobrecarregados por fluxos informacionais caóticos, de forma que o julgamento crítico é deturpado. Ocorre uma espécie de “redesignação cognitiva” que se agrava pelo caráter cada vez mais comercial da plataforma (Hissa, 2023). Se o valor está na atenção, a rede social mais utilizada pelos brasileiros não escapa da mercantilização. Quando a utilização é gratuita, o usuário é o produto.

Os algoritmos de personalização são programados não como meros

[6] “Os algoritmos de redes sociais têm a função de personalizar o conteúdo apresentado aos usuários, com base em seus interesses e comportamentos. Inicialmente, os algoritmos buscavam compreender os usuários e ofertar aos anunciantes um público mais segmentado, dando mais efetividade à publicidade nas redes” (Rocha, 2024, p. 24).

facilitadores técnicos, mas para agir como agentes ativos na construção de realidades digitais particulares. O conteúdo semelhante consumido e distribuído pelo algoritmo enseja a criação de uma bolha informacional hermética, quando os usuários são progressivamente isolados de perspectivas dissonantes. Não existe acesso algorítmico à pluralidade de ideias, mas sim um padrão de desejos, comportamentos e de visões de mundo. As redes sociais prometem conexão com a diversidade global, mas paradoxalmente reforçam visões unidimensionais e preconceitos já existentes (Hissa, 2023).

Na *internet* contemporânea, as redes sociais são regidas por algoritmos de inteligência artificial que moldam a experiência do usuário e a própria estrutura das interações sociais. Esses sistemas operam com mecanismos invisíveis de curadoria, os chamados *machine learning* e *deep learning*. Essas programações atuam nas redes neurais biológicas e processam vastos conjuntos de dados, identificando padrões e prevendo comportamentos (Kaufman, Santaella, 2020).

O resultado dos algoritmos atuantes nas redes sociais é que cada usuário vê um conteúdo personalizado na própria rede. Essa personalização, não obstante a eficiência em termos de engajamento, cria um inegável paradoxo: de um lado, facilita o acesso a informações relevantes; de outro, limita a exposição do usuário a perspectivas diversas, reforçando vieses cognitivos e alimentando a ignorância (Kaufman, Santaella, 2020).

Os algoritmos, inegavelmente ferramentas poderosas para organização de informações, podem constituir vetores de manipulação e fragmentação social. Como funcionam sob uma lógica preditiva que privilegia a relevância em detrimento da diversidade, os conteúdos são ranqueados com base em afinidades prévias do usuário. Esse processo ignora causalidades e a experiência humana em favor de correlações estatísticas, gerando um ciclo de retroalimentação: quanto maior a interação de um indivíduo com o conteúdo, mais o algoritmo fornece material semelhante (Kaufman, Santaella, 2020).

O processo de consumo de conteúdo idêntico aumenta o tempo de permanência na plataforma que o exibe. Trata-se, na verdade, do objetivo principal das empresas de tecnologia: reter a atenção. Os efeitos colaterais são graves, visto que a dependência de redes sociais gera um isolamento intelectual e uma fragilização dos laços humanos (Kaufman, Santaella, 2020).

A falta de transparência algorítmica viabiliza a inexistência de

responsabilização jurídica, que poderia, se existente, mitigar danos à democracia. As redes sociais atuam na modernidade como verdadeiras entidades que controlam o acesso a recursos, informações ou oportunidades, decidindo quem entra e quem não entra no jogo virtual. Não seguem parâmetros jornalísticos, mas sim métricas de rentabilidade sem regulação ou alfabetização midiáticas necessárias (Amaral, Santos, 2019).

Além disso, os algoritmos podem gerar preocupantes efeitos colaterais, especialmente em relação à formação das chamadas câmaras de eco. Os conteúdos alinhados às preferências do usuário, ao serem priorizados, limitam a exposição a perspectivas divergentes, reforçando a polarização (Kaufman, Santaella, 2020).

A tendência do ser-humano de interagir com ideias semelhantes é um fenômeno exacerbado pela lógica de maximização de engajamento das plataformas. Os algoritmos guiam-se pela economia (no sentido de atividade mercantil) da atenção, quando os usuários são expostos a informações que apenas confirmam e validam sua forma de ver o mundo, prejudicando a divergência e o contraditório[7]. É possível, inclusive, uma programação preditiva, para que o algoritmo consiga, com base em estatísticas, saber qual conteúdo é mais provável de ser consumido por relevante espaço de tempo por aquele usuário, vinculando pessoas com a mesma preferência de conteúdo em comunidades que podem compartilhar visões de mundo distorcidas, extremistas ou negacionistas.

A rede social *Instagram*, em 2016, passou a contar com o uso de algoritmos no *feed*, página que engloba as publicações feitas pelos usuários. A mudança do método pode ser comparada à lógica *EdgeRank* do *Facebook,* quando a ordem cronológica de publicações foi substituída por critérios de relevância baseados em afinidade, peso do conteúdo e temporalidade (Freitas, Borges, Rios, 2016).

A opacidade algorítmica revela-se como problema porque os critérios de relevância na filtragem de conteúdo não são transparentes, não sendo possível aos usuários que consigam discernir quais conteúdos são suprimidos ou promovidos. O

[7] “Porém, esta ferramenta cria também um ambiente no qual os usuários são expostos principalmente a informações que confirmam suas crenças e interesses preexistentes. Embora os algoritmos não impeçam que os usuários busquem ativamente por outros tipos de conteúdo, eles criam filtros que tendem a simplificar e facilitar a navegabilidade do usuário e a interação. Os algoritmos conseguem até mesmo ser preditivos, com bases estatísticas, em relação ao que iremos consumir, sejam produtos ou notícias. Tais filtros dos algoritmos podem resultar na formação de comunidades que compartilham percepções semelhantes de realidade, mesmo que distorcidas, negacionistas ou extremistas” (Rocha, 2024, p. 24).

interesse comercial das plataformas revela uma tendência ao favorecimento de perfis que investem mais em anúncios, monetizando a visibilidade (Freitas, Borges, Rios, 2016).

Além das já mencionadas medidas de educação digital e regulamentação dos algoritmos utilizados, uma possível solução seria permitir aos usuários o uso de mecanismos de ajuste manual, como a opção de desativar filtros. A ausência de personalização e a falta de uma regulação eficaz tornam os algoritmos subordinados à lógica de mercado, e não ao interesse público (Freitas, Borges, Rios, 2016).

No âmbito da educação, os algoritmos trazem desafios significativos diante da fragmentação da atenção e da dificuldade de filtrar informações confiáveis. As plataformas são arquitetadas para viabilizar recompensas variáveis e promover vícios comportamentais, reduzindo a capacidade de concentração dos estudantes. Estima-se que 97,7% dos universitários utilizam as redes sociais durante as aulas, prejudicando a assimilação de conteúdos em razão da economia do engajamento que prioriza interações superficiais em detrimento de aprendizados profundos (Santos, 2022).

Soluções propostas para mitigar o problema perpassam desde a assunção do professor de um papel de “curador de informações”, quando guia os alunos na avaliação crítica de fontes, até uma inclusão de alfabetização algorítmica nos currículos para que os alunos compreendam como as plataformas moldam seu acesso ao conhecimento. A assimetria de poder entre educadores e gigantes tecnológicas, cujos modelos de negócio dependem de uma contínua atenção dos usuários, entretanto, torna a tarefa complexa e desafiadora (Santos, 2022).

Porém, não existem apenas efeitos negativos. Os algoritmos também melhoram a experiência do usuário ao filtrar o excesso informativo. Contudo, a opacidade e dependência nas redes dependem da materialização de políticas de transparência. A educação digital ou o desenvolvimento de algoritmos éticos podem ser caminhos a serem adotados para reduzir danos, já que a autorregulação das plataformas tem se mostrado como caminho insuficiente (Kaufman, Santaella, 2020).

Em suma, o avanço da inteligência artificial dos algoritmos nas redes sociais representa um paradoxo do Século XXI: enquanto potencializam a eficiência informacional e a personalização dos conteúdos, geram distorções profundas na circulação do conhecimento e no tecido social. A Inteligência Artificial evoluiu de meros sistemas de processamento para ferramentas que são capazes de emular

cognição humana, aprendizado autônomo e a criação de conteúdos complexos. No entanto, a aplicação da IA nas redes sociais orientada por lógicas mercadológicas do engajamento amplificou fenômenos como a desinformação, a polarização e a fragmentação da atenção.

A economia da atenção encontra suporte nos algoritmos preditivos, substituindo a mediação ética do jornalismo por um ecossistema em que emoções e vieses determinam a viralidade, não a veracidade. Essa dinâmica criou bolhas cognitivas que isolam os indivíduos em suas narrativas autorreferenciais, inviabiliza o debate público e compromete a própria noção de verdade objetiva.

A solução não parece ser possível no retrocesso tecnológico. Talvez esteja na correção de rumos. Algoritmo não pode ser tratado como neutro, eis que reflete as escolhas humanas previamente feitas na sua concepção.

# 2 A REGULAÇÃO DAS REDES SOCIAIS DIGITAIS EM RAZÃO DO RISCO

## 2.1 A redação original do Marco Civil da *Internet*

O Marco Civil da *Internet* (Lei 12.965/2014) sem dúvida é um ponto de inflexão normativo para a regulamentação do ambiente digital no Brasil. A lei, em sua redação original, estabeleceu parâmetros claros para a responsabilização civil dos provedores de *internet*, principalmente nos casos de conteúdos ofensivos gerados por terceiros nas redes sociais (Dutra, Silva, 2016).

A mencionada lei surgiu como uma tentativa de equilibrar a liberdade de expressão com a proteção da intimidade, consagrando a privacidade como princípio basilar[8] do uso da *internet* no Brasil (Barreto Júnior, Gallinaro, Sampaio, 2018). A liberdade de expressão no direito brasileiro estaria mais afinada com o direito germânico, quando não está resguardada absolutamente e previamente na arquitetura dos direitos fundamentais, já que a própria Constituição Federal de 1988 assegura a inviolabilidade dos direitos à privacidade, à intimidade, à honra e à imagem, além de garantir o direito à indenização em caso de violações e consagrar o direito de resposta proporcional ao agravo (Sarlet, 2015).

Outros apontam que a lei surgiu em razão de demandas de regulamentação do ambiente digital brasileiro, com o estabelecimento de parâmetros claros para a atuação dos diversos agentes envolvidos no uso da *internet*. Teria sido adotada uma perspectiva principiológica, com fundamento na neutralidade da rede, na liberdade de comunicação e na proteção de dados pessoais, para tentar proteger direitos fundamentais, como privacidade e honra, através de uma aplicação relativamente flexível das normas (Leite, 2016).

A *mens legis* busca atender à necessidade de equilibrar direitos fundamentos em conflito, como a liberdade de expressão, a proteção à honra, a privacidade e a intimidade dos usuários. O objetivo maior é tutelar a liberdade da expressão no uso da *internet*, cotejando-a com a preservação da privacidade, sem que a balança se

[8] A Lei 12.965/2014 prevê, no art. 3º, os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; IV - preservação e garantia da neutralidade de rede; V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; VII - preservação da natureza participativa da rede; VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

desequilibre para a ausência de privacidade ou para a censura[9].

A necessidade de atualização legislativa surgiu porque a *internet* se transformou em um "segundo mundo virtual" onde a privacidade enfrenta, diuturnamente, desafios sem precedentes, especialmente em razão da massificação das redes sociais e da coleta massiva de dados pessoais (Barreto Júnior, Gallinaro, Sampaio, 2018).

Sobre esse ponto, o conflito entre privacidade e direito ao uso da *internet* ganhou especial tônica nos casos de divulgação não autorizada de conteúdo íntimo, viabilizando uma viralização (espalhamento descontrolado da informação) de conteúdo que pode destruir a intimidade de uma pessoa em segundos. A *internet* desafia o próprio conceito de privacidade, sendo necessária uma verdadeira redefinição do controle sobre os próprios dados, algo difícil de garantir em um ambiente de replicação infinita de informações (Barreto Júnior, Gallinaro, Sampaio, 2018).

Foram estabelecidos pela legislação em comento princípios específicos acerca da finalidade da coleta de dados, do consentimento livre e informado e a possibilidade de exclusão definitiva das informações ao término da relação contratual. Em diversos aspectos, foram antecipados muitos pontos da posterior Lei Geral de Proteção de Dados – LGPD. Nesse ínterim, especialmente relevante é a previsão sobre a guarda de registros de conexão[10], limitando temporalmente a retenção desses dados e exigindo autorização judicial para o acesso, salvaguardando vigilância indiscriminada e conferindo maior controle aos usuários sobre suas informações pessoais (Leite, 2016).

Existem plataformas, como o *Facebook*, por exemplo, que operam sob a lógica de vigilância e extração de dados. Referidos dados são compartilhados com terceiros sem consentimento, constituindo paradigmático exemplo de violação massiva da privacidade e de insuficiência de garantias legais vigentes (de Macedo Menna Barreto, 2015).

---

[9] "O fundamento do Marco Civil da *Internet* é a liberdade de expressão, sendo que as regras para o uso da Internet no Brasil. Ou seja, a liberdade de expressão é a base a ser observada para o regramento fixado para o ambiente virtual. [...] No entanto, o exercício da liberdade de expressão pode trazer algum prejuízo para a privacidade. O contrário também é verdadeiro: a preservação da privacidade pode trazer perdas à liberdade de expressão, uma vez que pode haver censura" (Teixeira, 2016, p. 18).

[10] O art. 7º da Lei 12.965/2014 dispõe como direitos do usuário a proteção aos registros de conexão e aos registros de acesso e aplicações da internet (inciso VI), assim como o não fornecimento a terceiros dos seus dados pessoais, inclusive os registros de conexão (inciso VII).

A nova lei optou por adotar um sistema de responsabilidade subjetiva para os provedores de aplicações, contanto que condicionada ao descumprimento de ordens judiciais específicas. Desta forma, percebe-se um esforço legislativo para evitar a censura prévia, mas garantindo mecanismos eficazes de reparação aos ofendidos. Referida abordagem demonstra a tentativa de adaptar o ordenamento jurídico às complexidades da sociedade da informação atual, de maneira que a rápida disseminação de conteúdos exige respostas ágeis, sem sacrificar garantias processuais (Dutra, Silva, 2016).

Ademais, com o Marco Civil, foi realizada uma distinção entre provedores de conexão e aplicativos. Os provedores de conexão são isentos de responsabilidade por conteúdos de terceiros, considerando que atuam como meros intermediários técnicos. Já os aplicativos – como plataformas de redes sociais – podem ser responsabilizados civilmente, caso sejam notificados judicialmente e não removam o conteúdo ofensivo no prazo estabelecido (redação original da lei)[11].

Dessa forma, existe uma distinção entre os provedores de conexão ou de serviços, que intermediam as informações entre a operadora e o usuário do serviço, e os provedores de conexão, que alcançam o usuário diretamente no acesso à rede[12].

A distinção entre provedores de conexão e aplicativos revela-se como prudente não apenas para preservar a neutralidade da rede e evitar ônus excessivos aos provedores, mas também para viabilizar às possíveis vítimas que tenham um canal eficiente de reparação (Dutra, Silva, 2016), já que a neutralidade da rede é abordada no art. 9º do Marco Civil da *Internet*. Entretanto, sua efetividade é relativizada diante de exceções previstas nos parágrafos do próprio artigo, que autorizam a discriminação ou degradação do tráfego em situações técnicas ou de emergência, através de regulamentação posterior por decreto.

---

[11] Merece menção que a Lei 12.965/2014, apesar de prever na Seção III a responsabilização dos aplicativos por danos realizados por terceiros, prevê no art. 21 uma exceção à necessidade de decisão judicial. Dessa forma, o provedor de aplicações também responde por danos causados em casos de divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado, se for notificado pelo participante ou representante legal e não promover, de forma diligente, a indisponibilização do conteúdo.

[12] “Estes provedores, chamados de provedores de conexão ou provedores de serviços, são os responsáveis pela intermediação entre a operadora e o usuário do serviço contratado. Nesta modalidade de provedor, é oferecida a conexão à Internet conforme especificidades e velocidades contratadas e o acesso pode ser feito através de uma identificação de usuário e senha, por exemplo. Os provedores de conexão são os responsáveis por alcançar ao usuário diretamente o acesso à rede” (Serro, 2015, p. 5).

Para Tomasevicius Filho (2016), essa fórmula legislativa torna incerto o alcance do princípio da neutralidade e, além disso, gera insegurança jurídica porque não há garantia de que os dados trafeguem sob o mesmo regime fora do território nacional. Nessa hipótese, a neutralidade assumiria caráter puramente retórico, incapaz de produzir qualquer impacto substancial no uso das redes.

Não obstante, a intenção da dinâmica de responsabilização das redes sociais prevista no Marco Civil da *Internet* é estabelecer um regime de responsabilidade dos provedores, de forma que tanto se evite a censura indiscriminada quanto a impunidade por danos decorrentes de conteúdos ilícitos (Leite, 2016). A redação do art. 19 da Lei 12.965/2014 adotou um sistema misto de notificação e remoção judicial, quando as plataformas deveriam ser responsabilizadas somente após o descumprimento de decisão judicial que imponha a remoção de dados, ressalvada a já mencionada exceção prevista no art. 21 da mesma verba legislativa.

Parte da doutrina, contudo, criticava a redação do art. 19 da Lei 12.965/2014[13] em relação à responsabilização civil de provedores por danos derivados de conteúdos gerados por terceiros. Apontava-se que a posição adotada pela norma permitia um desequilíbrio entre a proteção conferida aos provedores de aplicação e a tutela dos direitos fundamentais das vítimas. A exigência de ordem judicial específica como um requisito de responsabilização civil seria um mecanismo ineficaz para viabilizar a tutela da honra, da privacidade e da imagem dos indivíduos, notadamente diante da celeridade e do alcance exponencial da propagação de danos na *internet* (Schreiber, 2015).

Com efeito, o contexto do Marco Civil da *Internet* revela que a lei foi redigida sob o fundamento de que promoção da hierarquização dos direitos fundamentais, ainda que implicitamente. Para Teffé e Moraes (2017), existe uma preferência legislativa pela liberdade de expressão em detrimento da tutela adequada da privacidade e da dignidade da pessoa humana. Esses direitos, que devem coexistir e ser ponderados caso a caso, passam por conflito hermenêutico quando analisados de acordo com o art. 19 da lei, redigido para favorecer a manutenção de conteúdos

[13] A redação exata do art. 19 da Lei 12.965/2014: “Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário”.

ofensivos sob o pretexto de evitar a censura, diante da exigência de ordem judicial específica para a remoção compulsória pelos provedores de aplicação.

Antes do advento do Marco Civil da *Internet*, a jurisprudência brasileira já admitia a responsabilização objetiva de empresas proprietárias de redes sociais, especialmente em casos de omissão, quando cientes, na remoção de conteúdo lesivo. Adotava-se implicitamente o sistema de *notice and take down*[14], que se revelava mais dinâmico do que a nova exigência de judicialização como condição para a responsabilização civil. A posterior imposição da judicialização como condição para a responsabilização civil, rompendo com a evolução jurisprudencial pré-existente, segundo alguns críticos, configurava-se como retrocesso normativo e axiológico que desrespeita o princípio da vedação do retrocesso social em matéria de direitos fundamentais (Schreiber, 2015).

Segundo Schreiber (2015), o art. 19 do Marco Civil da *Internet* criou um regime de "blindagem das plataformas digitais", de forma que a vítima deve se submeter a um processo judicial prévio mesmo em situações em que a lesão à personalidade é indubitável. A sistemática violaria o princípio da reparação integral das vítimas prevista no art. 5º, inciso X, da Constituição Federal, e subverteria a lógica do acesso à justiça por criar uma condição de procedibilidade em detrimento de um direito da parte ofendida. Ainda segundo o autor, é um grande contrassenso que a norma permita que conteúdos que ofendam direitos autorais gozem de maior proteção que conteúdos que atentem contra os direitos de personalidade, em situação clara de inversão da hierarquia axiológica das normas.

Ainda segundo Schreiber (2015), o art. 19 do Marco Civil da *Internet* deveria ser interpretado à luz do art. 5º, inciso X, da Constituição Federal e do próprio art. 21 da mesma lei (trata da responsabilização pela veiculação de cenas íntimas). A possibilidade de notificação extrajudicial, valendo-se do já mencionado "*notice and take down*", seria medida que melhor harmoniza os valores constitucionais com a norma infraconstitucional. Referida exegese normativa permite resgatar a eficácia protetiva do ordenamento jurídico diante dos desafios postos pelas redes sociais modernas, reafirmando o papel do direito como verdadeiro garantidor da dignidade no

[14] Em tradução livre, a expressão significa "observe e retire", expressão que faz referência à possibilidade anterior à promulgação do Marco Civil da *Internet*, quando as plataformas precisavam remover o conteúdo imediatamente após a percepção da publicação indevida, sob pena de serem responsabilizadas judicialmente, independentemente de decisão judicial prévia.

ambiente virtual.

Como se vê, o avanço legislativo manteve a necessidade de ordem judicial específica para a remoção de conteúdos que não são excepcionalizados no art. 21 da Lei 12.965/2014. Tal medida, apesar de resguardar o devido processo legal, poderia mostrar-se excessivamente morosa em situações que demandem urgência como, por exemplo, os discursos de ódio ou a propagação de *fake news*. Além disso, a exigência de que a decisão judicial identifique de forma clara e inequívoca o material ofensivo pode criar obstáculos práticos em plataformas com alto volume de publicações (Dutra, Silva, 2016).

Não são incomuns casos em que existe uma flagrante dificuldade em responsabilizar civilmente os provedores de aplicação de *internet* pelo conteúdo gerado por terceiros, visto que a exigência de ordem judicial como condição para a responsabilização civil depende da capacidade do ofendido de identificar e acionar judicialmente os infratores, mesmo diante de conteúdos indevidamente publicados que violem gravemente sua intimidade, honra ou imagem (Teffé, Moraes, 2017).

A exigência de ordem judicial prévia, enquanto mudança normativa que rompeu com entendimento jurisprudencial anteriormente dominante, especialmente do Superior Tribunal de Justiça, poderia contribuir para o aumento de práticas abusivas no ambiente digital, eis que afasta o estímulo à autorregulação eficaz (Tomasevicius Filho, 2016). Anteriormente à redação da lei, a jurisprudência brasileira costumava orientar-se pela aplicação do “dever de diligência dos provedores”.

Em relação, especificamente, aos conteúdos íntimos gravados ou divulgados sem consentimento, as notificações extrajudiciais para a remoção podem ter sua efetividade condicionada à cooperação voluntária de provedores, sem mecanismos robustos ou modernos de fiscalização (Dutra, Silva, 2016).

A questão se agrava se analisada sob a ótica da falsa sensação de anonimato. Essa sensação estimula o cometimento de delitos no ambiente virtual, mesmo que por pessoas especializadas, não obstante a existência de ferramentas de rastreamento que permitem a punição de agentes maliciosos, a exemplo de *hackers* que roubam dados sigilosos (Barreto Júnior, Gallinaro, Sampaio, 2018).

É sabido que o direito à privacidade tem assento constitucional[15], todavia,

[15] O art. 5º, inciso X, da Constituição Federal de 1988, prevê como invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

referido direito encontra severos entraves no ambiente digital. A *internet* potencializa riscos à intimidade, permitindo o esquadrinhamento de pessoas através de bancos de dados interconectados (Barreto Júnior, Gallinaro, Sampaio, 2018).

Em razão desse problema, o próprio Marco Civil da *Internet* reafirma a inviolabilidade das comunicações privadas e exige o consentimento expresso para o tratamento de dados[16]. Tal avanço, apesar de louvável, não resolve o problema, já que permanece a dependência de serviços digitais essenciais, como *e-mails* e redes sociais, que forçam os usuários a aceitarem os termos abusivos de coleta de dados, como verdadeira forma de adesão contratual e abdicação involuntária da privacidade (Barreto Júnior, Gallinaro, Sampaio, 2018).

A lei avançou ao estabelecer critérios claros de responsabilização, oferecendo segurança jurídica aos servidores que podem operar sem o temor de censura arbitrária. Além disso, os usuários podem contar, ainda que minimamente, com a proteção dos direitos pessoais em face de abusos. A conclusão é que o Marco Civil da *Internet* é um marco, de fato, mas não final, e sim inicial, em relação à regulamentação do uso da *internet* no Brasil (Dutra, Silva, 2016).

Apesar dos avanços, ainda existiam entraves legislativos, especialmente diante da exigência de decisão judicial para viabilizar a responsabilização civil do provedor de conteúdo que, apesar de notificado, não realizou a remoção. Diante desse cenário, Teffé e Moraes (2017) propõem uma releitura constitucional do Marco Civil da *Internet* a partir do princípio da dignidade da pessoa humana.

Se a liberdade de expressão é indispensável para o regime democrático, ela não poderia ser utilizada de forma irrefutável como escudo para práticas abusivas, especialmente em ambientes digitais onde a difusão de informações ocorre em escala massiva e com profundas repercussões. Uma possível solução seria a adoção de mecanismos mais eficazes para a remoção de conteúdo ilícito, como a possibilidade de responsabilização jurídica do provedor de *internet* após a notificação extrajudicial promovida por aquele que teve seus direitos violados, posição que, como já visto, também é defendida por Schreiber (2015).

Esse era o cenário legislativo, doutrinário e jurisprudencial que vigorava, ao menos até a reinterpretação do Marco Civil da *Internet* pelo Supremo Tribunal Federal, ao julgar os Temas 987 e 533.

---

[16] Nesse sentido, o art. 7º, incisos VII e XIX, da Lei 12.965/2014.

### 2.1.1 A mudança de interpretação do Marco Civil da *Internet* pelo Supremo Tribunal Federal (Temas 987 e 533)

Como explicado, o regime jurídico trazido pelo art. 19 da Lei 12.965/2014 (Marco Civil da *Internet*) estabelecia que os provedores de aplicações (*Instagram, YouTube, Facebook*, por exemplo) possuem responsabilidade civil subjetiva, condicionada à prévia ordem judicial. Nessa esteira, se um influenciador digital postasse conteúdo ofensivo, a plataforma não poderia ser responsabilizada automaticamente, respondendo solidariamente apenas se descumprisse ordem judicial que determinasse a retirada do material. Excepcionalmente, em casos de nudez ou atos sexuais privados, segundo o art. 21 da mesma lei, seria possível a responsabilização extrajudicial e imediata (Dutra, Silva, 2016).

Segundo Schreiber (2015), é mister se despir de ilusões e de argumentos falaciosos em relação aos ambientes digitais como fóruns democráticos e de livre expressão. Em verdade, são espaços privatizados, regidos por interesses econômicos e operados por algoritmos que reforçam bolhas e polarizações. É impositivo que o direito se utilize da sua função reguladora, sob pena de se admitir que a liberdade de expressão seja instrumentalizada para reproduzir discursos de ódio, *fake news*, assédio e opressão, especialmente contra grupos mais vulneráveis.

Obviamente, o ambiente virtual, especialmente as redes sociais, transformou as dinâmicas sociais e jurídicas, criando novas formas de vulnerabilidade do sujeito que utiliza as redes. A privacidade ganhou contornos mais agressivos e complexos, exigindo do direito respostas legislativas e jurisprudenciais que pudessem dialogar com as profundas transformações da sociedade (de Macedo Menna Barreto, 2015).

Entrementes, entende-se que a *internet* passou a mediar relações sociais complexas e a expor a pessoa humana a novas formas de vulnerabilidade, especialmente em razão da coleta massiva de dados pessoais e da ampla exposição nas plataformas digitais (Teffé, Moraes, 2017).

Digno de menção que nem todos entendem ter sido a promulgação do Marco Civil da *Internet* um avanço legislativo significativo. Para Tomasevicius Filho (2016), embora exista uma celebração como um marco global de regulação da *internet*, a lei não trouxe efetivas inovações jurídicas, reproduzindo comandos constitucionais e normas já previstas em outras leis, a exemplo do Código Civil, do Código Penal e do Código de Defesa do Consumidor.

Segundo o sobredito autor, o Marco Civil da *Internet* apresentava inúmeras redundâncias e normas declarativas desprovidas de eficácia normativa própria. Durante o texto existiria a repetição desnecessária de diversos direitos fundamentais já consagrados na Constituição Federal. Além disso, existiria uma tentativa infrutífera do art. 11 de tentar estabelecer critérios para a aplicação extraterritorial da lei[17], sendo que a própria *internet* permanece, diante da sua arquitetura, imune à jurisdição exclusiva de um único Estado, o que esvaziaria o alcance da legislação doméstica (Tomasevicius Filho, 2016).

A forma das redes sociais não permitiria uma regulação centralizada e eficiente por parte do Estado. É possível aplicar uma metáfora como se as redes sociais fossem um *iceberg*: a parte visível das interações sociais é a ponta acima do nível da água, enquanto a captação massiva e silenciosa de informações ocorre na parte invisível e submersa, revelando verdadeira dicotomia (de Macedo Menna Barreto, 2015). A inexistência de mecanismo eficaz de fiscalização e controle transforma a legislação local em mera simbologia, incapaz de mitigar as assimetrias de poder entre usuários e corporações tecnológicas.

Ademais, apesar da lei fazer da privacidade um de seus pilares e trazer um avanço em termos de enunciação de direitos, ainda que, às vezes, de maneira redundante, ainda existe a interpretação de que carece de densidade normativa capaz de efetivar de modo robusto a tutela dos dados pessoais dos usuários. A previsibilidade do direito à intimidade e à vida privada prevista no art. 7º da Lei 12.965/2014, segundo alguns, somente pode ser compreendida dentro de uma lógica que transcenda a dogmática jurídica tradicional, contanto que sejam incorporados elementos sociotécnicos próprios do ciberespaço e reconhecidas estratégias empresariais de captação, tratamento e monetização de dados pessoais (de Macedo Menna Barreto, 2015).

A aplicação da nova legislação enfrentava desafios significativos, especialmente em razão da velocidade das transformações tecnológicas, da

[17] O art. 11 da Lei 12.965/2014 determina a aplicação da lei brasileira em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de *internet*, contanto que um desses tenha acontecido em rede nacional. Aplica-se a norma mesmo aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil (§1º). Além disso, a redação do artigo repete direitos fundamentais já consagrados na Constituição Federal, como os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

globalização das redes sociais e da extraterritorialidade das grandes plataformas digitais. O fato dessas plataformas serem sediadas no exterior cria diversos obstáculos à efetiva fiscalização e aplicação da legislação brasileira, considerando que muitas decisões de moderação de conteúdo e tratamento de dados são tomadas em matrizes localizadas no exterior, mas aplicadas no território brasileiro. Sem prejuízo, os conceitos de "liberdade de expressão", "tratamento de dados" ou "discurso de ódio" são sujeitos a interpretações divergentes em todo o mundo, gerando notória insegurança jurídica em casos de interpretação jurídica limítrofe (Leite, 2016).

Segundo Tomasevicius Filho (2016), outros avanços que podem ser citados é a vedação de censura estatal por *firewalls*[18], a regulamentação de *cookies*[19] e o estabelecimento de critérios formais para a requisição judicial de registros eletrônicos. Para alguns, são avanços tímidos que não justificam o entusiasmo que cercou a promulgação da norma. Para o autor, a solução mais eficaz para os problemas citados é a criação e adesão dos países a uma "Declaração Universal dos Direitos dos Usuários da *Internet*", no lugar de tentativas isoladas – através de leis nacionais – de regular fenômenos transnacionais e multijurisdicionais.

Trata-se, na verdade, de instrumento híbrido: se por um lado reforça direitos já constitucionalizados, como a privacidade, por outro, introduz mecanismos específicos para o ambiente digital, como a imposição de neutralidade da rede e a guarda de registros. Apesar de constituir um progresso na proteção de dados, a eficácia da legislação depende de uma combinação entre aplicação judicial coerente, avanços tecnológicos e conscientização dos usuários (Barreto Júnior, Gallinaro, Sampaio, 2018).

Antes, inclusive, da vigência do Marco Civil da *Internet,* a jurisprudência já tendia a responsabilizar de forma mais intensa as plataformas, inclusive de maneira objetiva, especialmente quando falhavam na remoção de perfis falsos ou de conteúdos ofensivos após notificações extrajudiciais. Entretanto, após 2014, com o

---

[18] Um *firewall* é um sistema de segurança que controla o tráfego de rede, permitindo ou bloqueando a passagem de informações com base em regras predefinidas. Atua como uma barreira entre uma rede interna confiável e redes externas não confiáveis, como a *internet*, e tem como objetivo principal proteger contra acesso não autorizado e ameaças de segurança (definição do autor).

[19] *Cookie* é um pequeno ficheiro de texto que um *website* envia ao navegador do usuário. O arquivo é armazenado no dispositivo utilizado para navegação. Esse arquivo permite que o *website* identifique o usuário quando ele retorna ao mesmo domínio, com a intenção de tornar a experiência de navegação mais personalizada e fluida porque armazena informações como a língua preferida, a localização, os dados de acesso, itens do carrinho de compras e outras informações. Podem ser usados para rastrear a atividade *on-line* em diferentes *websites* para direcionar anúncios mais relevantes ou até para coletar informações pessoais de preferências do usuário (definição do autor).

advento da lei, consolidou-se a exigência de ordem judicial (art. 19), trazendo restrições à responsabilização, o que gerou movimentos sucessivos de atuação dos tribunais para reafirmarem o dever de cooperação das plataformas, sobretudo no fornecimento de dados que permitam identificar autores de perfis falsos usados para ofensas (Maia, Curvo, 2025).

Acompanhando as considerações acima, feitas pela doutrina e pela sociedade civil, o Supremo Tribunal Federal recentemente julgou os Recursos Extraordinários 1.037.396 (Tema 987) e 1.057.258 (Tema 533), promovendo uma significativa alteração hermenêutica na interpretação, sobretudo, do art. 19 do Marco Civil da *Internet*.

Com julgamento do mérito em 27 de junho de 2025, a decisão foi responsável pelo abandono de uma interpretação estritamente literal da lei, que condicionava, como visto, a responsabilidade civil das plataformas digitais ao descumprimento de uma ordem judicial específica. O STF divulgou uma nota intitulada “Informação à Sociedade” (2025), explicando que passou a adotar uma interpretação conforme a Constituição, tendo como intuito conferir maior densidade normativa à tutela dos direitos fundamentais no ciberespaço.

De acordo com o novo entendimento da Suprema Corte, a mera exigência de ordem judicial como condição prévia de responsabilização não seria suficiente para tutelar bens jurídicos de alta relevância como a dignidade da pessoa humana, a honra e a própria democracia. Foi assumido um papel verdadeiramente ativo na construção de um novo paradigma regulatório, conferindo às plataformas digitais deveres de diligência na prevenção e na remoção de conteúdos ilícitos, o que substituiu a responsabilização exclusivamente reativa por uma lógica de atuação proativa.

De acordo com a nova interpretação, os provedores de aplicação de *internet* podem ser responsabilizados independentemente de ordem judicial quando forem notificados extrajudicialmente acerca da presença de crimes ou atos ilícitos em sua plataforma, contanto que fiquem inertes na remoção do conteúdo. Trata-se de verdadeira ampliação do regime de responsabilidade originariamente restrito aos casos de divulgação não consentida de nudez privada, conforme a redação do art. 21 do Marco Civil, para abranger ilícitos de natureza variada, inclusive a criação de perfis falsos e a disseminação de desinformação.

Por outro lado, foi preservada a necessidade de ordem judicial para os casos que envolvam crimes contra a honra, a exemplo da calúnia, da difamação e da injúria.

A decisão da Suprema Corte buscou preservar a liberdade de expressão, evitando que meras notificações realizadas de forma privada resultem em remoção sumária de conteúdos que possam veicular críticas legítimas. Por outro lado, estabeleceu que uma vez reconhecida judicialmente a ilicitude de determinado conteúdo, existe o dever das plataformas na remoção de publicações de forma imediata, a partir de simples notificação, sem que haja a necessidade de uma nova decisão judicial.

Outro ponto da decisão que, por ser inovador, merece registro, diz respeito ao reconhecimento de uma presunção de responsabilidade em situações específicas, como nos casos de anúncios ou impulsionamentos pagos e no uso de redes artificiais de distribuição ilícita (robôs ou *chatbots*). Nas referidas hipóteses, considera-se que o provedor é conhecedor da ilicitude, somente tendo sua responsabilidade afastada caso demonstre que atuou de forma diligente e em tempo razoável para indisponibilizar o conteúdo. Trata-se, na verdade, de aproximação ao conceito de vigilância que é adotado em regimes regulatórios internacionais.

O novo paradigma interpretativo da Suprema Corte também introduziu o “dever de cuidado” para os crimes que são de maior gravidade, a exemplo de terrorismo, pornografia infantil, tráfico de pessoas, discriminação, violência de gênero e atos antidemocráticos. Nessas hipóteses, foi determinado que as plataformas possuem o dever de atuar de forma preventiva, impedindo qualquer publicação ou circulação dos conteúdos independentemente de notificação ou ordem judicial. Contudo, a responsabilização dependerá da demonstração de uma falha sistêmica do provedor, no escopo de evitar uma responsabilização automática por ocorrências isoladas.

O novo entendimento estabeleceu, igualmente, obrigações de transparência e prestação de contas pelas plataformas. As empresas terão o dever de instituir sistemas de notificações que sejam acessíveis aos usuários, como canais de atendimento de ampla divulgação, por exemplo, assim como procedimentos internos de recurso e relatórios periódicos de transparência, representando verdadeiro avanço na autorregulação. A medida fortalece a responsabilização jurídica das plataformas, trazendo mais clareza à lógica da moderação de conteúdo.

Frise-se que a determinação de que provedores estrangeiros que atuam no Brasil mantenham representante legal no país, que tenha plenos poderes para responder administrativa e judicialmente, também foi relevante. A exigência tem o intuito de superar o problema da extraterritorialidade das grandes plataformas digitais, possibilitando que as decisões judiciais brasileiras sejam mais efetivas e contem com

uma facilitação na cooperação institucional.

Deve-se destacar também que os efeitos da decisão do Supremo Tribunal Federal foram modulados, sendo definido que a nova interpretação legislativa tenha aplicação prospectiva, preservando a segurança jurídica e evitando impacto desproporcional em processos judiciais já encerrados. Com a modulação dos efeitos da decisão, a Suprema Corte demonstrou uma preocupação à estabilidade das relações jurídicas e ao risco de responsabilização retroativa de plataformas que atuaram de acordo com o entendimento anteriormente vigente.

Por fim, a decisão reconheceu que a intervenção do Poder Judiciário deve ter caráter provisório e interpretativo, constituindo também um apelo do legislador para que sejam elaboradas novas leis que superem as insuficiências do Marco Civil da *Internet*. De fato, não pode o Poder Judiciário se imiscuir na atividade legiferante, substituindo o papel do Congresso Nacional, enquanto representantes do povo, na redação das leis.

Sem dúvidas, a nova interpretação, feita pelo Supremo Tribunal Federal, do art. 19 do Marco Civil da *Internet,* revela verdadeira mutação constitucional infralegal, com o objetivo de reconfigurar o equilíbrio entre liberdade de expressão, responsabilidade jurídica e proteção dos direitos fundamentais. Com a decisão é criado um novo modelo híbrido que mantém a essência da tutela judicial para crimes contra a honra, mas por outro lado, avança para exigir condutas diligentes em relação a ilícitos graves e a situações de risco sistêmico.

Em síntese, a mudança de paradigma reforça o papel regulador do Estado e do direito no ciberespaço, ao mesmo tempo em que aproxima o ordenamento jurídico brasileiro de tendências globais de regulação das plataformas digitais. Enquanto a liberdade de expressão ainda é resguardada como valor estruturante, a Suprema Corte tenta evitar que referido direito seja utilizado para perpetuar ilícitos e violações massivas de direitos fundamentais.

## 2.2 A Lei Geral de Proteção de Dados

Como visto, as redes digitais ocupam privilegiado espaço na sociedade contemporânea. Portanto, é natural que os dados que nelas trafegam sejam igualmente tutelados, considerando o tratamento massivo de informações pessoais que trafegam diariamente. Os usuários compartilham seus dados de forma voluntária,

entretanto, a obrigação das plataformas e dos influenciadores de cumprirem as diretrizes da Lei Geral de Proteção de Dados (LGPD), posterior e complementar ao Marco Civil da *Internet*, persiste.

Quando da promulgação do Marco Civil da *Internet,* apontava-se para uma lacuna normativa diante da ausência de legislação específica sobre proteção de dados, sendo do Marco Civil e de decretos regulamentadores a responsabilidade de suprir a lacuna e consagrar direitos fundamentais como a autodeterminação e o consentimento livre do tratamento de dados. Inexistia uma lei que previsse a transparência necessária entre os usuários em relação ao consentimento e à circulação livre de dados, situação agravada pela lógica econômica das redes que se mantêm financeiramente com a monetização de informações pessoais, de forma que a remuneração indireta torne o usuário o próprio produto (Teffé, Moraes, 2017).

A promulgação da LGPD (Lei nº 13.709/2018) foi um marco jurídico no ordenamento brasileiro, por ser a primeira a disciplinar de forma tão extensiva o tratamento de dados pessoais. Sua inspiração vem, de maneira forte, do Regulamento Geral sobre a Proteção de Dados da União Europeia. A lei estabelece diretrizes claras sobre as maneiras que órgãos públicos e entidades privadas devem coletar, armazenar, compartilhar e eliminar informações pessoais, de forma a resguardar a segurança jurídica e o respeito à privacidade (Brasil, 2021a).

Nos termos da LGPD, os dados pessoais são tratados como qualquer informação que permite a identificação direta ou indireta de uma pessoa natural, a exemplo do nome, do CPF, da localização geográfica, das preferências de consumo ou até dos padrões de comportamento (art. 5º, I). No escopo do ambiente digital, os dados são coletados de forma massiva e, na maioria das vezes, imperceptível ao titular. Ainda nos termos da LGPD (art. 5º, II), os dados sensíveis são aqueles que tratam de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato, além de dados relacionados à saúde, à vida sexual, genéticos ou biométricos, dentre outros. Devido à maior sensibilidade, esses dados demandam uma proteção ainda mais especializada.

O escopo normativo amplia o debate sobre uso ético dos dados no contexto digital, podendo o raciocínio ser aplicado às plataformas digitais e às redes sociais. A LGPD surgiu para proteger os direitos fundamentais em razão da expansão da tecnologia do mundo, da globalização e do aumento da importância da informação, que passou a ser um ativo de relevância. Quem tem os dados domina o capital e a

governança. Nesse contexto que surgiu a necessidade de criar mecanismos de regulação e de proteção de dados pessoais dos que utilizam os serviços digitais, impedindo um compartilhamento desenfreado que viole direitos fundamentais em nome da lógica do capital ou da dominação política[20].

A finalidade disposta na LGPD, que se aplica às redes sociais, é o estabelecimento do princípio da autodeterminação informativa, buscando conferir aos titulares um maior controle sobre seus próprios dados (Brasil, 2021a). Como exemplo, estão os direitos de acesso, correção, portabilidade, eliminação e informação sobre o uso. Trata-se de entendimento que, de certa maneira, reconfigura o papel do cidadão no mundo digital, permitindo-lhe maior protagonismo em relação às empresas e às plataformas que exploram sua identidade digital.

A LGPD também é permeada pelo princípio da finalidade, com a determinação de que os dados pessoais só podem ser tratados para propósitos legítimos, específicos, explícitos e informados ao titular (Brasil, 2021b). Referido princípio busca limitar a utilização indiscriminada de informações pessoais, obrigado os agentes de tratamento de dados a atuarem com transparência. No campo das redes sociais, a relevância do princípio ganha corpo com o uso constante de dados para fins de *marketing* direcional e análise comportamental (Brasil, 2021a).

Além disso, a LGPD estabelece as bases legais para o tratamento de dados, exigindo que exista uma justificativa jurídica para que uma organização possa coletar e utilizar informações pessoais. A base que mais comumente costuma ser utilizada é a do consentimento, que deve ser livre, informado e inequívoco (Brasil, 2021b). Não obstante, existem outras bases que podem se aplicar, como o legítimo interesse e o cumprimento de obrigação legal. A escolha da base legal adequada é essencial para que as práticas digitais estejam em conformidade com a LGPD, afetando diretamente

[20] “A LGPD surge com o intuito de proteger direitos fundamentais como privacidade, intimidade, honra, direito de imagem e dignidade. Pode-se pontuar também que a necessidade de leis específicas para a proteção dos dados pessoais aumentou com o rápido desenvolvimento e a expansão da tecnologia no mundo, como resultado dos desdobramentos da globalização, que trouxe como uma de suas consequências o aumento da importância da informação. Isso quer dizer que a informação passou a ser um ativo de alta relevância para governantes e empresários: quem tem acesso aos dados, tem acesso ao poder. Pensando nisso, a atuação das empresas no contexto digital trouxe consigo a necessidade de criação de mecanismos de regulação e proteção dos dados pessoais daqueles que utilizam serviços, compras ou realizam qualquer tipo de transação on-line que envolve o fornecimento de informações pessoais. Toda situação ou ação realizada no ambiente virtual faz parte da realidade de qualquer pessoa, portanto os direitos garantidos no ‘mundo offline’ devem ser assegurados também no espaço virtual. Em virtude disso, é importante apontar que a lei brasileira não protege somente os dados pessoais nos meios digitais” (Pinheiro, 2018, pp. 38-39).

a responsabilidade dos influenciadores digitais e das plataformas em que atuam.

A LGPD também define as figuras do controlador e do operador, responsáveis pela governança de dados. Enquanto o controlador é o agente que toma as decisões sobre o tratamento de dados, o operador é o que executa as decisões (Brasil, 2021b). A distinção tem implicações significativas para a responsabilização dos atores envolvidos na cadeia de dados. Nas redes sociais, por exemplo, um influenciador digital que coleta informações de seguidores para campanhas publicitárias pode ser equiparado à figura do controlador, sendo, portanto, responsável por garantir o cumprimento das normas da LGPD (Brasil, 2021a).

Percebe-se que a LGPD, ao regular o tratamento de dados digitais, impõe deveres às plataformas de mídia e anunciantes, especialmente quando há coleta e tratamento de dados para fins comerciais. A atenção monetizada e os dados íntimos dos usuários devem ser tratados e coletados com transparência, consentimento e segurança. A reputação digital e a responsabilidade civil dos agentes envolvidos emergem como componentes essenciais do respeito à privacidade.

Convém mencionar que a LGPD é uma lei principiológica, construída sobre os fundamentos da boa-fé, do respeito à privacidade, da autodeterminação informativa, da liberdade de expressão e do desenvolvimento econômico e tecnológico (Brasil, 2021a). A estrutura aberta da norma demanda constante interpretação hermenêutica e atualização jurídica, o que representa um verdadeiro desafio para consolidar o paradigma regulatório na dinâmica era da informação.

A realidade revela que muitos dos agentes que atuam com dados pessoais não possuem estrutura técnica ou conhecimento jurídico para assegurar a conformidade com os preceitos legais, evidenciando a necessidade de políticas públicas de capacitação e de incentivo à educação.

A LGPD é muito mais do que apenas um instrumento de tutela da privacidade: é um passo importante para a construção de uma sociedade digital mais ética, transparente, inclusiva e fraterna. O cenário de exposição e de vigilância do Século XXI exige que a lei possa emergir como um necessário contraponto, capaz de reequilibrar as relações entre indivíduos, empresas e tecnologia (Micheletti, 2021). O cumprimento das normas, todavia, capaz de transformar a promessa normativa em realidade vivida, depende do esforço coletivo entre Estado, setor privado e sociedade civil.

Percebe-se um esforço legislativo para que a LGPD possa estabelecer

diretrizes claras sobre o tratamento de dados pessoais, oferecendo um caminho jurídico e ético para as plataformas de redes sociais digitais, hoje partes essenciais da vida moderna que exercem forte influência nos modos de comunicação, consumo e formação de opinião (Carvalho, Oliveira, Cappelli, 2020).

A partir do momento em que se exige o consentimento expresso do titular para o tratamento dos seus dados, é possível que as redes sociais passem a operar de maneira mais transparente, aumentando a credibilidade e a confiança das plataformas digitais. O efeito, inclusive, pode ser benéfico às empresas, com aumento do tempo de permanência e redução da evasão de usuários, considerando o volume expressivo diário de tráfego de dados pessoais (Costa, Oliveira, 2019).

Para tanto, deve-se pensar em uma reestruturação dos sistemas de coleta, armazenamento e compartilhamento de dados, com investimentos em tecnologia e *compliance* que viabilizem um retorno positivo a longo prazo, inclusive com a redução de riscos jurídicos e o fortalecimento da reputação institucional (Carvalho, Oliveira, Cappelli, 2020).

As redes sociais que conseguirem se alinhar com as regras da LGPD, a exemplo da finalidade, da necessidade e da adequação, tendem a construir ambientes mais éticos e seguros, angariando vantagem competitiva no mercado. A questão adquire especial relevância no contexto global, em consonância com o Regulamento Geral de Proteção de Dados – GDPR europeu (Costa, Oliveira, 2019).

Outra questão sensível que deve ser considerada é o tratamento de dados de populações vulneráveis, como adolescentes e idosos, sendo que a rede social que siga as normas da LGPD estará alinhada a preceitos mínimos de responsabilidade social, o que pode atrair anunciantes e parceiros comerciais preocupados com critérios éticos (Carvalho, Oliveira, Cappelli, 2020).

Nesse sentido, tem especial relevância a promoção da autodeterminação informativa, garantindo ao indivíduo o controle sobre seus próprios dados, de maneira a viabilizar uma experiência mais justa e personalizada das redes sociais. A medida não somente atende aos critérios exigidos na legislação, como também viabiliza a melhora da percepção da plataforma pelo usuário (Costa, Oliveira, 2019).

O usuário adquire[21], com a promulgação da LGPD, especial relevância na

[21] Merece transcrição integral o art. 18 da LGPD:
“Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

centralização e controle dos seus direitos, podendo dispor sobre acesso, retificação e eliminação de dados, o que impõe às plataformas digitais que desenvolvam mecanismos internos de governança e tratamento de dados, com a profissionalização da gestão e impulsionamento de fluxos automatizados mais eficientes (Carvalho, Oliveira, Cappelli, 2020).

Além disso, com a LGPD, o usuário passa a contar com maior segurança em relação à mitigação de danos em caso de incidentes, já que a legislação exige que eventual vazamento ou mal tratamento dos dados sejam imediatamente comunicados ao usuário e à Autoridade Nacional de Proteção de Dados – ANPD, estimulando as redes sociais a adotarem políticas de segurança robustas e atualizadas (Costa, Oliveira, 2019).

Sem prejuízo, a adoção dos critérios previstos na LGPD reduz a opacidade algorítmica, considerando que as redes sociais são obrigadas a explicar o tratamento automatizado de dados. A clareza exigida visa diminuir o impacto das chamadas “bolhas de filtragem” e da manipulação de informações, viabilizando a formação de um ambiente digital mais transparente e democrático (Carvalho, Oliveira, Cappelli, 2020).

Em suma, a LGPD trouxe significativos avanços legislativos para proteger a privacidade do usuário, considerando os limites impostos ao compartilhamento de informações com os terceiros, além de hipóteses de responsabilização civil e criminal dos responsáveis pela quebra do correto tratamento dos dados.

O seguimento da LGPD por parte das plataformas digitais, inclusive as redes sociais, que operam no Brasil, além de incentivar a educação digital, é essencial para que estejam mais preparadas para auditorias e fiscalizações, seja da ANPD, seja de

---

I - confirmação da existência de tratamento;
II - acesso aos dados;
III - correção de dados incompletos, inexatos ou desatualizados;
IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;
VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei”.

outros órgãos, garantindo a continuidade de operações e o afastamento de sanções que possam prejudicar o posicionamento no mercado digital.

A cultura da privacidade imposta pela LGPD evita práticas abusivas, inclusive no *marketing* digital, viabilizando uma experiência do usuário que seja menos invasiva e mais ética. Além disso, uma maior proteção dos direitos de personalidade é possível através da regulação adequada do tratamento dos dados, garantindo que as interações digitais respeitem os limites da dignidade da pessoa humana e que seja viável um novo modelo de *internet* mais justa.

## 2.3 Fake news, discurso de ódio e polarização política

O avanço tecnológico possibilitou que a manipulação das informações deixe de ser ampla e uniformemente distribuída para ser individualizada. A coleta de dados de usuários, tratados sem o consentimento, permitiu que as plataformas digitais modulem o comportamento e as opiniões baseando-se nas interações personalizadas do usuário.

Por serem operados exclusivamente para a retenção do utilizador em relação ao “tempo de tela”, os algoritmos de redes sociais viabilizam a disseminação de *fake news* e distorcem informações através de uma desintermediação do jornalismo tradicional, quando editores podiam filtrar conteúdos com base em critérios éticos. Assim, atores não profissionais que atuam nas redes, guiados por emoções e preferências individuais, assumem o controle na circulação de informações, sendo o cenário agravado pelos algoritmos que priorizam engajamento em detrimento da veracidade, e criam ecossistemas de desinformação. Tem-se uma relação simbiótica entre plataformas digitais e a economia da atenção, quando conteúdos polarizadores e falsos viralizam mais rapidamente diante da capacidade de gerar reações emocionais (Amaral, Santos, 2019).

Este cenário viabiliza a criação de um ambiente em que a desinformação pode ser disseminada de forma eficiente e precisa, afetando as percepções e decisões de indivíduos de maneira muito mais direta do que antes, quando a propaganda eleitoral era veiculada de forma massificada. A nova manipulação é operada individualmente. Não é mais necessário manipular a opinião pública de forma ampla e massificada

quando cada pessoa pode ser manipulada diariamente[22] e individualmente, por horas, no uso da *Internet*.

A palavra “pós-verdade” foi eleita a “palavra do ano” em 2016 pelos Dicionários *Oxford*. Autores como Ralph Keyes já dizem que vivemos em uma era de pós-verdade, termo composto já catalogado em 1992, mas que ganhou larga importância na discussão política e acadêmica a partir do ano de 2016, especialmente após o *Brexit* ocorrido na Inglaterra e após a candidatura de Donald Trump à presidência dos Estados Unidos da América (Seixas, 2019). O aprofundamento em tais acontecimentos históricos não são, neste trabalho, o objetivo.

A pós-verdade pode ser definida como “um adjetivo definido como ‘relatando ou denotando circunstâncias em que fatos objetivos são menos influentes na opinião pública que os apelos emocionais e as crenças pessoais” (Dicionário Oxford, 2016). Não se trata, portanto, de sinônimo da mentira, apesar do problema semântico com o nome de algo que vem após a verdade.

O oposto se revela diante da inexistência de um denominador comum na opinião pública, já que a diferença é muito mais regra que exceção. Em um cenário de pós-verdade existe uma indisponibilidade no diálogo de diferentes opiniões. A valoração da própria opinião sobre determinada questão como “única verdade possível” é causada por um conjunto de vieses cognitivos, através de um viés de confirmação, para que o sujeito tenha contato apenas com informações que confirmem suas crenças em detrimento das que as invalidam (Seixas, 2019).

Em um ambiente de pós-verdade, os fatos objetivos perdem sua relevância em razão de narrativas emocionalmente carregadas. São criadas “bolhas cognitivas” que reforçam vieses e isolam usuários, como em fenômenos recentes de eleições presidenciais com campanhas de desinformação amplificadas por mecanismos de personalização[23].

Dessa forma, a mentira, as *fakes news* ou mesmo a verdade objetiva não são

---

[22] “A manipulação não é mais das massas, é dos indivíduos. Porque o padrão usado não é mais a manipulação da opinião pública de um emissor para milhares de receptores de forma uniformizada. Agora o que ocorre é a modulação da opinião e do comportamento quase que individualmente, a partir da circulação de conteúdos direcionados por interações estruturadas com base no tratamento de dados pessoais, coletados sem o consentimento e na maioria das vezes até sem o conhecimento dos usuários dessas plataformas” (Romanini, Mielli, 2019, p. 42).

[23] “Os indivíduos são expostos a conteúdos e opiniões que reforçam suas próprias visões de mundo, enquanto o diverso, o contraditório e até constatações científicas são marginalizadas, dentro desta lógica, quase que mecânica, do papel dos algoritmos para as redes sociais e até mesmo para os mecanismos de busca na *Internet*” (Rocha, 2024, p. 27).

sinônimos ou antônimos da pós-verdade, mas sim algumas de suas facetas, na medida em que o termo se preocupa necessariamente com a capacidade do sujeito de ser submetido ao contraditório, considerando-o como igualmente válido e como possível uma mudança racional e embasada de opinião[24].

Os conteúdos viralizáveis (por vezes, falsos ou sensacionalistas), ao serem privilegiados, facilitam a disseminação de desinformação. As plataformas digitais dificultam a distinção entre fatos e ficção, existindo teorias da conspiração (e.g., Terra Plana) que ganham relevância algorítmica devido ao alto engajamento, não obstante sejam acientíficas. O fenômeno é agravado pela criação da bolha informacional e do consumo de conteúdo semelhante, sendo que eventuais confrontos se polarizam a ponto de afastar o diálogo construtivo necessário ao ambiente educacional (Santos, 2022).

A desinformação não surge como um problema de percepção, mas sim com impactos reais e quantificáveis, citando-se como exemplo[25] uma pesquisa realizada nos Estados Unidos nas eleições de 2016, em que Donald Trump concorreu com Hillary Clinton nas eleições federais, quando 75% das pessoas que viram manchetes falsas consideraram-nas verdadeiras, com diferenças significativas de credulidade dependendo de orientação política.

O desafio moderno é equilibrar a liberdade de expressão com a necessidade de evitar danos à coletividade em razão da disseminação de informações falsas. Levantam-se vozes no sentido de que uma regulação estatal deve ter a capacidade de assegurar a liberdade de informação sem que seja sacrificada a proteção contra a desinformação (Nohara, 2020), que pode causar graves prejuízos à democracia e ao funcionamento justo dos processos eleitorais.

Não se pode conceber que o Estado Democrático de Direito tenha uma

---

[24] “Entendemos que informações podem ser inventadas ou manipuladas pelos veículos de mídia, por exemplo, desde que satisfaçam certas peculiaridades de um dado conjunto ideológico de crenças. Adotar a realidade como referência - uma referência inconstante, que sob a lógica discursiva ganha múltiplas leituras possíveis - se torna menos importante do que criar uma realidade particular, em que a interpretação se lineariza porque o acontecimento não existe fora de um contingente ideológico qualquer, sem espaço para a dúvida. Na *pós-verdade,* mais do que interpretar e significar o acontecimento, cria-se uma versão que o sujeito tende a interpretar como verdadeira ou não, independente de investigações científicas quaisquer. Tal gesto interpretativo é possível devido à fluidez da informação, por sua instabilidade, por retratar um mundo tão farto de acontecimentos, tão amplo em dimensões planetárias e contraditório nos dizeres” (Siebert, Pereira, 2020, p. 244).

[25] “[…] com mais de 3 mil norte-americanos, verificou que 75% daqueles que viram as manchetes das notícias falsas as julgaram como exatas. Na média, os partidários de Hillary Clinton consideraram 58% das manchetes das notícias falsas como verdadeiras, em contraste com 86% dos eleitores de Trump” (D'Ancona, 2018, p. 55).

liberdade indiscriminada, com danos causados pela coletividade a partir da tutela de uma liberdade de expressão absoluta. Nesse contexto que surge[26] o papel regulador do Estado, para garantir uma adequada compensação entre os princípios jurídicos em conflito.

Essa nova realidade sugere uma necessidade de que o Estado adote medidas eficazes para combater a disseminação de informações enganosas de forma individualizada, após a coleta e tratamento indevido de dados particulares. O conteúdo intencionalmente falso e distribuído costuma ser produzido para obtenção de vantagens econômicas ou políticas, disfarçadas para parecerem legítimas, imitando o formato da mídia tradicional, o que agrava ainda mais o problema (Gross, 2020).

Referido conteúdo falso, chamado de "*Fake News*", pode ser definido como um conteúdo intencionalmente mentiroso que foi fabricado com o objetivo de explorar circunstâncias do ambiente *on-line*: anonimato; rapidez de disseminação da informação; fragmentação das fontes de informação; atenção dos usuários da *internet*; apelo às emoções e; sensacionalismo (Gross, 2020).

Entretanto, é necessário certo cuidado na utilização do termo *Fake News*, de forma indiscriminada e generalizada, considerando a possibilidade de desvio da responsabilidade da verdadeira fonte de desinformação. No lugar de propagandistas estatais e outras entidades que espalham desinformação, o termo pode ser injustamente empregado para atacar a mídia e enfraquecer o papel crítico de jornalistas. *Fake News* existem, entretanto, a responsabilidade precisa ser abordada na raiz das práticas da desinformação, sob pena de prejudicar a capacidade da mídia de atuar como contrapeso essencial no sistema democrático (Gutiérrez, 2019).

Para o conteúdo falso que é realmente divulgado em redes sociais, tais veículos oferecem ferramentas sofisticadas de impulsionamento de publicações, viabilizando o direcionamento a públicos específicos com base em dados detalhados do uso individual[27]. Nessas hipóteses, a pessoa pode pagar um valor em dinheiro para

---

[26] "Conforme visto, o Estado Democrático de Direito não se alinha com uma proposta de liberdade indiscriminada, pois as pessoas não possuem liberdade para causarem danos à coletividade a partir da disseminação de fatos mentirosos na *web*. Portanto, o Estado deve regular essa liberdade para que haja medidas que garantam a liberdade preservada, sem fulminar, contudo, o núcleo essencial da liberdade de informação" (Nohara, 2020, p. 87).

[27] "As redes sociais […] oferecem o serviço de impulsionamento de publicações, por meio do qual a pessoa interessada paga um determinado valor com o fim de que sua publicação atinja um número maior de pessoas. […] Por meio dessa ferramenta, é possível determinar, a depender do valor pago, a quantidade de pessoas a serem atingidas, bem como definir o público-alvo que será alcançado pela publicação de acordo com sua residência, sexo, idade e interesses, aumentando de forma significativa a eficiência da publicação que se pretende divulgar" (Campello, 2017, p. 58).

que a publicação seja “impulsionada”, atingindo número maior que o normal de pessoas. O tamanho do investimento fica atrelado ao tamanho do alcance, sendo possível direcionar a publicação para que atinja um grupo específico de pessoas, de acordo com a característica escolhida (gênero, idade, local etc.).

No âmbito das redes sociais, é possível a utilização dos chamados *“Bots*”, *softwares* projetados para interagir com os usuários de plataformas digitais, desempenhando um importante papel na propagação de conteúdos falsos. Esses robôs virtuais podem utilizar avançadas técnicas de geração de linguagem natural ou simples respostas automáticas para manipular e influenciar a opinião pública, gerando a necessidade de um amplo debate social acerca da inclusão de medidas para monitoramento e controle, no escopo de evitar o uso indiscriminado para manipular e espalhar desinformação (Ruediger et al., 2019).

Vive-se a época das sociedades em rede, erigindo o simples cidadão, antes mero receptor de informações acerca de um candidato ou partido, à categoria de emissor ou divulgador de informações, “facilitando assim a disseminação de conteúdos altamente contamináveis não só pela ideologia impregnada mas pela própria falibilidade de sua verossimilhança” (Silva, Santos, 2019).

Percebe-se que a desinformação em redes sociais pode representar ameaça mais grave que a transmitida pelos meios tradicionais, a exemplo da televisão. Para esse contexto, contribuem a falta de regulamentação específica, a ausência de intermediação da mídia tradicional e a opacidade dos algoritmos de direcionamento, gerando um ambiente de desinformação que pode prosperar sem o adequado controle.

Nesse sentido, é necessário aferir se o direito à liberdade de expressão, embora fundamental, tem o condão de ser tomado como absoluto, ou se deve ser equilibrado com a proteção contra abusos e a manutenção da ordem pública.

Afinal, se por um lado a liberdade de expressão permite a propagação de ideias e opiniões, não deve, por outro lado, ser utilizada como justificativa para a disseminação de conteúdo falso ou prejudicial, devendo existir uma regulamentação que garanta seu exercício dentro dos limites de verdade e decência, evitando a propagação de discursos que possam incitar a violência ou prejudicar a integridade do processo eleitoral, questão jurídica tutelada deste a promulgação da Constituição Brasileira de 1981 (Maximiliano, 2005).

### 2.3.1 Caso prático, no Supremo Tribunal Federal, relacionado a discurso de ódio e desinformação: a suspensão da Rede Social X

Definidos contornos mínimos acerca dos conceitos de *fake news*, assim como sobre os danos que a polarização política e a desinformação podem causar para a democracia, torna-se imprescindível analisar um caso diretamente relacionado a tais conceitos. Com efeito, no ano de 2024, o Supremo Tribunal Federal lidou com a Rede Social X (antigo *Twitter*), através do julgamento da Petição 12.404/DF, sendo suspenso o serviço da plataforma e, posteriormente, reestabelecido após o cumprimento de condicionantes e o pagamento de multas impostas.

As decisões sequenciais prolatadas pelo Supremo Tribunal Federal (2024a) envolvendo a Rede Social X demonstram uma quebra de paradigma. O fundamento central diz respeito ao choque entre a efetividade das ordens judiciais e a existência de dificuldades práticas que o Poder Judiciário enfrenta para impor o ordenamento jurídico nacional a plataformas digitais de grande poder econômico e de alcance transnacional.

As atividades da Rede Social X foram inicialmente suspensas (STF, 2024a) com o fundamento de que reiteradas decisões judiciais foram descumpridas pela empresa, que deveria cumprir a determinação de ordens específicas e pagar multas impostas. A determinação inicial, feita monocraticamente, foi posteriormente referendada, à unanimidade, pela Primeira Turma da Suprema Corte.

A Petição nº 12.404/DF, em verdade, detalhou obrigações concretas (como a indicação de representante legal no Brasil e bloqueio de perfis que descumprissem a legislação) que deveriam, segundo o Supremo Tribunal Federal, ser cumpridas antes do reestabelecimento dos serviços.

Segundo o acórdão (STF, 2024c) prolatado pela Primeira Turma em 03/09/2024, os perfis utilizados na Rede Social X estavam sendo massificados para a divulgação de mensagens antidemocráticas e de discursos de ódio. Além disso, com a disseminação de desinformação e o descumprimento reiterado das decisões judiciais, não seria possível permitir a “utilização de desinformação para corroer os pilares da democracia e do Estado de Direito”.

Além disso, os ministros destacaram (STF, 2024a) que não é admissível no Estado de Direito Brasileiro que o poder econômico ou que a dimensão financeira das empresas gere uma espécie de imunidade no cumprimento das ordens judiciais,

devendo eventuais questionamentos às decisões ter tramitação através dos recursos cabíveis, e não via obstrução prática no cumprimento das determinações. Também foi determinada pela relatoria medida específica sobre as condutas de fraudar a suspensão através de recursos tecnológicos (como VPNs[28], por exemplo), para que fosse aplicada multa diária de caráter coercitivo.

As próprias decisões da Suprema Corte, todavia, foram concebidas como instrumentos provisórios e condicionantes. O objetivo, em verdade, era compelir a Rede Social X a cumprir as ordens judiciais, não punir de forma irreversível e com esgotamento dos mecanismos de regularização.

Dentre os requisitos técnicos e formais determinados (STF, 2024c), a retomada de serviço estava condicionada ao bloqueio de perfis apontados como violadores das normas brasileiras, à indicação de representante legal no país (enquanto empresa estrangeira que opera em território brasileiro) e à quitação de multas.

Posteriormente, a própria Rede Social X comprovou o cumprimento dos requisitos (STF, 2024b), demonstrando que bloqueou os perfis apontados, que nomeou representante legal em território nacional e que procedeu ao pagamento integral das multas – em torno de R$ 28,6 milhões.

Saliente-se que o parecer da Procuradoria-Geral da República (STF, 2024c) não trouxe qualquer óbice no reestabelecimento do serviço, sendo determinada à Agência Nacional de Telecomunicações (ANATEL) que adotasse as providências administrativas necessárias para viabilizar o restabelecimento do serviço.

Curioso que a intervenção da ANATEL e o papel da Procuradoria-Geral da República denotam a interação entre esferas judiciais e administrativas para atuação no manejo de provedores de aplicação. Obviamente, enquanto o Poder Judiciário atuou na tutela jurisdicional do Estado e impondo as medidas coercitivas, coube à ANATEL, enquanto instituição de cunho técnico e administrativo, executar os atos práticos de suspensão e restabelecimento do funcionamento. Trata-se de verdadeiro arranjo híbrido de governança regulatória, demonstrando que a eficácia das decisões judiciais na utilização da *internet* depende da coordenação do Poder Judiciário com

[28] “VPN significa “Virtual Private Network” (Rede Privada Virtual) e descreve a oportunidade de estabelecer uma conexão de rede protegida ao usar redes públicas. As VPNs criptografam seu tráfego de Internet e disfarçam sua identidade *online*. Isso torna mais difícil para terceiros rastrear suas atividades *online* e roubar seus dados. A criptografia ocorre em tempo real” (Kaspersky, 2025).

Órgãos Ministeriais e agências reguladoras.

O caso em espeque traz à tona os desafios contemporâneos do direito diante de plataformas globais, especialmente na imposição de mecanismos de representação legal local, na responsabilização de conteúdos e na imposição de sanções pecuniárias e tecnológicas que revelam tensões entre a proteção da liberdade de expressão e a tutela da ordem pública.

Em termo de precedentes e de política pública, sem dúvidas o episódio deverá ser invocado em futuras disputas sobre a compatibilidade de medidas jurisdicionais de suspensão de serviços e de garantias fundamentais. Em verdade, revela-se como predecessor lógico da reinterpretação do Marco Civil da *Internet*, realizada pela Suprema Corte Brasileira no ano de 2025, como já trabalhado anteriormente.

O caso da Rede Social X no Supremo Tribunal Federal, sem dúvidas, funciona como verdadeiro estudo sobre a crise normativa entre soberania, tecnologia e direitos. Por um lado, garante-se a supremacia das decisões judiciais; por outro, impõe-se o desafio de tornar essa supremacia compatível com princípios constitucionais e com soluções técnicas adequadas ao espaço compartilhado da *internet.*

## 2.4 Perspectivas regulatórias internacionais do uso da *internet*

Não existe, até o momento, um marco regulatório internacional para o uso da *internet*. Se, por um lado, a rede mundial aberta de computadores permite inovação, comunicação livre e acesso à informação, é necessário que se entenda como equilibrar os direitos dos usuários e como garantir a segurança *online.* Existem leis e regulamentos esparsos estabelecidos mundialmente, mas o debate sobre regulação é complexo e multiforme, envolvendo direitos e princípios em estado antinômico (Bueno Rocha Rodrigues de Faria, 2024).

A regulamentação da *internet* engloba diversos aspectos, da liberdade de expressão e de comunicação à impossibilidade de utilização desregulada que viole direitos alheios. Supostamente, o debate deve ser estritamente técnico, entretanto, não deve ser desconsiderado que a forma de funcionamento da infraestrutura da rede é o que define o seu funcionamento e a forma de controle. Existe, sem dúvidas, uma forte pressão do mercado e de governos para que a regulamentação perpasse interesses próprios em detrimento de difusos, controlando tanto a liberdade de

expressão quanto a criação e disseminação de conteúdo[29].

A neutralidade da rede é tratada como princípio fundamental na arquitetura da *Internet*, como imposição aos Provedores de Serviços de Acesso a vedação de quaisquer ações que bloqueiem, estrangulem ou priorizem pacotes de dados na rede. A intenção é garantir que os dados sejam tratados de maneira isonômica, sem distinção de conteúdo, origem, destino, serviço, terminal ou aplicação, de maneira que o usuário final seja completamente livre para escolher o conteúdo consumido (Setenareski, Peres, Bona, Duarte JR., 2020).

Sobre referida neutralidade, o maior debate é acerca da sua regulação, ou seja, em que medida os países podem evitar discricionariedade e discriminação de dados, causando a degradação de tráfego e prejudicando usuários, além de viabilizar uma rede mundial de computadores que seja aberta e plural, tal qual concebida. Essa regulação seria um termo genérico para o conjunto de regras, princípios ou leis em prol da neutralidade da rede (Setenareski, Peres, Bona, Duarte JR., 2020).

O Brasil é considerado como mundialmente reconhecido em razão da promulgação do já mencionado Marco Civil da *Internet* (Lei 12.965/2014), tanto em razão do caráter democrático quanto pelo estabelecimento de princípios, garantias, direitos e deveres para usuários e provedores. Referida lei é vista como uma espécie de "Constituição da *Internet*", considerada uma das mais avançadas do ponto de vista da garantia dos direitos civis e da promoção da cidadania. O art. 15, contudo, é alvo de severas críticas por prever a guarda de registros de acesso a aplicações de *internet* por provedores, existindo campanhas pelo seu veto sob o argumento de interferência direta na privacidade dos usuários (Segurado, Lima, Ameni, 2015).

No Japão, a regulação é consolidada pelo MIAC (*Ministry of Internal Affairs and Communications*), com a perspectiva de autorregulação pela indústria, visto que a *internet* é tratada como um serviço universal de telecomunicações que deve ser provido de maneira justa e estável. São estabelecidos três princípios centrais: a necessidade dos Provedores de Serviços de Acesso à *Internet* ampliarem a

[29] "Entre as questões presentes nesse debate, destaca-se a liberdade de expressão e de comunicação relacionadas às iniciativas de regulação e de regulamentação. Para essa discussão, essa distinção é importante e poderíamos dizer que a Regulamentação diz respeito ao conjunto de instrumentos legais, como a Constituição, leis complementares, leis ordinárias, decretos, portarias, normas, estatutos, códigos etc. Regular envolve o processo de regulamentação (e isso é importante reconhecer), mas vai além. É um conjunto mais amplo de práticas que visam acompanhar e interferir cotidianamente em determinado processo com vistas a um objetivo definido. Pode-se utilizar de instrumentos legais, mas também de diversas outras 'ferramentas sociais'" (Gindre, 2007, p.131).

infraestrutura para lidar com aumentos de tráfego; a permissão de alteração de velocidade de tráfego apenas em situações excepcionais; e a exigência de que tais alterações sejam justificadas por critérios objetivos (Setenareski, Peres, Bona, Duarte JR., 2020).

Na Noruega, a regulação é feita pela NKOM (*Norwegian Communications Authority*), sendo adotadas diretrizes que se configuram como uma abordagem de corregulação, envolvendo tanto o regulador quanto os diversos usuários. Ainda do ano de 2009, tais diretrizes asseguram ao usuário o direito a um serviço com *internet* que tenha qualidade pré-definida, com liberdade para enviar ou receber conteúdos e utilizar aplicações ou dispositivos de sua escolha, além do direito a um serviço que seja livre de discriminação. A NKOM sustenta a eficácia do modelo desde 2009, inclusive, tratando a “taxa zero” (quando provedores não cobram por acesso a alguns serviços, o que violaria a isonomia diante do favorecimento de uns em detrimento de outros) como violação clara do princípio da não-discriminação (Setenareski, Peres, Bona, Duarte JR., 2020).

Já no Canadá, a regulação é feita pela CRTC (*Canadian Radio Television and Telecommunications Commission*), que estabeleceu uma abordagem principiológica para o gerenciamento do tráfego dos Provedores de Serviços de Acesso à *Internet*. Buscando equilibrar a liberdade do usuário e os interesses dos provedores, foram adotados quatro pilares: transparência das práticas de gerenciamento, incentivo ao investimento em rede como principal solução para o congestionamento, clareza na não discriminação ou preferência indevida e neutralidade concorrencial (Setenareski, Peres, Bona, Duarte JR., 2020).

Um dos pioneiros a adotar o princípio da neutralidade da rede com disposição legal, o Chile promulgou a Lei 20.453/2010, aplicável tanto a concessionárias quanto aos provedores de acesso. Nos termos da mencionada lei, estão proibidas a interferência ou a discriminação arbitrária de conteúdo ou serviços legais, sendo limitado o direito do usuário de utilizar dispositivos em rede. A agência reguladora do Chile (SUBTEL) garante o cumprimento das normas através da padronização de informações mínimas e da transparência e da penalização de práticas de taxa zero (Setenareski, Peres, Bona, Duarte JR., 2020).

O Chile, inclusive, se destacou internacionalmente pela promulgação da Lei 20.453/2010, apesar de organizações apontarem que a consagração legal da neutralidade não é absoluta, devendo existir um direito dos usuários que não seja

sujeito a limitações significativas. Todavia, percebe-se que a lei chilena, assim como a brasileira, possui uma postura mais democrática e avançada, em comparação a outros países (Segurado, Lima, Ameni, 2015).

Na Colômbia, a regulação foi inserida no ordenamento jurídico através da Lei nº 1.450 de 2011, referente ao Plano Nacional de Desenvolvimento. Foram estabelecidos princípios como livre escolha, não discriminação, transparência e informação, vedando-se o bloqueio ou a restrição arbitrária de conteúdos e serviços. A lei excepciona, entretanto, as ofertas para segmentos de mercado específicos, contanto que não sejam interpretadas como discriminação, além de listar as práticas razoáveis de gerenciamento de tráfego (Setenareski, Peres, Bona, Duarte JR., 2020).

Em Singapura, a questão é definida pela IMDA (*The Info-communications Media Development Authority*), que desde 2011 proíbe o bloqueio de conteúdo legítimo, exige transparência, além do cumprimento de padrões mínimos de Qualidade de Serviço (QoS). Todavia, os provedores de serviços podem oferecer serviços diferenciados, especializados ou personalizados, além de executar práticas razoáveis de gerenciamento de rede, sendo vedadas, contudo, quaisquer práticas discriminatórias que tornem o conteúdo ilegítimo ou inacessível (Setenareski, Peres, Bona, Duarte JR., 2020).

Na Coreia do Sul, a KCC (*Korea Communications Commision*) estabeleceu princípios básicos sobre a administração da neutralidade da rede e do tráfego, também no ano de 2011. O foco foi nos direitos do usuário à informação e ao uso livre de conteúdo ou aplicações legítimas, assim como na administração transparente do tráfego. Entretanto, é proibido o bloqueio e a discriminação “não razoável”, devendo a gestão ser “razoável” para garantir a segurança da rede ou eliminar sobrecarga temporária (Setenareski, Peres, Bona, Duarte JR., 2020).

No Peru, a regulação da neutralidade da rede aparece com a Lei nº 29.904 de 2012, que regulamentou a promoção de banda larga, impondo aos provedores de acesso que não bloqueassem, interferissem ou discriminassem arbitrariamente aplicações ou protocolos. A OSIPTEL (*Organismo Supervisor de Inversión Privada en Telecomunicaciones*) detalhou, através da Resolução nº 165/2016, princípios como livre uso, precaução, equidade e transparência, delimitando taxativamente as medidas permitidas e proibidas para as operadoras (Setenareski, Peres, Bona, Duarte JR., 2020).

Na Nova Zelândia, o tema foi amplamente discutido e posto em consulta pública

pelo ComCom (*Commerce Commission of New Zealand*) e pelo Ministério dos Negócios, Inovação e Emprego. Apesar de não ter sido formalizada regulação específica sobre neutralidade de rede, em 2012 o ComCom considerou o mercado de provedores de serviços suficientemente competitivo, alegando que eventuais restrições apenas mitigariam problemas, chegando a considerar a prática de taxa zero como potencialmente benéfica (Setenareski, Peres, Bona, Duarte JR., 2020).

No México, a Lei Federal de Telecomunicações e Radiodifusão foi alterada em 2014, sujeitando os provedores de serviços às orientações do Instituto Federal de Telecomunicações e garantindo a liberdade de escolha, o acesso a qualquer conteúdo sem limitação arbitrária, a preservação da privacidade e a transparência das informações sobre o serviço. É permitido o gerenciamento de tráfego conforme políticas autorizadas pelo instituto para garantir a qualidade e a velocidade contratadas, contanto que não configurada prática anticompetitiva (Setenareski, Peres, Bona, Duarte JR., 2020).

Na Argentina, a neutralidade da rede foi garantida pela Lei 27.078 de 2014, com o objetivo de desenvolver o setor de tecnologia da informação e comunicação. A lei garante ao usuário o direito de utilizar qualquer conteúdo, aplicação ou protocolo através da *internet* sem bloqueio, restrição, discriminação ou degradação, proibindo expressamente os prestadores de serviços de bloquear, interferir, discriminar ou estabelecer preços de acesso em virtude dos conteúdos, serviços, protocolos ou aplicações (Setenareski, Peres, Bona, Duarte JR., 2020).

Nos Estados Unidos, país que criou o termo “neutralidade da rede”, houve uma oscilação na classificação do acesso à *internet* de banda larga. Inicialmente, foi classificado como “serviço de informação” (2002), gerando polêmica, razão pela qual a FCC (Federal Communications Commission) adotou em 2015 rígidas regas que reclassificaram para “serviço de telecomunicações”. Foram estabelecidas a impossibilidade de bloqueio da rede e a impossibilidade de estrangulamento e não priorização paga. Entretanto, em 2017 a regulação foi revogada, restaurando a classificação anterior e revelando a intensa disputa das forças no mercado (Setenareski, Peres, Bona, Duarte JR., 2020).

É consenso que, nos Estados Unidos, a regulamentação é fragmentada, com diversas iniciativas e leis que abordam o controle de acesso e a propriedade intelectual, como a *Digital Millennium Copyright Act* (DMCA), a *Children's Online Privacy Protection Act* (COPPA) e a tentativa de aprovação de projetos como SOPA e

PIPA. Entretanto, o país é mais retrógrado no que diz respeito às regras de privacidade, de segurança e de vigilância, especialmente após os ataques de 11 de setembro de 2001, que desencadearam o controle a espionagem da *internet* e de comunicações telefônicas de cidadãos de vários países, inclusive do Brasil. Foram promulgadas leis como a *Foreign Intelligence Surveillance Act* (FISA) e o *Patriot Act*, que expandiram a capacidade de vigilância das agências de inteligência. São exercidas medidas de segurança como práticas intervencionistas no fluxo de informações, evidenciando uma forte pressão do mercado e de governos para controlar a rede (Segurado, Lima, Ameni, 2015).

Na Índia, o órgão regulador indiano (TRAI – *Telecom Regulatory Authority of India*) realizou consultas públicas e estabeleceu, em 2016, um regulamento que proibia as práticas de taxa zero e as tarifas discriminatórias para serviços de dados, com a imposição de penalidades para o descumprimento por parte dos provedores de serviço. Posteriormente, em 2017 e em 2018, foram emitidas recomendações para reforçar o tratamento não discriminatório de conteúdo, a transparência e o gerenciamento razoável de tráfego, podendo ser priorizado apenas em casos excepcionais e justificados, como os serviços especializados, por exemplo (Setenareski, Peres, Bona, Duarte JR., 2020).

Na União Europeia, através também da Lei de Serviços Digitais, que tem como principal objetivo prevenir atividades ilegais e prejudiciais *online* e a propagação de desinformação, também avançou[30] com a implementação de medidas para combater conteúdos ilegais, direcionar publicidade, proteger crianças, garantir segurança das eleições e regular o comércio eletrônico. O bloco de 28 países editou a regulação sobre neutralidade da rede através de acordo, realizado em 2015, entre o Parlamento, o Conselho e a Comissão Europeia. A intenção foi garantir a *internet* aberta, sendo vedado o bloqueio, o estrangulamento e a priorização paga de tráfego. O BEREC

[30] “Dentre as medidas impostas pela lei às plataformas estão: Combate aos conteúdos ilegais: implementação de medidas para combater a difusão de bens, serviços ou conteúdos ilegais online; Transparência na moderação: dever de comunicar aos usuários os motivos que levaram à remoção de um conteúdo ou a restrição de acesso a uma conta; Controle sobre as opções de personalização: maior transparência e controle sobre o que é exibido ao usuário, além de direito à pessoa escolher se receberá ou não conteúdo personalizado; Publicidade direcionada: proibição de publicidade online focada no público menor de idade; propaganda direcionada a perfis que utilizam categorias, como etnia e orientação sexual, por exemplo, também é vetada; Proteção às crianças: obrigação de proteger a privacidade e segurança de usuários menores de idade; Segurança das eleições: medidas eficazes para garantir um processo eleitoral seguro; Comércio eletrônico: fornecedores devem garantir que seus vendedores online utilizam informações verídicas sobre seus produtos” (CNN Brasil, 2024).

(*Body of European Regulators for Eletronic Communications*) definiu as diretrizes em 2016, reforçando a transparência e o gerenciamento razoável e estabelecendo que a taxa zero deve ser avaliada caso a caso, no escopo de evitar a redução material da escolha ou de serem minados os direitos dos usuários (Setenareski, Peres, Bona, Duarte JR., 2020).

Especificamente na Espanha, o país promulgou a Lei *Sinde-Wert* em 2010, concentrando-se na propriedade intelectual e na vigilância de conteúdo. A lei criou uma Comissão de Propriedade Intelectual no Ministério da Cultura, com o escopo de intensificar a vigilância de dados e de diminuir a pirataria. Os provedores foram obrigados a ceder dados para a identificação de internautas infratores, sendo permitido ao Estado interromper o acesso à *internet* e remover conteúdo sem prévia autorização judicial. A Espanha é tida, internacionalmente, como defensora de maior controle dos acessos e de adotar uma postura similar à francesa em relação a propriedade intelectual (Segurado, Lima, Ameni, 2015).

A França, como dito, também adota foco legislativo na propriedade intelectual, podendo ser mencionada a Lei de Criação e *Internet* promulgada em 2009. É reconhecida internacionalmente por ter uma das legislações mais duras nessa seara. O controle é exercido pela Hadopi, uma autoridade pública independente responsável por monitorar o fluxo de conteúdos e aplicar o sistema de resposta gradativa (*réponse graduée*). A sistemática envolve advertências por *e-mail* e por carta, assim como acusação judicial, multas e interrupção do serviço de *internet* em casos de persistência na infração. Alinhada aos Estados Unidos da América, a França defende maior controle da *internet* e apresenta posições mais conservadoras em privacidade, segurança e vigilância (Segurado, Lima, Ameni, 2015).

No Reino Unido vigora a regra do *notice and take down*, que significa “notificar e remover”, já que as plataformas são “obrigadas a criar meios eficazes e transparentes para os usuários denunciarem qualquer tipo de conteúdo ilegal publicado nas redes”, especialmente se relacionados a pornografia infantil, racismo, discurso de ódio, *fake news* e violações aos direitos à honra subjetiva (G1, 2024). O descumprimento das regras gera para as empresas o pagamento de pesadas multas, podendo existir, inclusive, responsabilização penal dos responsáveis pelo inadimplemento. Exige-se das plataformas uma postura ativa de vigilância, sem que seja necessário aguardar denúncias dos usuários ou decisões judiciais.

Na Austrália, não foi adotada (até 2020) regulação exclusiva e abrangente

sobre neutralidade de rede, não obstante tenha o órgão regulador (ACMA) editado diretrizes sobre aplicações específicas e o tema tenha sido debatido. Nesse contexto, o presidente da NBN (Rede Nacional de Banda Larga) reconheceu, em 2015, a inevitabilidade de um debate nacional sobre o tema, em razão do crescente uso de serviços de *streaming* (Setenareski, Peres, Bona, Duarte JR., 2020).

Por fim, na África do Sul, o órgão regulador DTPS (*Department of Telecommunications and Postal Services*) fomentou discussões sobre o tema. Em relatório elaborado no ano de 2015, o DTPS delineou recomendações para a neutralidade da rede, incluindo transparência, não bloqueio de conteúdo legal e não discriminação não-razoável de tráfego, sendo admitidas exceções para serviços de emergência e o bloqueio de conteúdo considerado ilegal (Setenareski, Peres, Bona, Duarte JR., 2020).

Grandes os esforços, nos mais diversos países do mundo, porém, igualmente grande é a diversidade de enfrentamentos para o mesmo assunto. De um lado, louváveis avanços; do outro, o risco imposto a todos pela inexistência de regras claras e aplicáveis em consenso.

## 2.5 Revisitando o passado com olhar do presente: a sociedade de risco digital

Pede-se licença, sem qualquer fonte bibliográfica, apenas para partir do pressuposto de que a sociedade está em contante transformação. As dinâmicas sociais se alteram de forma intensa desde meados do Século XX, com o aumento da globalização, mas ganhou expressiva relevância a partir da construção da sociedade moderna e digital do Século XXI.

No Sistema Feudal que perdurou durante a Idade Média, o sistema capitalista hoje reconhecido como profundamente dominante criou suas raízes, marcando a transição para a Primeira Modernidade. Na Primeira Modernidade, a imprecisão e a heterogeneidade deram lugar à precisão e à homogeneidade, com o estabelecimento de um movimento de ordem e de certeza como transição da sociedade feudal para a sociedade capitalista (Bittar, 2005).

Desta maneira, entende-se que a Primeira Modernidade incorporou categorizações sociais com as sociedades do Estado nacional, as sociedades grupais coletivas, a distinção entre sociedade e natureza, a fonte inesgotável de recursos e as sociedades de trabalho ou de pleno emprego, frutos da dinâmica industrial (Cardoso,

2010).

Ulrick Beck propôs o conceito de sociedade de risco na sua obra seminal *Risk Society: Towards a New Modernity*, como aponta Guivant (2001). Trata-se de verdadeiro ponto de inflexão nas ciências sociais para deslocar o foco da análise das desigualdades estruturais para os riscos globais que são produzidos pela modernidade avançada. Segundo o autor, a sociedade moderna está em constante mudança porque é dinâmica, alterando sua organização de forma profunda. A constante transformação pode gerar uma "autodestruição", quando um tipo de modernização pratica autofagia ou modifica outro. A este estado constante de alteração e insegurança, o autor chamou de "modernização reflexiva"[31].

Trata-se de novo paradigma interpretativo da modernidade, ao propor uma ideia de sociedade de risco global de onde emergem perigos oriundos do próprio processo de modernização, sobretudo no âmbito da ciência e da tecnologia. Os riscos globalizados, produzidos de maneira invisível e difusa, desafiam os fundamentos da modernidade clássica e geram a necessidade de revisão crítica das categorias que sustentam o Estado de Direito (Guardia, Silva, 2019).

A tese central de Beck, ao conceituar sociedade de risco, aponta para a capacidade preditiva e controladora da ciência moderna. O avanço técnico-científico, ao invés de eliminar perigos, passa a produzir novas ameaças que são externalizadas economicamente, legitimadas cientificamente e minimizadas politicamente. Desta forma, a sociedade moderna, quando deveria garantir segurança, inaugura um novo tipo de vulnerabilidade que, em razão da globalização, não respeita fronteiras nacionais, classes sociais ou sistemas políticos. Tem-se que o conceito do risco adquire dimensões global e transversal (Guivant, 2001).

Em meados do Século XX, Ulrick Beck (1997) passou a apontar sobre um movimento de alteração e de extinção das formações de classe, camadas sociais, ocupação, papéis dos sexos, família nuclear, agricultura e setores empresariais, até então, tradicionais. Categorizando as mudanças como autodestruições sociais, quando a modernização do que é novo destrói ou modifica o antigo, o autor nomeou

---

[31] "Assim, em virtude de seu inerente dinamismo, a sociedade moderna está acabando com suas formações de classe, camadas sociais, ocupação, papéis dos sexos, família nuclear, agricultura, setores empresariais e, é claro, também com os pré-requisitos e as formas contínuas do progresso técnico-econômico. Este novo estágio, em que o progresso pode se transformar em autodestruição, em que um tipo de modernização destrói outro e o modifica, é o que eu chamo de etapa da modernização reflexiva" (Beck, 1995, p. 13).

o fenômeno de “modernização reflexiva”.

Deve-se ter em mente, contudo, que a visão de Ulrick Beck tinha o contexto de análise com a influência da observação das transformações sociais oriundas da Revolução Industrial, ocorrida entre as décadas de 1760 e 1840. Segundo o autor, o mundo é necessariamente uma sociedade de risco que tem níveis de ameaça muito superiores à imaginação. Existe um constante estado de “permanência da necessidade de tomar decisões que tocam a substância da sobrevivência” (Beck, 2003, p. 206).

Na análise de Ulrich Beck (1997), a discussão sobre lutas de classes trabalhadas por Karl Marx no desenvolvimento das suas teorias sobre o proletariado cedeu espaço para o dinamismo industrial. Esse dinamismo, por sua vez, passou a transformar a sociedade sem a necessidade de grandes revoluções. Desta forma, a transição da Primeira para a Segunda Modernidade, com a ausência de grande revolução, teria ocorrido de maneira apolítica e alheia ao parlamento, ao governo e ao público, passando a ser perceptível somente após conflitos de opiniões e de interpretações sobre a organização social (Cardoso, 2010).

Os paradigmas da Primeira Modernidade, que se caracterizava pela produção de riquezas e pela previsibilidade técnica, foram rompidos para dar lugar à modernização reflexiva, com riscos que extrapolam o domínio local, tornam-se transnacionais e, por vezes, imprevisíveis (Guardia, Silva, 2019). Na sociedade de risco, ninguém está seguro. São atingidos indistintamente produtores e consumidores, ricos e pobres, ainda que de forma desigual.

Referido movimento de transição, contudo, não foi desejado e sequer previsto. Em verdade, a ausência de percepção social gerou uma compulsividade em relação ao despertar do dinamismo da modernização reflexiva. Como explicado, Beck analisava o fenômeno da modernização reflexiva sob a ótica da sociedade pós-revolução industrial. A certeza de um progresso e a abstração dos possíveis efeitos e riscos ecológicos que dominam os pensamentos da sociedade de risco seriam as causas da produção das “constelações da sociedade de risco” [32], que continuam a

[32] “Pode-se virtualmente dizer que as constelações da sociedade de risco são produzidas porque as certezas da sociedade industrial (o consenso para o progresso ou a abstração dos efeitos e dos riscos ecológicos) dominam o pensamento e a ação das pessoas e das instituições na sociedade industrial. A sociedade de risco não é uma opção que se pode escolher ou rejeitar no decorrer de disputas políticas. Ela surge na continuidade dos processos de modernização autônoma, que são cegos e surdos a seus próprios efeitos e ameaças” (Beck, 1997, p. 16).

surgir diante da continuidade dos processos de modernização autônoma, “cegos e surgos a seus próprios efeitos e ameaças”.

O movimento de modernização reflexiva viabiliza o conceito de sociedade de risco, permeada de riscos ecológicos, conflitos na distribuição de renda e imprevisibilidade das ameaças provocadas pelo desenvolvimento técnico-industrial (Beck, 1997).

Os riscos não apenas coexistem com desigualdades estruturais, mas frequentemente as agravam, principalmente em países que contam com frágil institucionalidade democrática e precários mecanismos de controle social. A globalização, o avanço tecnológico e a desconstrução das instituições que causavam as certezas sociais geram um ambiente em que ninguém está seguro. A própria sociedade introjeta e alimenta o risco, gerando a descaracterização das categorias sociais e a geração de novas categorias autofágicas.

Zygmunt Bauman analisou o mesmo fenômeno, entretanto, optando por chama-lo de Pós-Modernidade, similar ao fenômeno da Modernidade Reflexiva de Ulrich Beck (Cardoso, 2010). No entender de Bauman (1999), a Pós-Modernidade é a modernidade reconhecendo sua própria impossibilidade, mas reconhecendo, também, a necessidade de automonitoramento e de conscientemente descartar o que outrora fazia inconscientemente.

Na verdade, para Bauman, a pós-modernidade não nasce com a intenção de rejeitar a modernidade, mas, na verdade trata-se de um processo de maturação em que aquela assume sua própria impossibilidade, visto que esta se automonitora e “descarta o que outrora fazia inconscientemente”[33].

Percebe-se um esforço para orientar a reinvenção da política e da sociedade, entretanto, sem mecanismos efetivos de implementação. A visão de sociedade de risco não pode ser eurocêntrica e tampouco linear diante da perspectiva evolutiva das diversas realidades híbridas do mundo contemporâneo. Muitas sociedades ocidentais ainda enfrentam, simultaneamente, condições de escassez e de exposição a riscos

[33] “A pós-modernidade não significa necessariamente o fim, o descrédito ou a rejeição da modernidade. Não é mais (nem menos) que a mente moderna a examinar-se longa, atenta e sobriamente, a examinar sua condição e suas obras passadas, sem gostar muito do que vê e percebendo a necessidade de mudança. A pós-modernidade é modernidade que atinge a maioridade, a modernidade olhando-se à distância e não de dentro, fazendo um inventário completo de ganhos e perdas, psicanalisando-se, descobrindo as intenções que jamais explicitara, descobrindo que elas são mutuamente incongruentes e se cancelam. A pós-modernidade é a modernidade chegando a um acordo com a sua própria impossibilidade, uma modernidade que se automonitora, que conscientemente descarta o que outrora fazia inconscientemente” (Bauman, 1999, p. 288).

modernos, evidenciando a coexistência de múltiplas modernidades (Guivant, 2001).

A transição da Primeira para a Segunda Modernidade gerou um ambiente em que a percepção de risco se dilui. Os geradores de risco estão, também, sujeitos aos riscos gerados, cenário potencializado diante da integração mundial de contextos ecológicos, sistemas políticos, de economia globalizada e do mundo virtual. Significa que ninguém está seguro porque mesmo os que geraram o risco podem ser atingidos pelas consequências[34].

Os conceitos de sociedade de risco ou de pós-modernidade, inicialmente trabalhados em um cenário analógico, ganham expressiva tônica com o advento da Rede Mundial de Computadores, conhecida como *internet*, contribuindo sobremaneira para a integração de um mundo cada vez mais conectado e globalizado. A ferramenta, com inegáveis alcance e capacidade de facilitar a vida humana, também viabiliza um exponencial aumento da exposição ao risco causado a si ou a terceiros.

Na *internet* acessível, que não conhece local, classe social ou faixa etária, torna-se praticamente ilimitada a possibilidade de transmissão de informações em um ambiente de ausência de regulação estatal. Além da possibilidade mundial de acesso a conteúdo, a disseminação pode ocorrer de forma instantânea, aumentando o conhecimento ou a reprodução de material produzido ou compartilhado *online*.

Apesar da *internet* ter surgido na década de 1960 através da rede *Arpanet*, como já explicado, apenas no Século XXI que ocorreu a sua efetiva democratização do acesso, especialmente com o avanço dos computadores, dos aparelhos celulares e das tecnologias de transmissão de dados.

A irreversibilidade da globalização é elemento estruturante da sociedade de risco. As tecnologias de informação são difundidas de forma acelerada, integradas a mercados financeiros e indústrias globais, criando um espaço social radicalmente novo. A nova lógica econômica é acompanhada pela produção massiva de riscos ecológicos, tecnológicos, sanitários e econômicos que impactam diretamente as estruturas jurídicas e marcos normativos tradicionais. O Estado não mais consegue mitigar ou controlar sozinho o risco globalizado (Guardia, Silva, 2019).

A própria responsabilidade política ganha nova dinâmica, visto que a produção

---

[34] “Numa sociedade de risco da Segunda Modernidade ninguém está seguro. Aqueles que geram os riscos não mais estão livres das consequências do que geraram. Os riscos ambientais e à saúde podem se transformar em riscos econômicos, gerando, por exemplo, a perda do valor das ações de empresas poluidoras ou que afetem, de algum modo, a saúde da população (indústria farmacêutica, por exemplo)” (Cardoso, 2010, pp. 108-109).

social de riscos, por ser inevitável, impõe desafios à governança democrática. A participação cidadã é enfraquecida diante do deslocamento do debate político para as esferas técnicas, frequentemente inacessíveis e opacas ao público (Guardia, Silva, 2019).

Com essa mudança social emerge a sociedade de risco digital. A autotransformação e autofagia sociais denunciadas anteriormente por Beck e Bauman, apesar de conceitos relativamente antigos, ganham tônica de modernidade ao gerar um ambiente virtual onde ninguém está seguro e todos alimentam e se expõem ao risco simultaneamente. É necessário investigar como o direito brasileiro vem lidando com a nova realidade.

# 3 A TUTELA JURÍDICA DE AGENTES DIGITAIS NO DIREITO BRASILEIRO

O termo “responsabilidade” diz respeito “à condição ou qualidade de alguém em ser responsável” (Normando, 2012). Significa que o responsabilizado deve ter consciência em relação aos atos que pratica e às consequências da sua vontade materializada, que podem ter relação com o plano jurídico diante de deveres ou obrigações morais e legais socialmente impostas.

No Brasil, o termo é largamente utilizado no direito, existindo as mais diversas responsabilizações: responsabilidade civil, responsabilidade penal, responsabilidade do Estado, responsabilidade administrativa, dentre outras. Em todas as responsabilizações, como será tratado adiante, exige-se que o agente tenha discernimento para entender o ato que está praticando (ou o risco do ato, mesmo que consiga prever o resultado), assim como que um efetivo dano tenha ocorrido. Além disso, o ato e o dano devem estar unidos por um nexo de causalidade, significando que, sem vinculação direta a um ato imputável a alguém, o dano nunca seria produzido.

Como já exposto, o advento da internet transformou as relações sociais, na medida em que a sociedade ficou mais conectada. É extremamente comum e até necessária a utilização de aparelhos celulares e computadores conectados à rede mundial de computadores, para que o usuário tenha mínimas condições de trabalhar e se relacionar socialmente, sob pena de ser extirpado da convivência social ou, no mínimo, segregado por não se adequar aos padrões.

Na persecução do lucro e com o mercado regido pela lógica do capital, programações e algoritmos disputam espaço para que os usuários consumam conteúdo e utilizem serviços, podendo os agentes digitais (provedores de serviços de internet, usuários, influenciadores, empresas etc.) incorrer em condutas vedadas pelo ordenamento jurídico que causam danos individuais ou à coletividade.

O termo *cyberanarchy*[35], ou “anarquia cibernética”, ganha expressivo relevo nessa realidade digital, tratando-se de nova conformação dos fatos de cunho libertário

[35] “O espaço virtual ultrapassa radicalmente a relação entre realidade virtual e localização física. O crescimento de uma rede global de computadores está destruindo a ligação entre localização geográfica e: (1) o poder dos governos locais de exercer controle sobre o comportamento *online*; (2) os efeitos do comportamento *online* em indivíduos e bens; (3) a legitimidade de determinado poder soberano local para regulamentar uma realidade global; (4) a capacidade de qualquer entidade física de declarar quais regras devem ser aplicadas” (Longhi, 2025, p. 85).

que prega a independência total do espaço virtual. Como reação, a regulamentação internacional sobre a utilização da *internet* ganhou força nos últimos anos, na tentativa legal e governamental de regular o risco social criado, já que em uma sociedade hiper conectada ninguém está seguro. Obviamente, os atos de governo e as leis são feitas por pessoas que podem utilizar a função para exprimir os próprios interesses. Entretanto, tal contexto da falibilidade humana não afasta uma tendência mundial de regulamentação e controle da utilização da *internet*.

Nesse complexo cenário digital que surge o desafio jurídico da tutela dos direitos de personalidade[36], que passam a incidir, segundo o direito brasileiro, a partir do nascimento com vida (concepção natalista dos direitos de personalidade). Em verdade, o nascimento com vida não é o marco inicial de direitos à vida, à integridade física, à honra e à imagem, que seriam atributos do nascituro desde o momento da sua concepção, mas apenas a consolidação, com a possibilidade jurídica de defendê-los (Asfor, 2015).

Além disso, como também explicado anteriormente, a questão da responsabilização jurídica por ofensa a direitos individuais e coletivos não pode ser analisada sem considerar a mudança interpretativa do Marco Civil da *Internet*, pelo Supremo Tribunal Federal, em relação ao julgamento dos Temas 987 e 533. Para mais detalhes acerca do que será revisado abaixo, conferir o tópico 2.1.1.

O sobredito julgamento alterou a interpretação da literalidade da lei, já que o STF passou a considerar que não é mais necessária, em regra, ordem judicial como condição prévia de responsabilização, quando for necessário tutelar bens jurídicos de alta relevância, como a dignidade da pessoa humana, a honra e a própria democracia.

Foi definido, em uma reinterpretação do art. 21 do *Marco Civil da Internet*, que os provedores de aplicação de *internet* podem ser responsabilizados independentemente de ordem judicial, mesmo que notificados extrajudicialmente acerca de crimes ou atos ilícitos em suas plataformas, se ficarem inertes na remoção do conteúdo. A ordem judicial remanesceu necessária para os casos de crimes contra a honra, sendo que, uma vez reconhecida judicialmente a ilicitude, a simples notificação já é capaz de obrigar as plataformas a removerem o conteúdo indevido.

---

[36] “A personalidade não é um direito, de modo que seria errôneo afirmar que o ser humano tem direito à personalidade. A personalidade é que apoia os direitos e deveres que dela irradiam, é o objeto de direito, é o primeiro bem da pessoa, que lhe pertence como primeira utilidade, para que ela possa ser o que é, para sobreviver e se adaptar às condições do ambiente em que se encontra, servindo-lhe de critério para aferir, adquirir e ordenar outros bens” (Diniz, 2007, p. 72).

Foi estabelecida também a presunção de responsabilidade em situações específicas, como anúncios ou impulsionamentos pagos e no uso de redes artificiais de distribuição ilícita. Também foram estabelecidos: o “dever de cuidado” para os crimes de maior gravidade (terrorismo, pornografia infantil, tráfico de pessoas, discriminação, violência de gênero, atos antidemocráticos); as obrigações de transparência e prestação de contas pelas plataformas; e a determinação de que provedores estrangeiros que atuem no Brasil tenham representante legal no país.

Feita essa recapitulação, é possível discutir como remanesce a responsabilização jurídica dos agentes digitais. Cabe analisar de forma breve, diante do escopo do presente trabalho, como o ordenamento jurídico brasileiro, assim como seus aplicadores, regula a responsabilização jurídica daqueles que atuam na internet, especialmente nas áreas jurídicas mais abrangentes.

## 3.1 A responsabilização cível *lato sensu*

A responsabilidade civil é instituto já bem desenvolvido no Direito Brasileiro, encontrando guarida em diversos artigos do Código Civil (Lei 10.406/2002). De início, o Código define o ato ilícito no art. 186, caracterizando-o como ação ou omissão voluntária, podendo ser negligente ou imprudente, que viole direito ou cause dano a outrem, ainda que exclusivamente moral.

Ou seja, nos termos do art. 189 do Código Civil, para o ofendido, em relação àquele que pratica ato ilícito e viola direito, nasce uma pretensão sujeita à prescrição, que sejam reconhecidos a responsabilidade civil e o dever de indenizar. O dever de indenizar decorrente da responsabilidade civil é reforçado no art. 927 da mesma lei, que obriga aquele que causa dano a outrem a repará-lo.

Inclusive, dependendo da situação, essa obrigação indenizatória pode ser decorrente exclusivamente de culpa (aqui, não no sentido do direito penal, mas sim no evidente nexo de causalidade entre a conduta do agente, indispensável para a consumação do ilícito, e o dano causado), ou independente de culpa, nos casos especificados em lei (art. 927, parágrafo único, do Código Civil).

Sobre o valor da indenização, o Código Civil determina que deve ser medida pela extensão do dano (art. 944), podendo haver redução equitativa do valor em caso de excessiva desproporção entre a gravidade da culpa e o dano (art. 944, parágrafo único) e a fixação do montante considerando eventual concorrência da vítima para o

resultado danoso (art. 945).

O instituto da responsabilidade civil, portanto, pressupõe que o sujeito ativo capaz de exigir o pagamento de uma indenização, a ser paga pelo sujeito passivo, tenha sofrido um prejuízo em razão de alguma ação ou omissão. Não se trata apenas de responsabilização que nasce de um negócio jurídico (como inadimplemento contratual, por exemplo), mas, também, de um ato ilícito ou de um fato jurídico[37].

Esses são, em suma, os mais importantes dispositivos do Código Civil, no que diz respeito à responsabilização, cabendo agora analisar a incidência do instituto nas relações jurídicas que tomam forma nas redes sociais.

Realmente, a aplicação da responsabilidade civil às plataformas digitais é tema de grande complexidade diante das novas dinâmicas de interação e consumo de informação. As plataformas digitais assumem relevante papel na mediação de relações sociais e comunicacionais, tendo o dever de moderação de conteúdo e de proteção de dados pessoais para zelar pela integridade dos usuários. A responsabilidade civil das empresas pode surgir, corolário, tanto em razão de atos próprios (falhas de segurança ou algoritmos discriminatórios, por exemplo) quanto por omissão em face de conteúdos gerados por terceiros que causaram danos a outrem (Soares, 2023).

No âmbito das *internet,* o fundamento de ação ou omissão, culpa ou dolo, nexo causal e dano se aplica a qualquer agente que viole direitos de personalidade de terceiros, como a honra, imagem, privacidade e intimidade, além de ser aplicável tanto a usuários comuns quanto a influenciadores digitais, uma vez que estes, ao atuarem nas redes, tornam-se emissores de conteúdos públicos potencialmente lesivos, estando sujeitos às mesmas regras que qualquer terceiro que venha violar direitos fundamentais ou causar prejuízo moral ou patrimonial (Dutra, Silva, 2016).

---

[37] “A doutrina tradicionalmente divide a responsabilidade civil em *contratual* e *extracontratual*. No primeiro caso, há contrato entre o credor e o devedor da obrigação de indenizar; no segundo, não. Quando o advogado indeniza o cliente por ter perdido o prazo para contestar, sua responsabilidade é considerada por este enfoque como contratual porque entre os sujeitos da obrigação de indenizar (prestação) há um contrato de mandato. Já na hipótese do acidente de trânsito, entre os motoristas não há nenhuma relação contratual, e o enfoque tradicional chama a hipótese, então, de responsabilidade civil extracontratual. A doutrina, então, dedica-se a discutir as diferenças entre uma e outra espécie de responsabilidade, tendo ultimamente predominado o entendimento de que não há relevância na distinção [...]. Com efeito, segundo as leis brasileiras, se o consumidor vitimado por acidente de consumo demandar o ressarcimento contra o fornecedor terá o mesmo direito, seja sustentando o pleito na relação extracontratual, seja na contratual – quadro que se repete nas demais hipóteses da chamada responsabilidade civil contratual” (Coelho, 2020, p. 150).

As plataformas e influenciadores digitais atuam como catalisadores desses efeitos, aumentando a frequência de ocorrência de danos morais extrapatrimoniais que devem ser tutelados pelo ordenamento jurídico brasileiro (Maia, Curvo, 2025). Na prática, o ambiente virtual não alterou a essência legislativa da responsabilização civil, mas intensificou os riscos e ampliou a complexidade na identificação dos atos ilícitos, especialmente em razão da velocidade na propagação das publicações, da amplitude das redes e da multiplicação de danos à honra, à imagem e à dignidade da pessoa humana.

Sem dúvidas as redes sociais intensificaram a vulnerabilidade dos direitos de personalidade, considerando a velocidade de propagação de informações e o comportamento dos usuários que frequentemente ultrapassam os limites da liberdade de expressão. Esse cenário engloba os influenciadores digitais que, em razão do alcance ampliado que possuem, podem provocar danos com maior repercussão quando divulgam comentários ofensivos ou conteúdos potencialmente ilícitos. Nesses casos que a responsabilização cível subjetiva emerge como independente do Marco Civil da *Internet*, já que são profissionais que produzem diretamente o conteúdo indevido (Dutra, Silva, 2016).

Neste norte, é imprescindível que seja feita uma distinção entre os autores de conteúdo e os provedores de aplicações. Enquanto os primeiros (influenciadores) respondem diretamente pelos danos decorrentes das informações que produzem, as plataformas digitais são responsáveis apenas nas situações específicas previstas no Marco Civil da *Internet*, inclusive com a já explicada reinterpretação realizada pelo STF, no julgamento dos Temas 533 e 987.

Quando um influenciador publica ofensas, viola a honra alheia ou divulga conteúdo ilícito, a responsabilização é exclusiva, cabendo reparação integral (salvo se a informação divulgada disser respeito a publicidade contratada que equipare o influenciador a um fornecedor de produtos e serviços, juntamente com outro agente, nas relações regidas pelo Código de Defesa do Consumidor). A solidariedade da plataforma, por outro lado, apenas vai surgir quando deixar de retirar o conteúdo indevido, antes ou após notificação extrajudicial ou judicial, conforme as hipóteses dos Temas 533 e 987 do STF (Dutra, Silva, 2016).

A distinção é relevante. Para os influenciadores digitais, enquanto pessoas físicas e autoras de conteúdo, a responsabilização subjetiva e imediata é aplicável desde o momento da atuação, podendo a plataforma, por outro lado, ser acionada

extrajudicialmente ou judicialmente, entretanto, com hipóteses mais restritas do que a pessoa física causadora do dano (Dutra, Silva, 2016), diante da reinterpretação do STF do Marco Civil da *Internet.* Tem-se uma responsabilização limitada e subsidiária das plataformas digitais, enquanto os autores de conteúdo respondem de forma direta e primária.

O maior problema das ofensas proferidas na *internet* diz respeito à identificação do autor direto das publicações ofensivas, questão que se agrava diante do anonimato e da proliferação de perfis falsos. Existem precedentes do Superior Tribunal de Justiça (a exemplo dos recursos especiais 1.993.896/SP e 1.829.821/SP) que determinavam, mesmo antes da mudança paradigmática realizada pelo STF, em 2025, na reinterpretação do Marco Civil da *Internet,* que as plataformas têm o dever legal de guardar e fornecer registros que viabilizem a identificação do responsável (Maia, Curvo, 2025).

Nesse raciocínio, uma possibilidade de responsabilização civil diz respeito às plataformas de mídia social que permitem a disseminação de conteúdos difamatórios. A jurisprudência tinha o entendimento de que existe a obrigação de remover o material ilícito imediatamente após o recebimento de notificação formal, devendo a empresa, caso mantenha o conteúdo ativo, assumir o risco de responder civilmente pelos danos causados, em homenagem ao princípio da boa-fé e ao dever de cooperação imposto a intermediários digitais (Soares, 2023).

Outro exemplo diz respeito a violações de dados pessoais, já que plataformas que armazenam grandes volumes de informações sensíveis podem ser responsabilidades por não adotarem medidas de segurança adequadas. Eventual negligência pode ser caracterizada em caso de ausência de aplicação de mecanismos eficazes de proteção, entendimento que encontra respaldo na Lei Geral de Proteção de Dados e em legislações internacionais, a exemplo do Regulamento Geral de Proteção de Dados (GDPR) europeu (Soares, 2023).

Também pode existir a responsabilização civil em casos de discriminação algorítimica, podendo ser exemplificada quando a plataforma de recrutamento utiliza sistemas automatizados que geram viés de gênero na seleção de pessoas. A tecnologia, mesmo sem intenção direta, pode produzir resultados discriminatórios, além de violar direitos fundamentais e princípios de igualdade. As plataformas devem zelar pela imparcialidade de decisões automatizadas, especialmente em razão da falta de auditoria e de transparência nos algoritmos (Soares, 2023).

Em relação aos direitos autorais, plataformas que permitem compartilhamento e visualização de vídeos, a exemplo do *YouTube,* também podem ser responsabilizadas. Geralmente, a plataforma não será responsabilizada se remover imediatamente o conteúdo após a notificação do titular do direito autoral, havendo distinção jurisprudencial entre a responsabilidade primária em relação ao usuário que postou o conteúdo violador, e a responsabilidade subsidiária para a plataforma que se omitiu após a ciência do conteúdo violador estar no ar (Soares, 2023).

Não se deve perder de vista que mecanismos eficientes de responsabilização civil funcionam, no ambiente digital, não somente como instrumento reparatório, mas também para prevenção e desestímulo de práticas ilegais. O espaço virtual, marcado por discursos discriminatórios, disseminação de *fake news* e exposições indevidas, por vezes potencializados pelo alcance de influenciadores, é inegável o caráter pedagógico da responsabilização. A atuação judicial deve ser firme e efetiva com a determinação de remoção de conteúdos indevidos, bloqueio de perfis ofensivos e indenizações por danos morais (Maia, Curvo, 2025).

Por outro lado, a regulamentação de plataformas e das publicações nas redes pode trazer tanto benefícios quanto riscos. O aumento da responsabilização tem o potencial de reforçar direitos de personalidade, entretanto, a excessiva regulação pode comprometer a liberdade de expressão, gerar censura ou mesmo remoções preventivas indevidas. A solução adequada é sempre o “dever ser” da proporcionalidade, de maneira que a responsabilização cível atinja as plataformas – e, por extensão, os influenciadores – através de critérios técnicos e jurídicos sólidos que assegurem a tutela efetiva sem restringir injustamente o espaço democrático digital (Maia, Curvo, 2025).

Sem pretensão de esgotar o tema, a responsabilização civil é gênero, conceito amplo que abarca outras hipóteses mais específicas, como a responsabilização jurídica nas relações de consumo ou a tutela dos direitos de grupos vulneráveis, como menores e idosos, temas trabalhados adiante.

## 3.2 A responsabilidade jurídica nas relações de consumo criadas na *internet*

Como exposto, a expansão das redes sociais transformou sobremaneira a forma que os indivíduos consomem informações e tomam decisões, criando um ambiente de alta exposição e intensa circulação de conteúdos, especialmente, com a

participação de influenciadores digitais. Essa nova categoria profissional exige que a responsabilização adquira novos contornos, no escopo de evitar danos que possam surgir especialmente na prestação defeituosa de serviços ou na venda de produtos viciados. Além disso, deve haver um zelo com a possibilidade de difusão de informações incorretas, enganosas ou incompletas que sejam capazes de afetar as escolhas de consumo. Nesse cenário que a responsabilização consumerista evolui para abranger danos decorrentes de publicidade enganosa, difamação e divulgação de conteúdos inverídicos, tanto de empresas quanto de indivíduos que utilizam as redes sociais para promover bens ou serviços (Lima, Menezes, Cardoso, 2023).

Com efeito, as redes sociais e a dinâmica comunicacional ampliaram sobremaneira mensagens publicitárias, que inclusive expõem os consumidores aos riscos decorrentes da circulação de conteúdo persuasivo, impreciso ou manipulado. Nesse contexto, a responsabilidade civil é instituto de grande importância, especificamente na difusão de informações que, não obstante estejam amparadas pela liberdade de expressão e pela livre iniciativa, deve respeitar os limites constitucionais, legais e éticos. (Furtado, Goulart, 2022).

Em verdade, vive-se em uma realidade agravada pela “sociedade de exposição”, quando a autopromoção torna-se mercadoria e a vida cotidiana dos influenciadores é utilizada como estratégia de marketing. Referido cenário torna dificultosa a distinção entre a vida real e a publicidade, dificultando que o consumidor possa identificar quando está diante de um anúncio ou de um conteúdo pessoal. Essa confusão reforça os casos de responsabilização, já que a ausência de transparência, principalmente quando inexiste indicação clara de conteúdo patrocinado, potencializa a percepção enganosa e conduz o consumidor a más escolhas (Lima, Menezes, Cardoso, 2023).

A publicidade, apesar de constitucionalmente protegida como forma de comunicação e instrumento econômico, não pode ser tratada como ilimitada quando ultrapassa os limites postos pelo ordenamento jurídico, devendo ser reconhecido, nesses casos, o dever de reparar os danos decorrentes da violação da boa-fé objetiva, da confiança do consumidor e da segurança das relações de consumo (Furtado, Goulart, 2022).

Ademais, o CDC traz diversas responsabilidades do fornecedor e direitos básicos do consumidor (art. 6º). Trata-se de lei de amplo espectro que busca proteger a parte vulnerável/hipossuficiente, prevendo, inclusive, o direito à inversão do ônus da

prova, a seu favor, no processo civil, quando houver verossimilhança de suas alegações ou hipossuficiência judicialmente reconhecida.

O Código de Defesa do Consumidor adota a responsabilização objetiva do fornecedor de produtos e serviços, aplicável, igualmente, aos influenciadores digitais e quaisquer outros agentes que passam a integrar a cadeia de consumo (art. 3º). Segundo o art. 7º, parágrafo único, do CDC, existe solidariedade entre todos os que concorrem para o evento danoso, o que alcança tanto o fornecedor formal quanto quem atua de forma intermediária. Ainda quanto à publicidade de produtos e serviços, os agentes digitais que lucram com a prática enquadram-se na teoria do risco-proveito: se auferem vantagens econômicas com a atividade, devem responder pelos riscos que criam ou ampliam, independentemente da aferição de culpa (Vale, Coimbra, Oliveira, 2023).

A capilaridade social dos influenciadores digitais adquire relevância quando mobilizam seguidores que criam identificação com os estilos de vida apresentados nas redes, exercendo influência direta sobre o comportamento de consumo. Muito mais do que a mera apresentação de produtos, é construído verdadeiro capital social, baseado na exposição de rotinas, preferências de intimidade que cria um vínculo de confiança com o público, aumentando a credibilidade das recomendações. Sob essa perspectiva, é possível enquadrar os influenciadores como verdadeiros atores na cadeia de consumo, de forma que se equiparem a fornecedores de produtos e serviços para fins de responsabilização civil, especialmente na promoção de produtos ou serviços sem a necessária verificação de qualidade, eficácia ou veracidade das informações divulgadas (Lima, Menezes, Cardoso, 2023).

Ainda sob a ótica do Código de Defesa do Consumidor, saltam aos olhos dois eixos fundamentais de responsabilização, relacionados à atividade publicitária: a publicidade enganosa e a publicidade abusiva. De acordo com o art. 37, §1º, do CDC, a publicidade enganosa pode ser caracterizada quando o consumidor é induzido a erro, seja de forma comissiva (a informação transmitida é total ou parcialmente falsa), seja de forma omissiva (quando há supressão de dado essencial para a compreensão adequada do serviço ou produto). Esse vício causa um desvirtuamento da vontade do consumidor, que age mal-informado para tomar uma decisão que não tomaria se conhecesse a verdade. Nesses casos, inexiste a necessidade de demonstração de culpa, visto que a responsabilização é objetiva (Furtado, Goulart, 2022).

Por outro lado, a publicidade abusiva descrita no art. 37, §2º, do CDC, é ainda

mais grave, já que se trata de mensagem contrária a valores jurídicos e sociais que são reconhecidos pelo ordenamento jurídico, a exemplo da dignidade da pessoa humana, da não discriminação e da proteção da saúde e da segurança do consumidor. Pode ser verificada, a título de exemplo, quando a mensagem incentivar comportamentos perigosos, explorar o medo, a superstição ou a vulnerabilidade emocional do consumidor. Trata-se de afronta não apenas ao CDC, mas principalmente, ao próprio sistema de proteção constitucional, sujeitando o fornecedor a sanções civis, administrativas e penais, incluindo a contrapropaganda e as demais medidas previstas nos arts. 56, 60, 67 e 68 do CDC (Furtado, Goulart, 2022).

A difusão digital, sem dúvidas, potencializa o risco da ocorrência das condutas de publicidades enganosa e abusiva, já que as redes sociais viabilizam ampla audiência e são operadas em ambiente de baixa regulação prévia, contando com forte apelo emocional, sensacionalista ou estético. Anda bem o ordenamento jurídico ao exigir uma ampliação do dever de cautela do fornecedor para que qualquer conteúdo inadequado, que possa rapidamente causar danos a muitos fornecedores, seja imediatamente removido (Furtado, Goulart, 2022).

Em relação à publicidade enganosa, existem diversas subcategorias, como a publicidade omissiva, exagerada, inteiramente ou parcialmente falsa e comissiva. Todos esses tipos de publicidade são capazes de induzir o consumidor a erro. Eventuais omissões de informações essenciais, a exemplo de riscos, contraindicações ou dados técnicos de determinado produto podem gerar responsabilização jurídica, principalmente quando o influenciador busca promover bens que prometem resultados estéticos ou de saúde (Vale, Coimbra, Oliveira, 2023).

Na publicidade simulada, o anúncio se apresenta de modo disfarçado, sendo impossível ao público que identifique claramente tratar-se de propaganda. A conduta, no caso dos influenciadores, é especialmente reprovável, já que a integração orgânica do produto ao conteúdo comum produzido pelo influenciador dificulta ao seguidor que identifique tratar-se de uma propaganda com intenção comercial. Existem diretrizes do Conselho Nacional de Autorregulamentação Publicitária que repudiam essa prática por impedir que o consumidor se coloque defensivamente diante do apelo publicitário, existindo uma orientação para que o influenciador sempre identifique a postagem como um anúncio, de forma clara e ostensiva (Vale, Coimbra, Oliveira, 2023).

Na lógica da publicidade contemporânea, com a comunicação deslocada dos meios tradicionais para as plataformas digitais altamente segmentadas, o

influenciador não apenas recomenda produtos, mas desempenha um papel central na influência exercida no consumidor, tanto na confiança quando na produção dos sentidos. É comum o exercício de um poder persuasivo que afeta, principalmente, consumidores vulneráveis, sendo o julgamento impactado pela identificação emocional e aspiracional (Vale, Coimbra, Oliveira, 2023).

Os consumidores, assim, têm uma tendência de adquirir bens e serviços não pela análise objetiva da oferta, mas principalmente pela credibilidade que é socialmente atribuída a determinado influenciador, agravando o risco de exposição a práticas ilícitas de publicidade, sobretudo as modalidades abusiva, enganosa e simulada (Vale, Coimbra, Oliveira, 2023).

Não é incomum que celebridades sejam contratadas por empresas para a realização de campanhas publicitárias, mesmo sem a colaboração para o conteúdo do anúncio, quando recebem valores expressivos para emprestar credibilidade à mensagem. Nessas hipóteses, mesmo sem ligação técnica com o produto, celebridades e influenciadores que realizem essa atividade profissional podem gerar responsabilização civil pelos danos decorrentes da publicidade enganosa, especialmente quando a credibilidade pessoal funciona como um elemento persuasivo e indispensável para a decisão do consumidor (Lima, Menezes, Cardoso, 2023).

Nesses casos explicados, o influenciador pode ser responsabilizado civilmente quando indica produtos e serviços porque assume a posição de garantidor, visto que sua credibilidade incentiva diretamente o comportamento do consumidor. Principalmente quando as qualidades divulgadas não correspondem à realidade, o poder persuasivo do influenciador se converte em elemento gerador de dano que viola os princípios da boa-fé e da confiança. A violação é ainda mais grave se dirigida a públicos vulneráveis que confiam sem reservas na autoridade simbólica do influenciador (Vale, Coimbra, Oliveira, 2023).

Um caso específico de responsabilização pode ocorrer quando um influenciador divulga, de maneira voluntária, informações sobre produtos e serviços sem que exista um roteiro prévio, com narrativas persuasivas que ocultam riscos, omitem características essenciais ou atribuem qualidades inexistentes. Na hipótese, existe um claro dever de informação, direito básico previsto no Código de Defesa do Consumidor como corolário do dever de lealdade e da boa-fé objetiva. No momento que o influenciador reforça as narrativas deturpadas, a atuação passa a contar como

publicidade enganosa e gera responsabilidade civil objetiva (Lima, Menezes, Cardoso, 2023).

Outra hipótese que merece menção diz respeito às situações em que os influenciadores digitais atuam como garantidores implícitos da qualidade de um produto, ao assumirem publicamente que é eficaz, seguro ou vantajoso, contribuindo para uma expectativa de confiança. Caso o produto não atenda às expectativas porque não possui as qualidades anunciadas, incide a responsabilidade civil pela quebra do princípio da confiança, indispensável para o sistema consumerista, inclusive porque o CDC presume a vulnerabilidade técnica do consumidor e estabelece a solidariedade entre todos os participantes da cadeia de fornecimento de produtos e serviços, incluindo quando influenciadores digitais atuam de forma decisiva para a formação da decisão de compra (Lima, Menezes, Cardoso, 2023).

Nas plataformas de comércio eletrônico, como o eBay, por exemplo, pode existir a responsabilização civil devido à venda de produtos falsificados. Nessas hipóteses, ainda que a empresa não produza os bens, a omissão na verificação da confiabilidade dos vendedores e dos produtos pode configurar falha na prestação de serviço, atraindo a responsabilização civil pela lógica aplicada ao Código de Defesa do Consumidor (Soares, 2023).

Por fim, em relação a profissionais de saúde, especialmente os médicos, a responsabilização civil decorrente de publicidade digital encontra guarida em rigorosos contornos estabelecidos pelo Código de Ética Médica e pelas Resoluções do Conselho Federal de Medicina, que proíbem a prática de publicidade que possa gerar risco à saúde, comprometer a dignidade do paciente ou transformar a atividade médica em produto comercial (Furtado, Goulart, 2022).

Como exemplos, podem ser citadas: a publicidade enganosa ao anunciar resultados ou técnicas de modo impreciso (quando o profissional atribui ao procedimento qualidades que não possui, omite riscos relevantes ou apresenta técnicas não reconhecidas pelo CFM); a publicidade abusiva (quando o médico divulga conteúdo que cria expectativas irreais, explora fragilidades emocionais ou incentiva comportamentos que podem colocar o consumidor em risco); a conduta de aparentar possuir especialidade que não detém (induzindo o público a acreditar que aquele conhecimento é mais avançado do que realmente é); e a conduta de expor indevidamente a imagem de pacientes, mesmo que exista autorização expressa, (Furtado, Goulart, 2022).

Em suma, sem quaisquer dúvidas, agentes digitais que são figuras centrais de publicidade *online* devem integrar a cadeia de fornecimento de produtos e serviços e observar preceitos essenciais como a boa-fé, a transparência e o dever de informação. A violação desses princípios pode gerar não apenas a responsabilização administrativa, mas também o dever de indenizar, com base no Código Civil e no Código de Defesa do Consumidor.

## 3.3 A proteção jurídica de menores de idade, grupo de hipervulnerabilidade digital

Desenvolvidos os contornos básicos de responsabilização jurídica, no uso da *internet* e na atuação dos provedores de serviços, nas áreas cível e consumerista, deve ser trabalhada de forma mais específica a responsabilização jurídica relacionada aos grupos hipervulneráveis, como menores de idade e idosos.

Se o Ordenamento Jurídico trata especificamente do termo "vulnerável"[38] como aplicado a determinados grupos, a exemplo do Direito do Consumidor, o termo "hipervulnerável" é ainda mais abrangente, já que inerente a uma situação especial do ofendido. Os hipervulneráveis são aqueles que, diante de fatores psicológicos, biológicos e até sociais, possuem fragilidade mais acentuada em relação aos demais indivíduos, como os idosos, crianças e pessoas com deficiência (Nishiyama, Densa, 2010, p. 3).

No aspecto do Direito do Consumidor, os menores, mais vulneráveis, a exemplo de adolescentes insatisfeitos com a própria aparência, podem ser mais facilmente persuadidos por mensagens simplificadas ou idealizadas sobre produtos de emagrecimento, cosméticos, suplementos etc. (Vale, Coimbra, Oliveira, 2023).

A vedação à publicidade abusiva está no art. 37, §2º, do CDC, sendo proibidas práticas que explorem medo, superstição, deficiência de julgamento de crianças ou o incentivo a comportamentos prejudiciais à saúde. No caso dos menores, eis que mais vulneráveis, que compõem grande parte da audiência, o discernimento é reduzido, o que justifica, de acordo com o CDC, o reconhecimento da hipótese de vulnerabilidade

[38] "A noção de vulnerabilidade no direito associa-se à identificação de fraqueza ou debilidade de um dos sujeitos da relação jurídica em razão de determinadas condições que lhe são inerentes ou, ainda, de uma posição de força que pode ser identificada no outro sujeito da relação jurídica" (Marques, Miragem, 2012, p. 162).

agravada. A publicidade realizada se aproveita dessa limitação cognitiva ou emocional para violar a boa-fé e sujeitar o influenciador às consequências civis decorrentes da violação do dever jurídico de não causar danos (Vale, Coimbra, Oliveira, 2023).

Sobre a exposição de imagem no ambiente digital, a responsabilização cível tem contornos específicos em relação a crianças e adolescentes. A condição peculiar de desenvolvimento os torna mais vulneráveis às dinâmicas de exposição, consumo e interação que dominam as redes sociais. A Era Digital, especialmente marcada pelos *smartphones* (telefones inteligentes) e redes sociais, transformou o ambiente familiar e passou a fazer com que pais e responsáveis integrem suas experiências parentais ao cotidiano *online*, frequentemente compartilhando rotinas, imagens, vídeos e até dados sensíveis dos filhos. Esse uso inconsequente pode transformar as plataformas digitais em veículos de constante exposição, existindo, inclusive, influenciadores mirins que atuam em uma hiperexposição infantil (Santos, Edler, 2022).

As crianças e adolescentes expostos nas redes são especialmente atingidos ao terem suas identidades digitais construídas e gerenciadas por terceiros, sem capacidade de consentimento ou de efeitos futuros dos registros e compartilhamentos permanentes. Nesse cenário que surge o fenômeno denominado *oversharenting*, quando os próprios pais promovem um excesso de compartilhamento das imagens dos filhos. A prática viola os direitos fundamentais ligados à imagem, à privacidade e à autonomia infantil, protegidos tanto constitucionalmente quanto pelo Estatuto da Criança e do Adolescente. A exposição massiva pode criar um “rastro digital” que acompanhará o menor ao longo da sua vida, gerando impactos que vão desde constrangimentos futuros até riscos imediatos relacionados à segurança, à saúde psicológica e à integridade moral, sobretudo quando os menores são utilizados como elementos centrais de *marketing* e engajamento nas redes sociais (Santos, Edler, 2022).

Os influenciadores, inclusive pais, que monetizam as imagens dos próprios filhos e participam desse ecossistema se tornam verdadeiros agentes ativos na manutenção de um mercado que é pautado pela exposição da infância. Influenciadores mirins com milhões de seguidores se expõem diariamente e celebram contratos com marcas, amplificando a exposição. Opera-se uma verdadeira “adultização precoce”, já que o estímulo de desempenho digital e a perda da espontaneidade são características frequentemente apontadas como efeitos diretos da transformação de menores em “produtos midiáticos”. Os algoritmos e modelos de

negócios das plataformas que recompensam o engajamento baseado na imagem infantil apenas pioram o problema (Santos, Edler, 2022).

Deve-se levar em conta que a superexposição amplia os riscos de segurança dos menores, facilitando a atuação de agentes mal-intencionados, a exemplo de sedutores digitais e criminosos que exploram a pornografia infantil, o que aumenta consideravelmente o perigo. Sem prejuízo, o cenário pode favorecer as práticas de violência simbólica, como o *cyberbullying,* fenômeno crescente no Brasil, país que ocupa posição crítica em *rankings* internacionais de agressões virtuais contra crianças e adolescentes. Os ambientes de rede que elevem a visibilidade de influenciadores mirins são verdadeiros espaços de risco não mitigado que reforçam a vulnerabilidade estrutural dos menores (Santos, Edler, 2022).

A responsabilização civil, nessas hipóteses, pode decorrer da violação direta ao direito de imagem do menor, expressamente protegido na Constituição Federal, no Código Civil e no Estatuto da Criança e do Adolescente. Quando existe uma extrapolação, por parte dos pais ou tutores, dos limites do poder familiar e a exposição dos filhos de maneira abusiva, é possível a incidência do instituto da responsabilização civil objetiva, dispensada a análise de culpa, nos termos dos arts. 187 e 927 do Código Civil. Ademais, o dano moral decorrente da exposição indevida nesses casos é presumido, já que a Súmula 403 do STJ[39] reconhece a lesão independentemente de prova do prejuízo, quando a imagem é utilizada para fins econômicos, situação típica de pais que monetizam as rotinas familiares nas redes sociais (Santos, Edler, 2022).

Gize-se, entretanto, que a responsabilização civil não se limita à esfera privada. Considerando que a Constituição Federal declara prioridade absoluta a crianças e adolescentes, o Ministério Público tem a competência, como fiscal da ordem jurídica, para intervir, ajuizar ações civis públicas, fiscalizar condutas e exigir medidas protetivas que limitem a exposição digital de menores. Além disso, o Judiciário pode nomear curador especial na hipótese de existir conflito de interesses entre pais influenciadores e seus filhos, podendo determinar restrições no uso de redes sociais, se entender que a imagem do infante está sendo explorada em desconformidade com os direitos fundamentais. Existe, portanto, um claro vetor de proteção estatal contra práticas de exposição abusiva desenvolvidas nas plataformas

[39] Súmula 403 do STJ: Independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais.

digitais (Santos, Edler, 2022).

A responsabilização civil em casos de exposição indevida de menores nas redes sociais e no contexto digital deve ser compreendida à luz da proteção integral do menor, já que, como sujeito vulnerável, não pode ser tratado como extensão da identidade digital dos pais nem como instrumento de performance social e econômica nas plataformas. O ato de forçar uma construção de identidade digital e estimular dinâmicas de engajamento regidas pela lógica dos influenciadores digitais adultos viola os direitos de personalidade e produz efeitos psicológicos, sociais e jurídicos que atrapalham a infância do indivíduo e geram efeitos por toda uma vida (Santos, Edler, 2022).

Em agosto de 2025, um influenciador chamado Felca publicou na *internet* um vídeo que “denuncia a adultização e a exploração sexual de crianças e adolescentes para criação de conteúdo na *internet*” (Agência Senado, 2025). A repercussão causou a movimentação do Poder Legislativo, sendo aprovado no Senado Federal o PL 2.628/2022, que cria o Estatuto Digital da Criança e do Adolescente, estabelecendo regras para proteger menores em ambientes digitais. A intenção do projeto, que surgiu em razão da preocupação com a adultização de crianças nas redes, é impor obrigações rígidas às plataformas, incluindo a remoção imediata de conteúdos envolvendo abusos ou exploração infantil, verificação de idade, ferramentas de controle parental e vinculação obrigatória de contas de menores de 16 anos a um responsável.

Segundo o PL 2.628/2022, as empresas devem adotar medidas para impedir o acesso de menores a conteúdos prejudiciais, com a remoção rápida e notificação às autoridades em casos graves. Além disso, as plataformas devem oferecer mecanismos de recurso para usuários, relatar semestralmente ações de moderação e implementar configurações padrão no nível máximo de proteção, bloqueando comunicação com adultos não autorizados, limitando funções que incentivem o uso excessivo e restringindo geolocalização (Agência Senado, 2025).

Como penalidades previstas estão advertência, multas de até 10% do faturamento ou 50 milhões de reais por infração, além da suspensão de atividades, aplicáveis conforme gravidade e reincidência. Além disso, foram estabelecidas proibições ao tratamento de dados que violem direitos de menores, ao acesso de crianças a conteúdos impróprios e ao direcionamento de publicidade a esse público, inclusive por análise emocional ou tecnologias imersivas (Agência Senado, 2025).

Os menores, enquanto hipervulneráveis, sem dúvidas constituem um dos grupos mais frágeis na *internet*, merecendo proteção jurídica, sobretudo, preventiva. Apesar dos esforços jurídicos, especialmente legislativos, a ausência de maturidade suficiente para lidar com problemas oriundos do mau uso da *internet,* inclusive com possibilidade de perduração dos efeitos pelo resto da vida, exige uma postura mais ativa do Estado na regulação para que o dano, ao invés de tratado, sequer seja causado.

### 3.4 A proteção jurídica de idosos, grupo de hipervulnerabilidade digital

No caso dos idosos, a maior vulnerabilidade ao ambiente digital revela a necessidade de repensar as bases jurídicas de responsabilização civil das plataformas digitais e, por extensão, dos influenciadores que nela atuam. O envelhecimento populacional está ocorrendo de forma simultânea à migração acelerada de serviços, informações e relações sociais para as redes, expondo o idoso a tecnologias cujo domínio depende de letramento digital específico e acessibilidade adequada (Teixeira, 2025).

No Brasil, a proteção à pessoa idosa é determinada na Constituição Federal, no artigo 230, e reforçada no Estatuto do Idoso (Lei 10.741/2003). Esses dispositivos impõem deveres ao Estado e à sociedade, que devem se comportar no ambiente digital em relação às plataformas e aos influenciadores, agentes privados que estruturam o ambiente virtual, de uma maneira especial. A proteção que deve ser dispensada aos idosos, quando ausentes de medidas preventivas, educativas e informacionais, é incompatível com o dever constitucional de proteção integral da pessoa idosa (Wojahn *et al.,* 2022).

O elemento central para compreender como as plataformas digitais e influenciadores podem ser responsabilizados civilmente por danos gerados a idosos reside na vulnerabilidade informacional, tecnológica e digital. Com a transição abrupta da era analógica para a era digital, foi produzido um grupo social com pouca capacidade de acesso, compreensão e tomada de decisão. Essa é uma situação diferente da geração que já nasceu com a ascensão da *internet*, especialmente a partir da década de 1990 (Almeida, Lemos, 2024).

É justamente nesse aspecto que reside o núcleo da vulnerabilidade, que exige uma resposta jurídica adequada do Estado. O idoso é notoriamente o grupo etário que

menos acessa a *internet*. Entretanto, o uso do espaço virtual pela população idosa tem aumentado exponencialmente, elevando a exposição a práticas econômicas massificadas que regem o ambiente digital. Sem habilidades adequadas e diante da ausência de conhecimento técnico suficiente, os idosos aderem indevidamente à contratação de serviços e realizam interações que são mediadas por grandes grupos econômicos (Almeida, Lemos, 2024).

A maior vulnerabilidade digital da população idosa, sem dúvidas, é elemento central na compreensão da responsabilização civil de agentes que atuam no ambiente virtual, especialmente em relação às plataformas digitais e aos influenciadores. Com o aumento da participação de idosos no universo tecnológico, a assimetria entre a complexidade exigida pela educação digital e as limitações cognitivas se evidencia (Wojahn *et al.,* 2022).

Essa assimetria pode ser derivada de fatores fisiológicos ou da falta de domínio técnico, o que transforma os idosos em alvos hipervulneráveis para golpes cibernéticos. É nesse cenário que a responsabilidade civil de plataformas digitais e influenciadores ganha maior tônica, especialmente à luz da fragilidade estrutural, da previsibilidade do risco e da necessária imputação de responsabilidade (Wojahn *et al.,* 2022).

A maior parte dos crimes digitais praticados contra idosos, a exemplo de estelionatos, falsos empréstimos, engenharia social e solicitações indevidas de dados, ocorre em razão da exploração recorrente da vulnerabilidade, com a utilização de técnicas por parte dos criminosos para manipular decisões, sobrecarregar cognitivamente as vítimas e criar falsas relações de confiança. Essa utilização de modos operandi semelhantes reforça a previsibilidade do risco, que é um critério fundamental na teoria civil da responsabilidade (Wojahn *et al.,* 2022).

A ausência de intimidade do idoso com a tecnologia o transforma em alvo preferencial de golpes, fraudes, desinformação e engenharia social. O cenário revela a necessidade de a responsabilização de plataformas digitais não poder ser analisada exclusivamente à luz de um paradigma de neutralidade tecnológica, já que a insuficiência de mecanismos de segurança, de transparência e de usabilidade contribui diretamente para o dano (Teixeira, 2025).

A maior parte da vulnerabilidade do idoso não decorre somente da sua falta de familiaridade com as ferramentas digitais, mas principalmente da própria arquitetura das plataformas, que não oferece suporte acessível, linguagem simples ou

sistemas de verificação adequados. Pode ser citada como exemplo a utilização do aplicativo do Instituto Nacional do Seguro Social – INSS, responsável por exclusão digital, já que impossibilita milhões de idosos de acessar informações essenciais para evitar fraudes em benefícios previdenciários e assistenciais (Teixeira, 2025).

As plataformas digitais operam com falhas estruturais que ampliam o risco de dano e podem configurar defeito na prestação do serviço, na medida em que a proteção ao consumidor, nessas hipóteses, deve ser analisada sob a perspectiva da dignidade da pessoa idosa. A responsabilização jurídica não deve depender apenas de condutas ativas ilícitas, mas também da omissão em criar ambientes digitais que sejam minimamente seguros e compatíveis com o perfil etário dos usuários (Teixeira, 2025).

Em relação aos influenciadores digitais, a responsabilidade é potencializada pela posição de confiança que ocupam perante a sociedade. Geram vínculos emocionais e uma simulação de familiaridade, e eles próprios são alvos de ofertas de vantagens enganosas. Na aplicação de golpes baseados na reputação do influenciador, especialmente por meio da manipulação psicológica e da criação de relacionamentos artificiais, é possível influenciar a mentalidade do idoso, que fica mais suscetível à promoção de serviços, produtos financeiros ou interações que aumentam o risco (Wojahn *et al.,* 2022).

É também comum a atuação de influenciadores e perfis falsos dentro das plataformas. Perfis falsos que se passam por celebridades podem ser utilizados para aplicar golpes em idosos e induzir a perdas financeiras expressivas, já que os golpistas se aproveitam da credibilidade da celebridade, exploram a confiança e desconhecimento do funcionamento das redes sociais e pedem transferências de valores vultuosos em dinheiro. A proliferação de perfis fraudulentos está ligada, principalmente, à ausência de mecanismos eficazes de verificação, monitoramento e remoção de conteúdos enganosos. Esse *déficit* técnico e operacional pode ser um fundamento para a responsabilização civil das plataformas, especialmente quando a inércia no poder geral de cautela – segurança virtual – contribui para o dano (Teixeira, 2025).

Considera-se, igualmente, a disseminação de desinformação, especialmente as impulsionadas por anúncios pagos, que costuma atingir com maior intensidade a população idosa. No ecossistema Meta (antigo *Facebook*), principalmente, existem milhares de anúncios maliciosos produzidos com o auxílio de inteligência artificial,

direcionados a usuários particularmente vulneráveis. A veiculação desse tipo de conteúdo reforça que as plataformas lucram com a circulação de material enganoso, configurando falha no dever de vigilância e na moderação preventiva. É possível discutir a possibilidade de responsabilização civil nesses casos, diante da presença de benefício econômico e de previsibilidade do risco, além da ausência de filtros adequados que impeçam o impulsionamento do material considerado nocivo (Teixeira, 2025).

O cenário se agrava imensamente quando as decisões tomadas pela população idosa são induzidas por influenciadores que atuam profissionalmente na promoção de produtos e serviços, exercendo um papel relevante na formação da vontade do consumidor. Pelos danos decorrentes dessa indução, é possível extrair fundamentação jurídica para atribuir responsabilidade civil tanto às plataformas que permitem essas práticas, quanto aos próprios influenciadores (Almeida, Lemos, 2024).

Quanto à atuação dos influenciadores, o papel por eles exercido na cadeia de circulação de informações tem o potencial de amplificar a vulnerabilidade de idosos, principalmente quando os conteúdos enganosos, superficiais ou mal verificados são difundidos sem uma mediação crítica. Em razão da suscetibilidade de idosos à desinformação, a golpes e a conteúdos mentirosos travestidos de legitimidade, o conteúdo mediado por figuras públicas ou perfis de grande alcance tem o condão de facilitar a ocorrência de danos, ainda que por negligência, especialmente quando os influenciadores se beneficiam economicamente (Teixeira, 2025).

Especificamente em relação às plataformas digitais, a responsabilização civil deve ser analisada pela ótica do risco estrutural. O ambiente virtual, sem dúvida, favorece a ação de criminosos, porque permite anonimato, facilidade de execução de estratégias ilícitas, baixa probabilidade de punição e desproporcionalidade entre o dano causado e a resposta do Estado (Wojahn *et al.,* 2022).

Se esses espaços digitais não forem estruturados com mecanismos eficientes de proteção dos usuários mais vulneráveis, a exemplo de sistemas de verificação, alertas antifraude, programas de educação digital e ferramentas de denúncia, as plataformas, sem dúvidas, contribuem, ainda que de forma não intencional, para a manutenção do risco. Diante da previsibilidade do risco e da omissão da plataforma, é natural que surja um dever de reparar o dano causado (Wojahn *et al.,* 2022).

Nesse sentido, as plataformas digitais possuem responsabilidade jurídica, a partir do reconhecimento de que essas empresas compõem o núcleo de um novo

modelo econômico que detém base em dados e informação. Por possuírem uma posição privilegiada na cadeia informacional, além do evidente domínio tecnológico, a omissão no dever de prevenção de danos e na adoção de mecanismos de segurança deve ser encarada como juridicamente relevante quando afetar grupos vulneráveis. Supondo que o idoso não consiga compreender os riscos digitais, golpes, técnicas de persuasão algorítmica ou o sistema de coleta de dados, é crucial a implementação de mecanismos compatíveis para combater essa vulnerabilidade. É possível entender que a responsabilização jurídica emerge quando existe uma falha na promoção de um ambiente digital seguro (Almeida, Lemos, 2024).

No caso dos influenciadores, a responsabilização civil decorre do papel ativo que desempenham na indução comportamental dos usuários. Idosos costumam aderir a práticas contratuais e comerciais justamente por não dispor do domínio técnico necessário para compreender a dinâmica deste tipo de ambiente. Os influenciadores, quando operam no ambiente digital como agentes que estimulam o consumo, podem explorar, mesmo que de forma involuntária, essa vulnerabilidade, produzindo prejuízos econômicos significativos (Almeida, Lemos, 2024).

Portanto, quando a atuação de um influenciador contribui para a tomada de decisões prejudiciais por parte das pessoas com vulnerabilidade agravada, a conduta pode ser enquadrada como causa do dano, emergindo a responsabilidade civil subjetiva ou mesmo objetiva, dependendo do regime jurídico aplicado, a exemplo da relação regida pelo direito do consumidor. Sem dúvidas, o idoso, ao ser excluído da plena participação digital, deixa de ter acesso à informação e, consequentemente, aos mecanismos de proteção dos seus próprios direitos (Almeida, Lemos, 2024).

Os impactos gerados na pessoa idosa, como perdas financeiras, abalos emocionais, ansiedade, depressão e isolamento social demonstram que a vulnerabilidade digital não é apenas tecnológica, mas profundamente humana, questão relevante para a responsabilização civil, já que danos podem ultrapassar o patrimônio e atingir direitos de personalidade existenciais que são protegidos pelo ordenamento jurídico. Auferir lucro com a exploração da audiência de público etariamente vulnerável tem como decorrência lógica a assunção dos deveres de cuidado e do risco gerado, sob pena de responsabilização civil pela violação de direito (Teixeira, 2025).

Os intermediários digitais devem adotar postura ativa na promoção de ambientes informacionais que sejam compreensíveis e seguros. Esse dever decorre,

sobretudo, do art. 19 do Marco Civil da Internet, especialmente depois da reinterpretação, recentemente, que foi promovida pelo Supremo Tribunal Federal. Quando plataformas digitais e influenciadores participam de atividade que, de forma direta ou indireta, restringe o acesso seguro à informação, a responsabilidade civil se justifica com o objetivo normativo de proteção da dignidade da pessoa idosa (Almeida, Lemos, 2024).

Sem dúvidas, o maior desafio é a insuficiência legislativa e a ausência de políticas estatais adequadas aos danos experimentados pelos idosos. Nesse sentido avançou bem o Supremo Tribunal Federal, ao trazer nova interpretação ao artigo 19 do Marco Civil da *Internet*, medida que, aliada a iniciativas de orientação ao idoso, pode ser capaz de mitigar os danos causados (Wojahn *et al.,* 2022).

Registra-se que os danos às pessoas idosas, nesses casos em que são vítimas de golpes digitais, não são apenas patrimoniais, mas também psicológicos, decorrentes de manipulação emocional, perda de autonomia e abalo à dignidade. Estudos sobre violência psicológica contra idosos reforçam a necessidade de considerar as plataformas e os influenciadores como parte da cadeia causal de comunicação e comportamento digital, devendo existir uma responsabilização jurídica como resposta aos danos causados (Wojahn *et al.,* 2022).

Em conclusão, é possível pensar que a inclusão digital se tornou verdadeiro direito humano, já que a omissão das plataformas e influenciadores na mitigação dos riscos digitais representa, além de falha técnica, uma violação estrutural de direito fundamental contemporâneo. Com isso, a tecnologia se tornou uma condição para o exercício pleno da cidadania (Almeida, Lemos, 2024).

Sem dúvidas, o idoso que venha a sofrer prejuízo por práticas abusivas ou por ausência de mecanismo de proteção deve ter o direito de acionar tanto as plataformas quanto os influenciadores responsáveis. A responsabilidade civil, nesses casos, ultrapassa a mera compensação individual do dano, exercendo uma verdadeira função de equalização estrutural das desigualdades tecnológicas.

## 3.5 A responsabilização criminal

### 3.5.1 Os crimes contra a honra praticados na *internet*

É bem sabido que o Código Penal prevê, nos artigos 138, 139 e 140, respectivamente, os crimes de calúnia, difamação e injúria, que podem ser praticados contra a honra objetiva ou subjetiva de alguém[40].

Sem dúvidas, esses delitos revelam-se especialmente facilitados, tanto na prática quanto na difusão, quando analisados sob a ótica do ambiente virtual. Seja porque aquela pessoa que comete o delito se sente mais segura de fazê-lo por estar protegida por uma tela de um aparelho eletrônico, seja em razão da rápida e ampla disseminação de informações.

Especificamente em relação ao artigo 138 do Código Penal[41], existe a punição de caluniar alguém, imputando-lhe falsamente fato definido como crime, com pena de detenção de seis meses a dois anos e multa. Esse delito ofende objetivamente a honra da pessoa lesada e ocorre quando o sujeito ativo leva ao conhecimento de terceiros uma suposta infração penal, que sabe nunca ter acontecido, supostamente praticada pelo sujeito passivo (vítima).

Segundo ainda o artigo 138, parágrafo terceiro[42], do Código Penal, trata-se do único crime que admite a prova da verdade, ou seja, a chamada exceção da verdade, podendo o sujeito ativo provar, se chamado em procedimento investigativo ou em juízo, que, na verdade, aquele delito ocorreu.

O artigo 139 do Código Penal também tutela a ofensa à honra objetiva de alguém, prevendo a conduta de difamar o sujeito passivo (vítima), imputando-lhe fato ofensivo à sua reputação. A pena é prevista de detenção de três meses a um ano e multa. A distinção é relevante, porquanto no crime de calúnia o sujeito ativo imputa a terceiro um crime que nunca ocorreu; já no crime de difamação, imputa-se um fato ofensivo à reputação que, entretanto, não é previsto como crime, como, por exemplo, ter traído algum cônjuge ou estar se prostituindo. A exceção da verdade só é admitida

---

[40] "É, em outros termos, o sentimento do outro que incide sobre as nossas qualidades ou nossos atributos, ou seja, enquanto a *honra subjetiva* representa o sentimento ou a concepção que temos a nosso respeito, a *honra objetiva* constitui o sentimento ou o conceito que os demais membros da comunidade têm sobre nós, sobre nossos atributos. Objetivamente, *honra* é um valor ideal, a consideração, a reputação, a boa fama de que gozamos perante a sociedade em que vivemos" (Bitencourt, 2018a, p. 304).

[41] "Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
Pena - detenção, de seis meses a dois anos, e multa.
§ 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga".

[42] "§ 3º - Admite-se a prova da verdade, salvo:
I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;
II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;
III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível".

se o ofendido for funcionário público e a ofensa for relativa ao exercício das funções, conforme o artigo 139, parágrafo único, do Código Penal[43].

Enquanto os artigos 138 e 139 do Código Penal tutelam a honra objetiva, ou seja, a percepção que a sociedade ou um grupo de pessoas têm sobre o sujeito passivo ou a vítima, por outro lado, o artigo 140, que trata do crime de injúria, tutela a honra subjetiva, justamente porque a conduta ocorre quando o sujeito ativo injuria ou ofende diretamente a dignidade ou o decoro diretamente ao sujeito passivo.

Diferentemente da calúnia e da difamação, que o sujeito ativo conta a terceiros o suposto crime que nunca ocorreu ou um ato ofensivo à reputação do ofendido, na injúria a ofensa é proferida de forma direta, ou seja, sem intermediações entre sujeito ativo e sujeito passivo. A pena é de detenção de um a seis meses ou multa, podendo o juiz deixar de aplicar a pena quando o ofendido, de forma reprovável, provocou diretamente a injúria, ou no caso de retorsão imediata que consista em outra injúria, nos termos do artigo 140, parágrafo primeiro, do Código Penal[44].

Curiosamente, em relação ao ambiente virtual, o artigo 141 do Código Penal prevê que as penas se aumentam em um terço quando um dos crimes é cometido, nos termos do parágrafo segundo do mesmo artigo, ou divulgado em quaisquer modalidades das redes sociais, da rede mundial de computadores. Na verdade, segundo o artigo 141, parágrafo segundo, se o crime for cometido ou divulgado em quaisquer modalidades das redes sociais, da rede mundial de computadores, aplica-se o triplo da pena, conforme alterações da Lei 13.964 de 2019.

Percebe-se que a Lei 13.964/2019 buscou tutelar a ocorrência dos crimes contra a honra em redes sociais ou na rede mundial de computadores, considerando a maior capacidade de propagação ou de reprodução, já que um crime de calúnia ou um crime de difamação cometidos na *internet* atingem um número indeterminado de pessoas, com possibilidade de viralizar o conteúdo indevido, e o crime de injúria expõe aquela ofensa praticada diretamente a diversas pessoas que acompanhem a publicação ou as mensagens proferidas.

---

[43] “Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
Pena - detenção, de três meses a um ano, e multa.
Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções”.

[44] “Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
Pena - detenção, de um a seis meses, ou multa.
§ 1º - O juiz pode deixar de aplicar a pena:
I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;
II - no caso de retorsão imediata, que consista em outra injúria”.

### 3.5.2 Influenciadores digitais e a divulgação de jogos de azar

Define-se como jogo de azar qualquer atividade lúdica em que o resultado é determinado única e exclusivamente pela sorte, de forma que não é importante a habilidade do jogador. É comum que os jogadores apostem dinheiro e outros bens de valor para participar, sendo o resultado, que depende exclusivamente do acaso, completamente incerto (Marçal, 2023).

Não obstante existam registros de jogos de azar desde a antiguidade (China e Egito, 3000 a.C.), passando por diferentes períodos históricos como a Idade Média até a Idade Moderna, no Brasil, os jogos de azar eram comuns no período colonial, tanto para a elite portuguesa quanto para colonos abastados. Os jogos eram realizados especialmente no Rio de Janeiro e em Salvador. Eram tratados pela liderança religiosa, entretanto, como uma ameaça à moralidade e à ética da sociedade, como se pudessem causar a ruína financeira e espiritual dos envolvidos[45].

A Proclamação da República e o fim do absolutismo monárquico levaram ao período, no Brasil, conhecido como a “Era de Ouro dos Cassinos”, entre os anos de 1920 e 1930, diante da inexistência de regulamentação específica acerca dos jogos de azar (Marçal, 2023).

Com a promulgação do Código Penal da República, a prática de jogos de azar passou a ser designada como contravenção penal, situação que persiste, até hoje, na atual Lei de Contravenções Penais (art. 50), não obstante a existência de autorizações para loterias, apostas em corridas de cavalos e comercialização de apostas esportivas de quota fixa, nos termos da Lei 13.756/2018 e do Decreto-Lei 6.259/1944.

Além disso, existe uma determinação de que parte da receita gerada por apostas seja direcionada para investimentos em esportes, segurança pública, cultura e saúde, não obstante a ausência de clareza na regulamentação, já que as leis brasileiras proíbem jogos de azar, mas, ao mesmo tempo, traz algumas exceções sem

[45] “Com a independência do Brasil em 1822, e o consequente rompimento entre Brasil e Portugal, o ordenamento jurídico brasileiro passou a ter o próprio Código Criminal, criado em 1830 para substituir as Ordenações Reais. À medida que os jogos de azar foram evoluindo junto com a sociedade, os governantes visualizaram a necessidade de regulamentar a prática dos mesmos, de modo que a sua proibição passou a ser uma questão política e social cada vez mais importante. Assim, em atendimento aos pedidos da Igreja Católica e líderes da política que argumentavam que as jogatinas eram imorais e desviavam as pessoas de suas obrigações e deveres, foi incluído no Código Criminal de 1830, pelo imperador Pedro I, penalidade para quem praticava jogos de azar e para o funcionário público que estivesse envolvido em jogos de azar” (Marçal, 2023, p.12).

regulamentação precisa[46].

Apesar da polêmica acerca da regulamentação dos jogos de azar no Brasil, salta aos olhos que o Ministério Público tem investigado ativamente influenciadores digitais que recebem patrocínio ou dinheiro contratual para divulgar plataformas de jogos de azar aos seus seguidores, utilizando as redes sociais e as métricas algorítmicas de engajamento.

Nesse sentido, podem ser citadas: Operação *Game Over,* nos Estados de São Paulo e Alagoas (Terra, 2024); Operação Truque de Mestre, nos Estados do Pará e Pernambuco (G1, 2024); Operação *Smurfing*, no Estado de Minas Gerais (O Tempo, 2024); e Operação *Ludus*, no Estado de São Paulo (Band Vale, 2024).

Em todas as operações, o Ministério Público, em parceria com as polícias, movimentou o aparato estatal para que a Justiça Penal pudesse tutelar a conduta de divulgação de jogos de azar virtuais, conduta não regulamentada para os influenciadores digitais, especialmente porque os vídeos divulgados são produzidos com “contas de demonstração”, que mostram ganhos relevantes e impossíveis, já que o produto (algoritmo) fornecido aos seguidores é totalmente diferente do produto (algoritmo) utilizado pelo influenciador digital na gravação (Uol, 2024).

Feito este introito, consigna-se que existem no ordenamento jurídico brasileiro algumas leis que preveem crimes que estão sendo utilizados no enquadramento penal dos influenciadores digitais, na divulgação de jogos de azar. Obviamente, o dispositivo que salta aos olhos reside no art. 50 da Lei de Contravenções Penais[47], que proíbe o estabelecimento e a exploração de jogos de azar em local público ou inacessível ao público, com pena de prisão simples de três meses a um ano, além de multa e possível perda de bens. Além disso, existe a possibilidade de causa de aumento de um terço (empregados ou participantes da casa de exploração de jogos de azar menor de 18 anos).

Segundo o próprio artigo de Lei (art. 50, § 3º, LCP), são jogos de azar: a) o

---

[46] “Cumpre ressaltar, no entanto, que os efeitos legais da Lei n.º 13.756/2018 estão à espera de regulamentação por parte do Poder Executivo Federal, visando a emissão de licenças que permitam a realização desta atividade. É notório que a ausência de normatização gera questionamentos sobre a sua legalidade no mercado brasileiro, além disso, diante do vácuo regulatório e da omissão legislativa, empresas envolvidas nesta atividade têm optado por estabelecer suas operações fora do território nacional, com o intuito de evitar o enquadramento nos termos do artigo 50 do Decreto-Lei n.º 3.688/41, a supracitada Lei de Contravenções Penais [...]” (Soares, 2024).

[47] “Art. 50. Estabelecer ou explorar jogo de azar em lugar público ou acessível ao público, mediante o pagamento de entrada ou sem ele: Pena – prisão simples, de três meses a um ano, e multa, de dois a quinze contos de réis, estendendo-se os efeitos da condenação à perda dos moveis e objetos de decoração do local”.

jogo em que o ganho e a perda dependem exclusiva ou principalmente da sorte; b) as apostas sobre corrida de cavalos fora de hipódromo ou de local onde sejam autorizadas; c) as apostas sobre qualquer outra competição esportiva.

Como amplamente sabido, a configuração do crime exige uma concepção tripartite, já que exige fato típico, ilícito e culpável. A tipicidade, especificamente, divide-se em tipicidade subjetiva (aferição do elemento volitivo, dolo ou culpa, quando cabível, segundo a Teoria Finalista de *Hanz Welzel*) e a tipicidade objetiva[48].

A tipicidade objetiva repousa no art. 1º do Código Penal Brasileiro, consagrando princípio basilar, conforme um dos dez axiomas garantistas de Luigi Ferrajoli (2014): *nullum crimen sine lege*. Segundo o art. 1º do Código Penal, não há crime sem lei anterior que o defina nem pena sem prévia cominação legal. Significa dizer que alguém só pode ser punido por um crime se a conduta estiver objetivamente prevista no ordenamento jurídico como ilícito penal.

Portanto, é possível argumentar que a conduta de divulgação, por influenciadores digitais, de plataformas virtuais de jogos de azar poderia ser enquadrada no art. 50 da LCP, já que haveria proibição expressa e adequação aos núcleos verbais do tipo penal normativo.

Na verdade, o influenciador digital não estaria estabelecendo ou explorando jogo de azar, mas atuando como intermediador direto mediante remuneração, através de propaganda. Rememore-se que o princípio da legalidade, característico do direito penal, exige que a conduta praticada esteja plenamente amalgamada ao tipo, sob pena de não estar configurada a tipicidade objetiva. Em situação distinta, ou seja, quando a conduta humana (ação ou omissão) não corresponde ao modelo legal, ou quando não existe uma exata coincidência entre o comportamento humano e a norma penal incriminadora, a violação jurídica deve ser resolvida por outro ramo que não seja o direito penal (Queiroz, 2012).

Os núcleos verbais previstos no art. 50 da Lei nº. 3.688/1941 revelam que são condutas típicas o ato de estabelecer, organizar, instituir, criar ou fundar um local físico onde se pratique o jogo, e explorar – auferir lucro com o jogo fora da condição de apostador – direta ou indiretamente jogos de azar, dependentes da sorte, sendo

[48] “Tipicidade é a conformidade do fato praticado pelo agente com a moldura abstratamente descrita na lei penal. Tipicidade é a correspondência entre o fato praticado pelo agente e a descrição de cada espécie de infração contida na lei penal incriminadora. Um fato para ser adjetivado de típico precisa adequar-se a um modelo descrito na lei penal, isto é, a conduta praticada pelo agente deve subsumir-se na moldura descrita na lei” (Bitencourt, 2018b, p. 506).

sujeito passivo a coletividade (Gonçalves, 2017).

Ato contínuo, parte da doutrina trata o estabelecimento ou a exploração de jogos de azar como crime que busca tutelar os bons costumes, sendo o Estado o sujeito passivo. Trata-se de um conceito elástico, variável com a evolução da própria sociedade, em relação “às condutas virtuosas que se estabelecem por força de hábito e uso continuado, tendo para a sociedade caráter de obrigatoriedade do ponto de vista moral” (Oliveira Neto, 1994).

Portanto, na situação atual, depreende-se que existe uma lacuna normativa na Lei de Contravenções Penais em relação à divulgação, por influenciadores digitais, de plataformas virtuais de jogos de azar, considerando que não são realizadas apostas em estabelecimentos físicos, assim como que os *websites* são hospedados em países estrangeiros.

No que diz respeito às apostas online, ao contrário do cenário físico, devido à falta de amparo legal, o usuário não se encontra diante uma conduta ilícita. A explicação para isso reside no fato de que as plataformas de apostas esportivas têm sua sede em outros países, o que permite que os apostadores acessem quaisquer plataformas de apostas pela rede mundial de computadores sem que isso resulte no enquadramento na Lei de Contravenções Penais.

Nesta lógica, ainda que o Código Penal estabeleça que a prática de crimes ocorridos no exterior esteja sujeita à legislação penal brasileira, esta possibilidade não se aplica às contravenções penais porque, conforme observa Masson (2021), não é admitida a aplicação da lei penal brasileira no que refere às contravenções penais praticadas em território estrangeiro, nos termos do art. 2º da Lei de Contravenções Penais: “A lei brasileira só é aplicável à contravenção praticada no território nacional”.

Tendo em vista a limitação deste dispositivo, cuja incidência é restrita ao território nacional, para lidar com esse fenômeno, é imperativo ressaltar que cabe ao Poder Legislativo a incumbência de acompanhar as transformações que permeiam a sociedade contemporânea, a fim de regulamentar, de maneira precisa e sem margem para ambiguidades, os conflitos emergentes (Soares, 2024).

Conclui-se que sequer existe a possibilidade de aplicação da lei penal brasileira nesses casos, já que a Lei de Contravenções Penais não admite a regra geral, aplicada para delitos de maior potencial ofensivo, de aplicação da lei penal brasileira para crimes ocorridos no exterior. Assim, considerando as diversas operações policiais e procedimentos conduzidos pelo Ministério Público no país, o

problema, quando confrontado com a legislação penal brasileira, admite dois caminhos para enquadramento e tutela penais.

O primeiro caminho seria a investigação e punição de crimes associados, como lavagem de dinheiro e organização criminosa, esbarrando no delicado contexto de necessidade de comprovação da ilicitude do dinheiro originariamente obtido com a tentativa de escamoteamento de sua natureza, ou de composição estruturada e hierárquica de um grupo de pessoas com a finalidade específica de prática de delitos.

Além disso, existe a possibilidade da prática de um crime contra a ordem tributária, a exemplo de sonegação fiscal, caso todo o dinheiro obtido não seja declarado à Receita Federal com o recolhimento dos impostos incidentes.

O segundo caminho seria enquadrar a divulgação de casas de apostas virtuais por influenciadores digitais como relação de consumo, existindo o fornecimento de um produto defeituoso em sua gênese, configurando a prática de crimes específicos contra o consumidor previstos na Lei 8.078/1990, ou como estelionato, nos termos do art. 171 do Código Penal Brasileiro.

O Código de Defesa do Consumidor estabelece, no art. 3º, que se enquadra como fornecedor de produtos a pessoa física que distribui ou comercializa produtos. Os influenciadores digitais, ao divulgarem plataformas virtuais de jogos de azar pertencentes a terceiros, expõem ao mercado e aos consumidores em geral a disponibilidade de produtos.

O Código de Defesa do Consumidor também prevê a existência de infrações penais específicas da relação de consumo: fazer afirmação falsa ou enganosa, ou omitir informação relevante sobre a natureza, característica, qualidade, quantidade e segurança de produto (art. 66); fazer ou promover publicidade que sabe ou deveria saber ser enganosa ou abusiva (art. 67); fazer ou promover publicidade que seja capaz de induzir o consumidor a se comportar de forma prejudicial à sua saúde ou segurança (art. 68).

Como visto, a maioria das divulgações de influenciadores digitais sobre as plataformas virtuais de jogos de azar são realizadas com a gravação de vídeos que mostram ganhos expressivos em uma conta de demonstração, disponibilizada pelo proprietário do *website* de apostas apenas para que o *influencer* grave seu vídeo mostrando ganhos financeiros extremamente relevantes.

A partir do momento em que é divulgado um vídeo, entretanto, disponibilizado um produto completamente distinto aos consumidores em que existe a impossibilidade

de ganhar dinheiro ou, em alguns casos, até de sacar qualquer valor obtido, ter-se-ia, em tese, a disponibilização ao mercado de produto defeituoso através de propaganda enganosa.

Existe, igualmente, a possibilidade de enquadramento da conduta do influenciador digital na conduta de estelionato prevista no art. 171 do Código Penal Brasileiro, na medida em que o *influencer* obteria vantagem ilícita (dinheiro pago pelo dono do *website*) para induzir ou manter terceiros a erro, utilizando-se de artifício, ardil ou qualquer outro meio fraudulento.

Assim, percebe-se que o fenômeno recente, popularizado com o avanço das relações interpessoais na *Internet*, revela um desafio à justiça na tipificação, na investigação e na punição da conduta em comento, diante da inexistência de tipo penal específico, sendo necessário realizar uma adequação fático-normativa a outros tipos penais previstos no ordenamento jurídico, como crimes contra as relações de consumo ou o crime de estelionato. O ordenamento jurídico precisa se adaptar às mudanças para tutelar os direitos fundamentais lesados.

A forma do direito penal de lidar com a situação da divulgação, por influenciadores digitais, de plataformas virtuais de jogos de azar, parece deficiente no tocante à normatização, sendo necessária uma atualização legislativa ou, atualmente, uma interpretação mais elástica acerca do conceito de tipicidade objetiva para enquadrar as condutas em crimes já existentes no ordenamento jurídico.

### 3.5.3 Os *Deepfakes*

Como visto, a inteligência artificial atualmente é capaz de processar um grande volume de informações e de interagir de forma praticamente senciente, de forma apta a simular a consciência humana e a criar conteúdo em forma de imagens e vídeos de praticamente qualquer objeto ou ser vivo. Inclusive, as inteligências artificiais modernas conseguem criar vídeos a partir de imagens pré-existentes que são fornecidas pelo usuário, sendo capazes de alterar conteúdo de fala, simular a voz ou até transmutar a face da pessoa para o corpo de outra pessoa.

Esses vídeos falsos, denominados *deepfakes*, são, na verdade, identidades falsas que são criadas com o sistema de *deep learning*, ou aprendizagem profunda, de maneira que a imagem humana é sintetizada pela inteligência artificial e usada para combinar e sobrepor imagens, transformando-as em novos vídeos que não

ocorreram na realidade[49]. A inteligência artificial, dessa forma, é capaz de praticamente conjurar pessoas que não existem na realidade, ou de utilizar imagens de pessoas que existem e colocá-las em situações que não foram filmadas em um momento que tenha ocorrido de verdade.

Nesse sentido, diversos *deepfakes* já tiveram ampla disseminação e repercussão, inclusive a nível mundial, envolvendo pessoas famosas. Tais vídeos foram criados com a intenção de ludibriar as pessoas, especialmente em relação a falas ou ações que nunca ocorreram de verdade. Já foram vítimas de *deepfakes* personalidades mundiais como Barack Obama, ex-presidente dos Estados Unidos da América, Volodymyr Zelensky, presidente da Ucrânia, e até Mark Zuckerberg, criador do Facebook (CanalTech, 2022).

Outros exemplos mundiais de *deepfake* podem ser citados. O jornal parisiense *Le Monde*, por exemplo, já publicou uma matéria em maio de 2024 sobre a maneira que os *deepfakes* estão impactando severamente as eleições presidenciais na Índia (LeMonde, 2024). Em 2021, por outro lado, uma mulher chamada "Jodie" (nome fictício), foi vítima de *deepfake* porque um vídeo que continha seu rosto no corpo de outra mulher que estava em ato sexual com vários homens ao mesmo tempo. Em razão desse *deepfake* e das informações digitais inverídicas, foram causados severos abalos psicológicos à vítima (BBC News, 2024). Kate Isaacs, mulher que se intitula ativista contra o pornô de vingança, foi alvo de *deepfake* com um vídeo pornográfico quando seu rosto foi inserido digitalmente no corpo de outra mulher (G1, 2022). Até a primeira-ministra italiana, Giorgia Meloni, também foi alvo de *deepfake* pornográfico, chegando a pedir na justiça 100 mil euros em um processo aberto contra dois homens que supostamente sobrepuseram seu rosto em corpos de mulheres que atuaram em vídeos pornográficos (CNN, 2024).

O perigo do *deepfake* ocorre, portanto, no grau de verossimilhança, porque as vozes e imagens geradas com a inteligência artificial nos vídeos são hoje tão próximas da realidade que podem ludibriar um imenso número de pessoas com

[49] “Deepfakes são, essencialmente, identidades falsas criadas com o *Deep Learning* [aprendizagem profunda, por meio de uso maciço de dados], por meio de uma técnica de síntese de imagem humana baseada na inteligência artificial. É usada para combinar e sobrepor imagens e vídeos preexistentes e transformá-los em imagens ou vídeos ‘originais’ [...] Essa combinação de vídeos existentes e ‘originais’ resulta em vídeos falsos, que mostram uma ou algumas pessoas realizando ações ou fazendo coisas que nunca aconteceram na realidade. Em 2019, também estamos vendo uma explosão de faces fake, através das quais a IA é capaz de conjurar pessoas que não existem na realidade, e que têm um certo fator de fluência” (Spencer, 2019).

assuntos de grande seriedade ou relevância. A questão adquire expressiva tônica no ambiente da internet devido à possibilidade de propagação de informações, como já visto.

Dessa forma, os algoritmos de inteligência artificial, que estão avançando de forma vertiginosa, podem a cada dia gerar conteúdo ainda mais realista, aplicando-se a autocorreção, sem a necessidade de intervenção humana, para a melhoria gráfica dos vídeos e fotos gerados e melhorias dos áudios. Os algoritmos que criam *deepfakes* possuem um aprendizado profundo e são capazes de analisar e prever automaticamente diversos erros. As máquinas conseguem utilizar o conhecimento e a linguagem de forma muito próxima à realizada pelo ser humano[50].

Existe, portanto, um risco duplo na verossimilhança do *deepfake*. Por um lado, o potencial de desinformação é imenso, e por outro lado, há uma clara violação ao direito de imagem da pessoa que teve sua fala, expressões faciais ou suas ações modificadas em um vídeo ou foto que não correspondem à realidade e que foi compartilhado a esmo na *internet*.

A criação de *deepfake* já é uma realidade acessível à maioria das pessoas diante do avanço e da popularização da inteligência artificial, sem a necessidade de que exista conhecimento ou habilidade específica. A prática viola diversos direitos tutelados pela Constituição Federal Brasileira de 1988, especificamente no artigo 5º, inciso X, especialmente a honra e a imagem das pessoas, sendo a honra de caráter subjetivo e ligada ao valor moral do sujeito, e a imagem abordada em uma dupla acepção: a imagem-retrato, que é o direito à reprodução gráfica da imagem do sujeito, e a imagem-atributo, que é a imagem do sujeito no contexto do meio social[51].

---

[50] "Já é sabido que o algoritmo de criação dos *deepfakes* possui um aprendizado profundo que analisa e prevê automaticamente, corrigindo prováveis erros. Tem-se a inteligência artificial produzindo máquinas capazes de utilizar o conhecimento e a linguagem de uma forma bem próxima da que o ser humano realiza. A inteligência artificial caminha cada vez mais rápido, permitindo que a ciências da computação crie suas máquinas com capacidade de inteligência cada vez mais próxima à realidade do homem. Da mesma forma que os seres humanos utilizam a cognição e a linguagem para evoluir e comunicar, a inteligência artificial busca através de seus algoritmos que as funções cognitivas e comunicativas humanas, sejam reproduzidas pelos programas virtuais" (Lessa, Moyana Mariano Robles; Cabral, Hildeliza Lacerda Tinoco Boechat; Silvestre, Gilberto Fachetti, 2020, pp. 475-487).

[51] "Toda nova informação sobre a pessoa importa uma alteração do seu espaço de intimidade. *Prima facie*, assim, as atividades que levassem a modificações do conceito social de alguém estariam violando sua intimidade, porquanto não consentida. Há algo mais, porém. Sob o direito à honra, dá-se mais do que simples manipulação de um determinado dado pessoal, pois se acrescenta a intenção dirigida à sua depreciação, à sua desvalorização, que pode ser inexata, confundindo-se, certa medida, com a identidade; mas dela se diferençando, pois pode ser verdadeira; pode dizer respeito a aspectos particulares, privados, confluindo com as águas da intimidade" (Canotilho, 2018, p. 579).

Portanto, o problema do *deepfake* pornográfico engloba direitos de ordem constitucional que gozam do *status* de garantias fundamentais. Não existindo no ordenamento jurídico brasileiro, atualmente, uma figura típico-normativa específica para punir, com a utilização do direito penal, o *deepfake* de conteúdo pornográfico cometido contra vítima do sexo feminino.

A conduta pode, por exemplo, ser enquadrada como violência psicológica contra a mulher, prevista no artigo 147-B do Código Penal[52], inserido em 28 de julho de 2021 pela Lei 14.188/2021. Apesar de não ser totalmente atípica a conduta da criação do *deepfake*, existe a possibilidade de enquadramento do núcleo verbal fático no tipo penal normativo, sendo aplicada a pena de reclusão de somente seis meses a dois anos, se não constituir crime mais grave. Saliente-se que o delito não necessariamente é cometido no contexto da Lei 11.340/2006 (Lei Maria da Penha), já que a criação de *deepfake* não pressupõe a existência de uma convivência doméstica ou familiar contra a mulher ou uma situação de vulnerabilidade.

Ademais, não existe impedimento para que casos previstos no artigo 147-B do Código Penal viabilizem a suspensão condicional do processo, uma vez atendidos os requisitos do artigo 89 da Lei 9.099/1995, ou a transação penal prevista no artigo 76 da mesma verba legislativa. E, uma vez aplicada a pena privativa de liberdade, pode ser realizada a substituição por pena restritiva de direitos, nos termos do artigo 44 do Código Penal, por se tratar de pena não superior a quatro anos e de crime que não é cometido com violência ou grave ameaça à pessoa, desde que não haja reincidência, e o condenado possua culpabilidade, antecedentes, conduta social e personalidade favoráveis em caráter subjetivo. O cumprimento da pena, ato contínuo, ocorreria em regime aberto, a teor do artigo 33, parágrafo 1º, alínea “c”, do Código Penal Brasileiro.

Percebe-se, portanto, que existe uma insuficiência na tutela penal[53] da

---

[52] “Art. 147-B. Causar dano emocional à mulher que a prejudique e perturbe seu pleno desenvolvimento ou que vise a degradar ou a controlar suas ações, comportamentos, crenças e decisões, mediante ameaça, constrangimento, humilhação, manipulação, isolamento, chantagem, ridicularização, limitação do direito de ir e vir ou qualquer outro meio que cause prejuízo à sua saúde psicológica e autodeterminação:
Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave”.

[53] “Pode-se falar, em resumo, que a necessidade de legislação a respeito da IA se relaciona intrinsecamente com a noção de garantia da segurança jurídica e digital, a minimização dos riscos a todos os envolvidos, a exigência de transparência, ética e respeito aos direitos humanos e fundamentais” (Melo Júnior, José Eustáquio de; Oliveira, Gustavo Paschoal Teixeira de Castro, 2023, pp. 99-114).

conduta de criar *Deepfake,* especialmente o pornográfico, o que motivou tanto a Câmara dos Deputados quanto o Senado Federal a tramitarem projetos de lei que tipifiquem a conduta criminalmente.

### 3.5.4 Outros temas pertinentes sobre o direito penal e o uso da *internet*

Não obstante tenham sido trazidos, no entender do autor deste trabalho, os principais pontos que envolvem o direito penal e a utilização do ambiente virtual da *internet*, existem outros pontos jurídicos que merecem menção.

De início, a Lei 12.737/2012 inseriu no Código Penal a tipificação criminal dos delitos informáticos, especificamente os arts. 154-A e 154-B. Foi definida como crime a conduta de invasão de dispositivo informático conectado ou não à rede, através de violação indevida de mecanismos de segurança. O agente invasor deve ter o objetivo de obter, adulterar ou destruir dados e informações sem autorização do titular, ou instalar vulnerabilidades para obtenção de vantagem ilícita.

A mesma lei prevê a punição para quem produz, oferece ou distribui dispositivos e programas de computador que tenham o objetivo de permitir as referidas invasões. Também foi alterado o art. 266 do Código Penal para criminalizar a interrupção ou perturbação de serviços telemáticos ou de informação de utilidade pública, com pena aplicada em dobro se o crime ocorrer em ocasiões de calamidade pública.

Já a Lei 14.132/2021 instituiu o crime de perseguição, inserindo o art. 147-A no Código Penal e revogando a contravenção penal de perturbação da tranquilidade. Em suma, é punida a conduta de perseguir alguém, de forma reiterada e por qualquer meio (inclusive no ambiente virtual), ameaçando a integridade física ou psicológica da vítima ou invadindo a liberdade ou privacidade.

A referida lei prevê causas de aumento de pena, com elevação à metade se o crime for cometido contra crianças, adolescentes, idosos ou contra mulheres em razão da condição do sexo feminino. É imprescindível a representação da vítima e as penas devem ser aplicadas sem prejuízo das correspondentes a eventuais atos de violência praticados durante a perseguição.

A Lei 14.811/2024 também merece menção, já que trouxe medidas rigorosas para a proteção da criança e do adolescente contra a violência praticada no ambiente digital. O marco fundamental foi a alteração do Código Penal para agravar as punições

de crimes cometidos nas redes virtuais, como induzimento, instigação ou auxílio ao suicídio ou à automutilação, com pena aplicada em dobro se o autor for líder ou administrador de grupo ou rede virtual.

A lei mencionada também estabeleceu a Política Nacional de Prevenção e Combate ao Abuso e Exploração Sexual da Criança e do Adolescente, com o objetivo de fortalecer as redes de proteção e a produção de conhecimento sobre o tema, impondo obrigações às instituições que trabalham com menores e exigindo a manutenção de certidões de antecedentes criminais atualizados de todos os colaboradores.

Além das leis acima, está em trâmite no Senado Federal o Projeto de Lei 4161/2020, com o objetivo de alterar o Código Penal para aumentar em dois terços a pena de estelionato e fraude no comércio cometidos na *internet*. Com o intento de endurecer as regras já vigentes para ampliar a proteção do consumidor e reduzir a incidência de delitos, o Legislativo volta os olhos para o aumento expressivo de crimes de estelionato por meio eletrônico, que conta com crescimento de 17% em 2024, segundo o Anuário Brasileiro de Segurança Pública (Radio Senado, 2025).

Percebe-se, portanto, um esforço legiferante para acompanhar as alterações da realidade. Práticas comuns podem ser citadas, como: *phishing*, uso de comunicações aparentemente fidedignas para "pescar" informações confidenciais do usuário, como senhas e dados pessoais; *malware*, software malicioso desenvolvido para infectar máquinas e roubar dados; *spoofing*, técnica em que o invasor falsifica endereços de e-mail ou IP para se passar por uma fonte segura; e *ransomware*, um ataque complexo que pode paralisar operações inteiras e afetar a reputação das organizações, exigindo medidas preventivas como o uso de antivírus, atualizações constantes de software e sistemas eficazes de *backup* e a utilização de *malwares* (Compuworks, 2024).

Diante do exposto, observa-se que o ordenamento jurídico brasileiro tem buscado se direcionar para uma tutela penal específica, segmentada e expandida, reagindo tanto à sofisticação das condutas invasivas quanto à vulnerabilidade de sujeitos determinados, como crianças e adolescentes. A transição revela uma política criminal que reconhece o ambiente virtual não apenas como um meio de execução, mas como um espaço de lesividade autônoma e ampliada aos direitos da personalidade.

## 3.6 A tutela jurídica do direito brasileiro no contexto das eleições digitais

É bem sabido que a Constituição Federal de 1988 garante a liberdade de expressão e a liberdade de imprensa, além de estabelecer sólidas bases para uma sociedade democrática. O art. 5º, incisos IV e IX, da *Lex Mater* garantem a livre manifestação de pensamento com vedação ao anonimato, assim como a livre expressão de atividade intelectual, independentemente de censura ou licença. De forma complementar, o art. 220 resguarda à liberdade de imprensa a categoria de essencialidade para o funcionamento do sistema democrático, sendo o direito à expressão um dos pilares fundamentais do Estado Democrático de Direito (Ferrajoli, 2014).

Apesar das disposições constitucionais, o avanço da era digital impõe novos desafios para a aplicação dos direitos estabelecidos. O risco da desinformação e da propagação de *fake news* nas redes sociais podem colocar em risco a integridade do processo eleitoral, levantando o debate sobre até que ponto é aceitável limiar a liberdade de expressão para proteger a legitimidade das eleições, sendo absolutamente necessário equilibrar a proteção da ordem pública com a liberdade individual (Queiroz, 2012).

Segundo Alvim (2020), o pleito eleitoral se reveste de grande complexidade quando os influenciadores digitais exercem sua liberdade de expressão política. Esses agentes, apesar de possuírem direito de se manifestar como qualquer cidadão, podem utilizar esse poder de comunicação para pôr em risco o equilíbrio do processo eleitoral, especialmente quando existe compensação financeira envolvida.

A título de exemplo, no julgamento do Recurso Especial Eleitoral 458-67/PI, o Tribunal Superior Eleitoral, sob a relatoria do ministro Luiz Fux, tratou de caso que, embora não configurasse a captação ilícita de sufrágio, foi considerado abuso de poder devido à gravidade do desequilíbrio causado no processo eleitoral, o que reforça a necessidade de encontrar um ponto de equilíbrio entre a liberdade de expressão e a manutenção da igualdade de chances no pleito.

Percebe-se um esforço da Justiça Eleitoral para implementar estratégias de comunicação que desmintam informações incorretas e forneçam esclarecimentos para preservar a confiança pública no processo eleitoral. Diversas campanhas foram realizadas e massivamente compartilhadas, pelo Tribunal Superior Eleitoral, para esclarecer sobre o processo eleitoral *stricto sensu*, explicando ao eleitor sobre a

segurança no procedimento de votação[54].

Ato contínuo, a Resolução 23.551/2017, do Tribunal Superior Eleitoral, determinou que apenas duas modalidades de divulgação de propaganda eleitoral na *internet* são lícitas: o impulsionamento e o uso de *links* patrocinados. A modalidade de impulsionamento, desta forma, seria uma ampliação de visibilidade de determinado conteúdo dentro de uma rede social. Já o uso de *links* patrocinados apareceria na forma de anúncios ou *banners* transmitidos aos usuários.

Ademais, a legislação eleitoral, especialmente a Lei 13.488/2017, permite apenas o impulsionamento e o uso de *links* patrocinados para propaganda eleitoral na *internet*, o que demonstra um esforço para regular a influência digital de maneira a proteger a equidade no desenvolvimento do pleito. As formas de publicidade identificáveis e reguladas visam evitar abusos e garantir que todos os candidatos tenham oportunidades semelhantes de promoção.

Acerca do entendimento sobre a restrição da propaganda eleitoral paga na *internet*, conforme estipulado pela Lei 9.504/1997, busca assegurar que a promoção de candidatos seja realizada de maneira transparente e regulada, proibindo outros tipos de propaganda paga que causem distorção no processo eleitoral diante de interesses financeiros desiguais.

A liberdade de expressão, cara para a vitalidade do debate democrático, pode ser deturpada para espalhar desinformação e comprometer o processo eleitoral, surgindo a necessidade de medidas que assegurem a transparência e a lisura das eleições. Desta forma, qualquer intervenção aplicada deve ser cuidadosamente calibrada para evitar censura excessiva, o que pode prejudicar a própria essência da democracia. Não se trata a liberdade de expressão de direito absoluto, devendo ser implementadas medidas que assegurem a integridade do processo eleitoral (Gonçalves, 2017).

Uma democracia sólida e funcional deve proporcionar ampla liberdade de expressão e participação política (Diamond, Morlino, 2004), ao mesmo tempo em que garanta mecanismos institucionais de controle e de responsabilidade. Desta forma, a

---

[54] “Com duração de cerca de 1 minuto, este conteúdo buscava esclarecer informações sobre o processo eleitoral como um todo e foi também divulgado nos perfis da Justiça Eleitoral no *Facebook*, *Instagram*, *Twitter* e *YouTube*. A abordagem clara e incisiva contribuiu para que o eleitor votasse com a segurança de que as eleições brasileiras estavam sendo conduzidas de forma absolutamente legal e justa. A medida se mostrou muito eficaz. Tanto que os vídeos de esclarecimento de informações falsas produzidos pela Ascom do TSE foram compartilhados por várias instituições integrantes do sistema de Justiça, assim como por entidades ligadas à imprensa” (Rosa, 2020, n.p.).

qualidade da democracia não se limita apenas à liberdade, mas igualmente à capacidade de assegurar que todos os cidadãos possam julgar e influenciar o desempenho de seus governos através de eleições livres e justas. A proteção da liberdade de expressão deve existir, mas não a ponto de comprometer a legitimidade do processo eleitoral, que depende de instituições estáveis e imparciais.

Nenhuma democracia em estágio relativamente avançado adota o direito à liberdade de expressão como absoluto. Referido direito encontra limites nos aspectos "morais" que vigoram naquela sociedade, esses, sim, passíveis de variações culturais. Todavia, em casos de desvios abusivos do sistema constituído, é comum que seja exercido o poder repressivo do Estado, em caráter pedagógico e corretivo[55].

A discussão entre a ponderação de direitos fundamentais e a necessidade de tutela da integridade eleitoral reflete uma busca por equilíbrio que respeite tanto a liberdade de manifestação quanto a necessidade de eleições justas e transparentes. De forma decorrente, o desenvolvimento de normas que tratem desses pontos no âmbito digital é uma resposta à crescente complexidade do cenário político moderno. Neste ponto, o respeito às normas postas revela-se como imprescindível para a manutenção do Estado de Direito e da democracia (Oliveira Neto, 1994).

Segundo Sartori (1999), existe um perigo iminente do sensacionalismo no espaço público, especialmente quando acarreta um desvio do foco dos debates substanciais para ataques superficiais e espetaculares. A prática de dar ênfase exagerada a uma única perspectiva, sem dar voz à outra parte envolvida, corrompe o princípio básico da convivência civil e do embate democrático, que exige que todas as partes sejam ouvidas. No ambiente eleitoral, tal prática pode ser amplificada pelas

---

[55] "Nem no Brasil, nem nos Estados Unidos, apesar dos termos amplos da primeira emenda à Constituição Norte-Americana, o direito de exprimir o pensamento é absoluto. A licença, em que degenerou a liberdade, não provém dos textos, nem de exegese rigorosa, e, sim, da tolerância tradicional dos governantes e abuso inveterado de governados. A franquia tem por limite a incolumidade moral dos cidadãos; pouco importa que sejam poderosos ou humildes; porém o governo jamais deveria transformar-se em pelourinho para a probidade de receber insultos. O direito assegurado pelo §12 consiste na isenção da censura prévia e da apreensão policial dos exemplares. Nem judicária e posteriormente qualquer pena se aplica, se os comentários se mantêm nos limites da verdade e da decência, vigorosos, porém não insultantes. Entretanto, a má fé não se presume. Vigora o preceito *in dubiis pro libertate*. Permite-se até a propaganda de doutrina anarquista; porém não o excitamento à revolta, à destruição da propriedade, ao dano, ao assassinato ou qualquer atentado pessoal, sobretudo por meio da tribuna ou de cartazes e folhas avulsas distribuídas gratuitamente. Em todos esses casos, intervém logo a polícia; chama à ordem os oradores, priva da palavra os recalcitrantes, arranca das paredes os convites à desordem, apreende os papéis impressos em que se incita ao crime. Em se tratando, porém, de jornais, deve-se recorrer ao processo judicial, salvo se ofenderem escandalosamente a moral ou constituírem forma disfarçada de publicações distribuídas gratuitamente" (Maximiliano, 2005, p. 325).

redes sociais, capazes de promover o “efeito manada”, com distorção da liberdade de expressão e limitação do diálogo público a narrativas simplistas e tendenciosas.

A análise do papel exercido pelos influenciadores digitais nas eleições evidencia que a influência pode ser positiva, mas também acompanhada de riscos significativos. A possibilidade, por parte do influenciador digital, de apoio condicionado a remuneração financeira ou à obtenção de vantagem pode distorcer a equidade do processo eleitoral, o que se distingue da sua possibilidade de manifestação de pensamento ou ideologia. Influenciadores digitais são cidadãos e, como tais, também titulares de direitos, mas não podem se utilizar do alcance na população, mediante remuneração, para influenciar no pleito eleitoral, sob pena de configuração de captação ilícita de sufrágio[56].

Nesse sentido, é possível que haja uma responsabilização jurídica para tutelar a liberdade de expressão, que admite intervenções quando a imprensa ou as divulgações em redes sociais, a partir de uma utilização distorcida, criam um ambiente de falsas ideias e sentimentos pervertidos (Barbosa, 2016), comprometendo a capacidade do cidadão de tomar decisões informadas e racionais. Os usuários da rede mundial de computadores, de forma prévia à utilização, sequer podem ser considerados totalmente livres (Silva; Nascimento, 2023), considerando que o acesso à *internet* ocorre somente após o aceite de termos, condições e permissões, o que viabiliza igualmente um controle das informações divulgadas que possam macular a lisura dos processos eleitorais.

Desta forma, a qualidade do sistema democrático é influenciada pelo funcionamento das instituições e pela capacidade dos cidadãos exercerem seus direitos políticos de maneira efetiva, sendo imprescindível a manutenção da estabilidade das instituições em um ambiente de livre expressão, sem que seja alimentada a desinformação. Na aferição dessa qualidade, a integridade das eleições revela-se como componente crucial, exigindo cuidadoso equilíbrio entre liberdade e regulamentação.

---

[56] “[…] em princípio, não existe qualquer anormalidade no fato de um influenciador digital manifestar-se favorável ou contrariamente a esse ou aquele candidato ou projeto de poder. Os formadores de opinião, dentro ou fora da rede, são cidadãos e, como tal, fazem jus a todas as prerrogativas fundamentais na Carta Fundamental. Todavia, por analogia com aquilo que fora decidido pelo TSE nos autos do Recurso Especial Eleitoral 458-67/PI, de relatoria do ministro Luiz Fux (cujo tema de fundo tratou da "compra" de apoio político), não se olvida que a cooptação de um influenciador digital, apesar de não configurar captação ilícita de sufrágio, possui gravidade suficiente a ser qualificada como abuso de poder, caso se verifique que o ‘apoio’, na verdade, lastreou-se em contrapartida financeira a macular a igualdade de chances do processo eleitoral” (Alvim, 2020, n.p.).

## CONSIDERAÇÕES FINAIS

A evolução histórica da *internet* e o atual estado de hiperconectividade social apontam para o diagnóstico de que o ambiente virtual, especialmente nas redes sociais, é sustentado por uma arquitetura técnica e econômica que não é neutra, mas constituída de diversos fenômenos sociais. A comunicação, que era de “um para todos”, ao dar lugar à comunicação de “todos para todos” sob a promessa da democratização e da pluralidade, foi cooptada por um modelo de mercantilização da atenção humana.

Mecanismos implementados, como o de “rolagem infinita” de conteúdo, além dos algoritmos de curadoria e de personalização extrema não são, apesar do discurso, simples aperfeiçoamentos de usabilidade, mas na verdade os pilares de um sistema que é projetado e mantido para maximizar o tempo de uso e aumentar as métricas de engajamento às custas de saúde cognitiva, de coesão social e da integridade informacional.

A lógica algorítimica e sua fundamentação em aprendizagem (*machine learning*), reinvenção e processamento de dados em massa são responsáveis por alterar a forma de interagir socialmente e de perceber a realidade. São criadas verdadeiras bolhas informacionais baseadas na homofilia sistematizada. A fragmentação de informações em estímulos contínuos, desconexos e desprovidos de um senso crítico não são falhas desse sistema, mas sim provas de sua funcionalidade e rentabilidade. De um lado, a promessa de diversidade global no acesso através de um universo informacional; de outro, um ambiente unidimensional que retroalimenta vieses e preconceitos.

No âmbito das redes sociais, os influenciadores digitais que atuam com os algoritmos não estão em um vácuo técnico, mas são produtos e agentes da própria lógica aplicada às redes. Mais do que uma *expertise* em determinadas áreas do conhecimento humano ou conquistas tradicionais, é recompensado aquele que melhor se adapta e performa dentro de parâmetros estabelecidos para a retenção de atenção. A capacidade de moldar opiniões e comportamentos não pode ser ignorada, já que é amplificada exponencialmente por sistemas de recomendação que privilegiam o tempo de tela e o lucro, mitigando efeitos nocivos da hiperconectividade, como a fragmentação do tecido social, a manipulação do processo político e a ofensa à dignidade humana.

A postura de encarar os algoritmos como preditivos, e não ideológicos, apesar de ser tecnicamente correto, ignora as consequências sociais de incentivo à produção de material polarizador e sensacionalista. Os influenciadores digitais que dominam esse *modus operandi* ganham visibilidade em detrimento de pessoas que prezam pelo contraditório ou pela complexidade de informações tecnicamente corretas e bem articuladas, verdadeiros marginalizados no sistema de distribuição de conteúdo. A lógica da atenção se sobrepõe à lógica da informação qualificada, sendo os discursos da liberdade de expressão e da liberdade de consumir qualquer conteúdo aplicados para justificar uma ausência de curadoria nas redes.

A *internet* contemporânea reacende o já antigo conceito de sociedade de risco, inicialmente idealizado por pensadores como Ulrick Beck e Zygmunt Bauman, mas em um ambiente digital. A escala e a velocidade de produção e disseminação de conteúdo, antes inimagináveis, mostram que vivemos uma modernidade reflexiva hiper acelerada, com a introjeção do risco em tempo real. A desinformação massiva, a violação sistêmica da privacidade e a manipulação algorítimica viabilizadas pelo desenvolvimento tecnológico são riscos difusos e transnacionais, tanto na origem quanto no impacto. O direito, que teve suas bases construídas sobre os paradigmas da Primeira Modernidade, com características de territorialidade, causalidade linear e responsabilização individual após o dano, mostra-se estruturalmente desafiado para tutelar a nova realidade. Em uma sociedade de risco digital, ninguém está seguro; todos aumentam o risco a si e a outros simplesmente por estarem dentro das redes.

Pensando nesse cenário, avançou o Marco Civil da *Internet* quando regulamentou, juntamente à Lei Geral de Proteção de Dados, o uso das redes e o tratamento dos dados pessoais do usuário. Entretanto, foi essencial a reinterpretação, sobretudo do art. 19 da Lei 12.965/2014, pelo Supremo Tribunal Federal, quando do julgamento dos Temas 987 e 533, diante da necessidade de aplicação da lógica de responsabilização baseada no dever de diligência e na prevenção de riscos. A imposição do dever de cuidado não ignora a já tradicional tutela judicial para conflitos que possam demandar maior ponderação (crimes contra a honra, por exemplo), mas reconhece de forma especial a necessidade de imposição de obrigações proativas de moderação para conteúdo de ilicitude manifesta.

Nesse sentido, qualquer regulação Estatal que pretenda ser efetiva, portanto, deve atuar sobre referidos elementos estruturais, visto que a tecnologia não é um mero palco onde os conflitos sociais acontecem, mas sim um verdadeiro agente ativo

que, em verdade, pode configurá-los e amplificá-los. O uso indiscriminado das redes não pode ser fundamento para a erosão dos fundamentos do debate público em razão de polarização, desinformação e da substituição da reflexão crítica por uma reação emotiva e performática. A reação, por mais ágil que seja, não substitui a necessária prevenção.

Portanto, a sociedade de risco digital denuncia a falência do modelo regulatório clássico baseado na reação e na reparação. Não obstante existam leis e entendimentos judiciais que apontam para uma responsabilização jurídica no direito brasileiro, como visto, é ineficaz a ideia de conter danos de um conteúdo indevido após sua viralização; é inocente – ou mal-intencionada – a ideia de responsabilizar agentes de forma isolada por fenômenos sistêmicos. A opacidade algorítimica e a complexidade do tratamento de dados são indecifráveis para o indivíduo e para o Estado de Direito tradicional. A regulação deve migrar para de um paradigma corretivo para um paradigma constitutivo e preventivo.

O cenário se agrava, na aplicação do direito brasileiro, com o conflito entre o capital e a soberania interna. Grandes empresas internacionais do ramo de tecnologia devem se adequar às normas brasileiras para terem suas operações viabilizadas, sendo completamente inadmissível qualquer pressão ou influência indevida na criação de leis ou na interpretação jurídica que sejam baseadas em poderio econômico ou uso indevido de dinheiro.

A resposta jurídica, desta forma, não pode caminhar para a remediação de danos individuais após a materialização, como a remoção de conteúdo indevido já publicado ou a responsabilização jurídica posterior. Tais medidas tratam os sintomas, mas não a doença. Ignorar a velocidade e a capacidade de causar danos das informações difundidas na *internet* é fechar os olhos para o real problema. É necessária uma autêntica mudança no paradigma regulatório, orientada pela precaução e modulação de riscos. Corolário, devem ser impostas obrigações positivas no *design* dos projetos das plataformas de acesso à *internet*, ou se existir uma manutenção, deve ser imposta a obrigação de reavaliação dos próprios algoritmos, dos sistemas de recomendação de conteúdo e das métricas de engajamento.

Sobretudo, devem ser aplicadas severas sanções, especialmente aos provedores de conteúdo que desobedeçam às regras do jogo anteriormente estabelecidas. A fiscalização Estatal que aplica legitimamente as regras criadas pelo Poder Legislativo e interpretadas pelo Poder Judiciário não pode permitir que

eventuais descumprimentos de normas sejam aceitos sob o pálio da liberdade de expressão, ou pior, que eventuais sanções pecuniárias não inviabilizem o negócio porque o lucro supera as penas através de mero cálculo aritmético. Se pertinente, deve ser aplicada a sanção de impedimento de operação, por quanto tempo for necessário, até que as necessárias adequações sejam realizadas.

Conclui-se que o Estado deve atuar para modelar o ambiente onde os riscos são causados, impondo padrões de *design*, de transparência e de governança que internalizem a mitigação de danos coletivos. Não se trata de o que está sendo dito, mas de como o sistema permite, seleciona, amplifica e distribui o que foi dito. Devem ser impostos aos agentes digitais, de forma contínua e auditável, o dever de identificar, avaliar e mitigar os riscos em seus sistemas que coletam dados e aplicam algoritmos e modelos de negócios.

O cenário do avanço tecnológico e dos riscos sociais causados pelas redes e pela *internet* não se resolverá na aplicação irrestrita da “liberdade de expressão” ou da “liberdade na escolha do conteúdo consumido”, mesmo que em conflito com outros direitos constitucionalmente protegidos; tampouco na responsabilização jurídica individual e posterior. Somente com o estabelecimento, *a priori* e pelo Estado, de rígidos critérios de criação, disseminação e governança de informações, e principalmente, com uma fiscalização efetiva (incluindo a proibição de operação de provedores de conteúdo, se necessário), que a sociedade terá chance de avançar pelas próximas décadas sem a corrosão dos tecidos social e jurídico sofridamente criados ao longo dos últimos séculos.

## REFERÊNCIAS

10 deepfakes mais impressionantes que confundiram a internet. **Canaltech**, 2022. Disponível em: https://canaltech.com.br/internet/deepfakes-mais-impressionantes-que-confundiram-a-internet-219962/. Acesso em: 15 dez. 2025.

ABREU, Karen Cristina Kraemer. História e usos da Internet. **Bocc.ubi.pt**, [S. l.], p. 1-9, [s. d.]. Disponível em: https://arquivo.bocc.ubi.pt/pag/abreu-karen-historia-e-usos-da-internet.pdf. Acesso em: 02 mar. 2012.

AGÊNCIA SENADO. **Adultização: Senado aprova projeto para proteger crianças em ambientes digitais**. 27 ago. 2025. Disponível em: https://www12.senado.leg.br/noticias/materias/2025/08/27/adultizacao-senado-aprova-projeto-para-proteger-criancas-em-ambientes-digitais. Acesso em: 19 nov. 2025.

ALMEIDA, Gregório Assagra; LEMOS, Laís Machado Porto. A Vulnerabilidade Informacional e Tecnológica na Era Digital: Análise dos Desafios Enfrentados pelos Idosos. **Anais do Congresso Brasileiro de Processo Coletivo e Cidadania**, [S. l.], v. 12, n. 12, p. 726–751, 2024. Disponível em: https://revistas.unaerp.br/cbpcc/article/view/3558. Acesso em: 25 nov. 2025.

ALVIM, Marcio. O papel dos influenciadores digitais nas eleições municipais de 2020. **Artigo de Opinião**, 2020. Disponível em: https://www.conjur.com.br/2020-jun-04/marcio-alvim-influenciadores-digitais-eleicoes. Acesso em: 01 set. 2024.

AMARAL, Inês; SANTOS, Sofia José. Algoritmos e redes sociais: a propagação de fake news na era da pós-verdade. In: SANTOS, Sofia José (org.). **As fake news e a nova ordem (des)informativa na era da pós-verdade**. Coimbra: Imprensa da Universidade de Coimbra, 2019. p. 63–85. Disponível em: https://hdl.handle.net/10316/96605. DOI: https://doi.org/10.14195/978-989-26-1778-7_5. Acesso em: 06 maio 2025.

ASFOR, Ana Paula. Do início da personalidade civil. **JusNavigandi**, Teresina, ano 18, n. 3629.8, jun. 2013. Disponível em: http://jus.com.br/artigos/24650/do-inicio-da-personalidade-civil. Acesso em: 19 nov. 2025.

Aumentam casos de estelionato digital. Brasília: **Rádio Senado**, 12 ago. 2025. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2025/08/12/aumentam-casos-de-estelionato-digital. Acesso em: 23 dez. 2025.

BARBOSA, Rui. **A imprensa e o dever da verdade**. São Paulo: Hunter Books, 2016.

BARRETO JUNIOR, I. F.; GALLINARO, F.; SAMPAIO, V. G. R. Marco Civil da Internet e direito à privacidade na sociedade da informação. **Revista Direito, Estado e Sociedade**, n. 52, 2018. Disponível em: https://doi.org/10.17808/des.52.835. Acesso em: 12 maio 2025.

BAUMAN, Zygmunt. **Modernidade e ambivalência**. Tradução: Marcus Penchel. Rio de Janeiro: Jorge Zahar Editor, 1999.

BECK, Ulrich. “A reinvenção da política” In: GIDDENS, Anthony; BECK, Ulrich; LASH, Scott. **Modernização reflexiva: política, tradição e estética na ordem social moderna**. São Paulo: Ed. Unesp, 1995.

BECK, Ulrich. **Liberdade ou Capitalismo: Ulrich Beck conversa com Johannes Willms**. São Paulo: Ed. Unesp, 2003.

BECK, Ulrich; GIDDENS, Anthony; LASH, Scott. **Modernização reflexiva: política, tradição e estética na ordem social moderna**. Tradução: Magda Lopes. São Paulo: Editora da Universidade Estadual Paulista, 1997.

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte especial 2: crimes contra a pessoa**. 18. ed. São Paulo: Saraiva Educação, 2018a.

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte geral 1**. 24. ed. São Paulo: Saraiva Educação, 2018b.

BITTAR, Eduardo C. B. **O direito na pós-modernidade**. Rio de Janeiro: Forense Universitária, 2014.

BOBBIO, Norberto. **A era dos direitos**. 9. ed. Rio de Janeiro: Elsevier, 2004.

BORDIGNON, C.; BONAMIGO, I. S. Os jovens e as redes sociais virtuais. **Pesquisas e Práticas Psicossociais**, São João del Rei, v. 12, n. 2, p. 1-16, maio/ago. 2017. Disponível em: https://seer.ufsj.edu.br/revista_ppp/article/view/2456/1699. Acesso em: 03 abr. 2025.

BRAGA, Renê Morais da Costa. A indústria das fake news e o discurso de ódio. In: PEREIRA, Rodolfo Viana (Or.). **Direitos políticos, liberdade de expressão e discurso de ódio**. Volume I. Belo Horizonte: IDDE, 2018, p. 203-220. ISBN 978-85-67134-05-5.

BRASIL. Presidência da República. **Guia de boas práticas da Lei Geral de Proteção de Dados Pessoais**. Secretaria-Geral da Presidência da República, 2021a.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade n. 3741**, Relator: Min. Ricardo Lewandowski, julgado em 06 set. 2006. Diário da Justiça, Brasília, DF, 6 set. 2006. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=408096. Acesso em: 24 set. 2024.

BRASIL. Supremo Tribunal Federal. **Informação à Sociedade: RE 1.037.396 (Tema 987) e RE 1.057.258 (Tema 533): responsabilidade de plataformas digitais por conteúdo de terceiros**. Brasília: STF, 26 jun. 2025. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/Informac807a771oa768SociedadeArt19MCI_vRev.pdf. Acesso em: 18 set. 2025.

BRASIL. Supremo Tribunal Federal. **Petição 12.404 Distrito Federal**. Primeira Turma. Relator: Min. Alexandre de Moraes. Julgamento colegiado em 03 set. 2024c. Disponível em: https://noticias-stf-wp-prd.s3.sa-east-1.amazonaws.com/wp-content/uploads/wpallimport/uploads/2024/10/08171351/Pet-12404-Merito-desbloqueio.pdf. Acesso em: 01 out. 2025.

BRASIL. Supremo Tribunal Federal. **STF autoriza retorno imediato do X e determina que Anatel adote providências para retomada do serviço**. Empresa cumpriu condições estipuladas pelo relator, ministro Alexandre de Moraes, e a plataforma poderá voltar a ser utilizada pelos brasileiros. 08 out. 2024b. Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-autoriza-o-retorno-imediato-do-x-e-determina-que-anatel-adote-providencias-para-a-retomada-do-servico/. Acesso em: 01 out. 2025.

BRASIL. Supremo Tribunal Federal. **STF confirma decisão que suspendeu o X, antigo Twitter, em todo o país**. Por unanimidade, a Primeira Turma referendou a medida adotada pelo ministro Alexandre de Moraes. 02 set. 2024a. Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-confirma-decisao-que-suspendeu-o-x-antigo-twitter-em-todo-o-pais/. Acesso em: 01 out. 2025.

BRASIL. Tribunal Superior Eleitoral. **Resolução n. 23.551, de 18 de dezembro de 2017**. Dispõe sobre propaganda eleitoral, utilização e geração do horário gratuito e condutas ilícitas em campanha eleitoral nas eleições de 2018. Diário da Justiça Eletrônico, Brasília, DF, 18 dez. 2017. Disponível

em: https://www.tse.jus.br/legislacao/compilada/res/2017/resolucao-no-23-551-de-18-de-dezembro-de-2017. Acesso em: 24 set. 2024.

BRASIL. **Código Civil**. Lei nº 10.406, de 10 de janeiro de 2002. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 07 nov. 2025.

BRASIL. **Código de Processo Penal**. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 15 dez. 2025.

BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 15 dez. 2025.

BRASIL. **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 23 set. 2024.

BRASIL. **Lei das Contravenções Penais**. Decreto-Lei nº 3.688, de 3 de outubro de 1941. Diário Oficial da União: seção 1, Rio de Janeiro, RJ, 3 out. 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3688.htm. Acesso em: 31 out. 2025.

BRASIL. **Lei Geral de Proteção de Dados Pessoais: Anotada**. 1. ed. Brasília: Senado Federal, 2021b.

BRASIL. **Lei nº 11.340, de 7 de agosto de 2006**. Cria mecanismos para coibir a violência doméstica e familiar contra a mulher, nos termos do § 8º do art. 226 da Constituição Federal e do Capítulo VII do Título II da Parte Especial do Código Penal, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11340.htm. Acesso em: 15 dez. 2025.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República, [2012]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 23 dez. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: seção 1,

Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12 maio 2025.

BRASIL. **Lei nº 13.488, de 6 de outubro de 2017**. Altera as Leis nº 9.504/1997, 9.096/1995 e 4.737/1965, para dispor sobre a propaganda eleitoral e outros temas. Diário Oficial da União, Brasília, DF, 7 out. 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13488.htm. Acesso em: 23 set. 2024.

BRASIL. **Lei nº 14.132, de 31 de março de 2021**. Acrescenta o art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição. Brasília, DF: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm. Acesso em: 23 dez. 2025.

BRASIL. **Lei nº 14.192, de 4 de agosto de 2021**. Estabelece normas para prevenir, reprimir e combater a violência política contra a mulher e altera o Código Eleitoral. Diário Oficial da União, Brasília, DF, 5 ago. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14192.htm. Acesso em: 23 set. 2024.

BRASIL. **Lei nº 14.811, de 12 de janeiro de 2024**. Institui medidas de proteção à criança e ao adolescente contra a violência nos estabelecimentos educacionais ou similares [...]. Brasília, DF: Presidência da República, [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/l14811.htm. Acesso em: 23 dez. 2025.

BRASIL. **Lei nº 4.737, de 15 de julho de 1965**. Institui o Código Eleitoral. Diário Oficial da União, Brasília, DF, 19 jul. 1965. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l4737.htm. Acesso em: 23 set. 2024.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 07 nov. 2025.

BUENO ROCHA RODRIGUES DE FARIA, Cybele. Regulação da Internet e a Proteção das Liberdades Individuais. **Revista Ibero-Americana De Humanidades, Ciências E Educação**, 10(8), 15–21. 2024. https://doi.org/10.51891/rease.v10i8.15053.

BÜRGER, Gabriela. **Ecologia da informação: como a hiperconectividade e o excesso de informação afetam a sociedade**. 2014. 46 f. Trabalho de Conclusão de Curso (Tecnologia em Segurança da Informação) - Faculdade de Tecnologia de Americana, Americana, 2014. Disponível em: http://ric-cps.eastus2.cloudapp.azure.com/bitstream/123456789/1089/1/20141S_BURGERGabriela_TCCPD1273.pdf. Acesso em: 02 abr. 2025.

CAMPELLO, Cristiane Cavalcanti Barreto. A propaganda eleitoral antecipada após a lei 13.165/2015 e a ferramenta de impulsionamento de publicações nas redes sociais. **Revista de Estudos Eleitorais**, Recife, n. 1, p. 55-64, 2017. Disponível em: http://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/4236. Acesso em: 05 set. 2024.

CANOTILHO, J. J. Gomes [et al.]. **Comentários à Constituição do Brasil**. 2. ed. São Paulo: Saraiva Educação, 2018.

CARDOSO, Henrique Ribeiro. **Controle da Legitimidade da Atividade Normativa das Agências Reguladoras**. Rio de Janeiro: Editora Lumen Juris, 2010.

CARVALHO, Luiz Paulo; OLIVEIRA, Jonice; CAPPELLI, Claudia. Pesquisas em Análise de Redes Sociais e LGPD, análises e recomendações. In: BRAZILIAN WORKSHOP ON SOCIAL NETWORK ANALYSIS AND MINING (BRASNAM), 9., 2020, Cuiabá. **Anais [...]**. Porto Alegre: Sociedade Brasileira de Computação, 2020. p. 73-84. ISSN 2595-6094. DOI: https://doi.org/10.5753/brasnam.2020.11164.

Casal de influenciadores é alvo de operação contra jogos de azar online em MG. **O Tempo**, 1 ago. 2024, 16h20. Disponível em: https://www.otempo.com.br/cidades/2024/8/1/casal-de-influenciadores-e-alvo-de-operacao-contra-jogos-de-azar?fbclid=PAZXh0bgNhZW0CMTEAAaaQb794O8mgLAS9DIDpp_LS19Q_adlcQCnHioWkjExaVJBXYoJuSV1-Fsg_aem_N1cbYHwhArfFagbF9wrF-g. Acesso em: 15 dez. 2025.

Cerca de 15 influenciadores são investigados em operação contra "Jogo do Tigrinho" em SP. **Band Vale**, 17 jun. 2024, 14h53. Atualizado em: 17 jun. 2024, 16h56. Disponível em: https://www.band.uol.com.br/band-vale/noticias/cerca-de-15-influenciadores-sao-investigados-em-operacao-contra-divulgacao-do-jogo-do-tigrinho-202406171453. Acesso em: 15 dez. 2025.

CNN Brasil. Como funciona a regulamentação das redes sociais em outros países. **CNN Brasil**, 2024. Disponível

em: https://www.cnnbrasil.com.br/politica/como-funciona-a-regulamentacao-das-redes-sociais-em-outros-paises/. Acesso em: 27 out. 2025.

COELHO, Fábio Ulhoa. **Curso de direito civil: obrigações [livro eletrônico]: responsabilidade civil**, volume 2. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. OS DIREITOS DA PERSONALIDADE FRENTE À SOCIEDADE DE VIGILÂNCIA: PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E CONSENTIMENTO NAS REDES SOCIAIS. **Revista Brasileira de Direito Civil em Perspectiva**, Florianópolis, Brasil, v. 5, n. 2, p. 22–41, 2019. DOI: 10.26668/IndexLawJournals/2526-0243/2019.v5i2.5778. Disponível em: https://www.indexlaw.org/index.php/direitocivil/article/view/5778. Acesso em: 07 abr. 2025.

D'ANCONA, Matthew. **Pós-verdade: a nova guerra contra os fatos em tempos de fake news**. Barueri: Faro Editorial, 2018.

DAQUINO, Fernando. A história das redes sociais: como tudo começou. **Tec Mundo**. Nov. 2012. Disponível em: http://www.tecmundo.com.br/redes-sociais/33036-a-historia-das-redes-sociais-como-tudo-comecou.htm. Acesso em 18 maio 2025.

DE MACEDO MENNA BARRETO, R. Privacidade e redes sociais na internet: notas à luz da Lei nº 12.965/2014 (Marco Civil da Internet). **Revista da Faculdade de Direito do Sul de Minas**, v. 31, n. 1, 2015. Disponível em: https://revista.fdsm.edu.br/index.php/revistafdsm/article/view/49. Acesso em: 12 maio 2025.

Deepfake: Colocaram meu rosto em um vídeo pornô. **G1**, 2022. Disponível em: https://g1.globo.com/mundo/noticia/2022/10/21/deepfake-colocaram-meu-rosto-em-um-video-porno.ghtml. Acesso em: 15 dez. 2025.

DIAMOND, Larry; MORLINO, Leonardo. The Quality of Democracy: an Overview. **Journal of Democracy**, v. 15, n. 4, p. 20-31. Johns Hopkins University Press, out. 2004.

DINIZ, Maria Helena. **Curso de direito civil brasileiro**. Vol. 7. Responsabilidade civil. 21. ed. rev. e atual. São Paulo: Saraiva, 2007.

Dreamgrow. **The 15 biggest social media sites and apps in 2025**. Dreamgrow, 23 jan. 2025. Disponível em: https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/. Acesso em: 04 abr. 2025.

DUTRA, Maristela Ap.; SILVA, Lorena Jaqueline. A responsabilidade civil dos provedores de internet diante de comentários ofensivos inseridos por terceiros nas redes sociais à luz do Marco Civil da Internet. **Revista Jurídica UNIARAXÁ**, Araxá, v. 20, n. 19, p. 141–168, ago. 2016.

FERRAJOLI, Luigi. **Direito e Razão**. 4. ed. São Paulo: RT, 2014.

FINNIS, John. **Direito natural em Tomás de Aquino: sua reinserção no contexto do juspositivismo analítico**. Tradução: Carlos Eduardo Adriano Júnior. São Paulo: Martins Fontes, 2007.

FREITAS, Carlos Eduardo Pereira; BORGES, Messias Vasconcelos; RIOS, José Riverson Araújo Cysne. O algoritmo classificatório no feed do Instagram. In: CONGRESSO BRASILEIRO DE CIÊNCIA DA COMUNICAÇÃO – INTERCOM, 39., 2016, São Paulo. **Anais...** São Paulo: Intercom, 2016. Tema: Comunicação e educação: caminhos integrados para um mundo em transformação. Disponível em: http://www.repositorio.ufc.br/handle/riufc/44471. Acesso em: 06 maio 2025.

Fui colocada em deepfake pornô pelo meu melhor amigo. **BBC NEWS**, 2024. Disponível em: https://www.bbc.com/portuguese/articles/cev992wp5zwo. Acesso em: 15 dez. 2025.

FURTADO, Alessa Aparecida Costa; GOULART, Libia Kicela. Inobservância da ética médica na publicidade nas redes sociais: uma análise dos impactos na responsabilidade civil. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 8, n. 11, p. 1153-1166, 2022.

DOI: https://doi.org/10.51891/rease.v8i11.7713

G1. **Acesso à internet em residências brasileiras salta de 13% para 85% em 20 anos, aponta pesquisa TIC Domicílios 2024**. G1, 31 out. 2024. Disponível em: https://g1.globo.com/tecnologia/noticia/2024/10/31/acesso-a-internet-em-20-anos-pesquisa-tic-domicilios-2024.ghtml. Acesso em: 01 abr. 2025.

G1. **Europa e Reino Unido já adotam leis que exigem responsabilidade das redes sociais e das grandes empresas de tecnologia**. G1, 2024. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2024/12/18/europa-e-reino-unido-ja-adotam-leis-que-exigem-responsabilidade-das-redes-sociais-e-das-grandes-empresas-de-tecnologia.ghtml. Acesso em: 27 out. 2025.

GABRIEL, Martha. **Marketing na era digital**. São Paulo: Novatec, 2010.

GINDRE, Gustavo. Agenda de regulação: uma proposta para o debate. In: SILVEIRA, Sergio A. et al. **Comunicação digital e a construção dos commons:**

**redes virais, espectro aberto e as novas possibilidades de regulação**. São Paulo: Perseu Abramo, 2007.

GONÇALVES, Victor Eduardo Rios. **Legislação Penal Especial**. 3. ed. São Paulo: Saraiva, 2017.

GROSS, Clarissa Piterman. Fake news e democracia: discutindo o status normativo do falso e a liberdade de expressão. In: RAIS, Diogo. **Fake News: a conexão entre a desinformação e o direito**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. n.p. Disponível em: https://proview.thomsonreuters.com/title.html?redirect=true&titleKey=rt%2Fmonografias%2F156970600%2Fv2.5&titleStage=F&titleAcct=i0adc41900000015b364ba976eee27f33#sl=p&eid=b4f8b515abd8a3cc1534ffd1815763dd&eat=%5Bereid%3D%22b4f8b515abd8a3cc1534ffd1815763dd%22%5D&pg=RB-2.1&psl=&nvgS=false. Acesso em: 15 set. 2020.

GUIVANT, Julia S. A teoria da sociedade de risco de Ulrich Beck: entre o diagnóstico e a profecia. **Revista Brasileira de Ciências Sociais**, v. 15, n. 44, p. 95–101, abr. 2001. Disponível em: https://revistaesa.com/ojs/index.php/esa/article/view/188/184. Acesso em: 15 abr. 2025.

GUTIÉRREZ, Ricardo. Combatendo a desinformação e preservando a liberdade de expressão. **Seminário Internacional Fake News e Eleições**, Brasília, p. 28-31, maio 2019. Disponível em: https://www.justicaeleitoral.jus.br/desinformacao/arquivos/livro-fake%20news-mioloweb.pdf. Acesso em: 21 out. 2020.

HANSEN, Berta Hoffmann Azevedo et al. Hiperconectividade e exaustão. **Jornal de Psicanálise**, São Paulo, v. 55, n. 102, p. 1-3, 2022. Disponível em: https://pepsic.bvsalud.org/pdf/jp/v55n102/v55n102a02.pdf. Acesso em: 02 abr. 2025.

HISSA, D. L. A. O design multimodal de plataformas de mídias sociais: da barra de rolagem infinita à organicidade algoritmizada do feed de notícias. **Revista Intersaberes**, v. 18, p. 1-21, 2023. Disponível em: https://www.revistasuninter.com/intersaberes/index.php/revista/article/view/2496. Acesso em: 03 abr. 2025.

HOBSBAWM, Eric J. **Bandidos**. Tradução: Donaldson M. Garschagen. 4. ed. São Paulo: Paz e Terra, 2010.

India's general election is being impacted by Deepfakes. **Le Monde**, 2024. Disponível em: https://www.lemonde.fr/en/pixels/article/2024/05/21/india-s-general-election-is-being-impacted-by-deepfakes_6672168_13.html?utm_source=the_news&utm_medium=newsletter&utm_campaign=24-05-2024. Acesso em: 15 dez. 2025.

Influenciadores são alvos de operação contra ‘Jogo do Tigrinho’. **TERRA**, 17 jun. 2024, 15h30. Disponível em: https://www.terra.com.br/economia/nao-caia-nessa/influenciadores-sao-alvos-de-operacao-contra-jogo-do-tigrinho,8c142f0f3005608957b684101902dc63jbbwds46.html?utm_source=clipboard. Acesso em: 17 ago. 2024.

Influenciadores são presos em operação contra 'Jogo do Tigrinho' em Alagoas. **UOL**, 25 jun. 2024, 08h56. Atualizado em: 25 jun. 2024, 10h29. Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2024/06/25/prisao-influenciadores-jogo-do-tigrinho.htm?cmpid=copiaecola. Acesso em: 17 ago. 2024.

'Jogo do Tigrinho': entenda a operação que prendeu influenciadores digitais no Pará. **G1 Pará e TV Liberal**, Belém, 19 dez. 2023, 00h01. Disponível em: https://g1.globo.com/pa/para/noticia/2023/12/19/jogo-do-tigrinho-entenda-a-operacao-que-prendeu-influenciadores-digitais-no-para.ghtml. Acesso em: 17 ago. 2024.

KASPERSKY. **O que é uma VPN? Como funciona, tipos e benefícios**. Kaspersky, 2025. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-a-vpn. Acesso em: 21 out. 2025.

KAUFMAN, D.; SANTAELLA, L. O papel dos algoritmos de inteligência artificial nas redes sociais. **Revista Famecos**, Porto Alegre, v. 27, p. 1-10, jan.-dez. 2020. Disponível em: https://pucrs.emnuvens.com.br/revistafamecos/article/view/34074. Acesso em: 03 abr. 2025.

LEITE, Flávia Piva Almeida. O exercício da liberdade de expressão nas redes sociais: e o Marco Civil da Internet. **Revista de Direito Brasileira**, Florianópolis, v. 13, n. 6, p. 150–166, 2016. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/2899. Acesso em: 12 maio 2025.

LEMOS, A.; LÉVY, P. **O futuro da internet: em direção a uma ciberdemocracia**. São Paulo: Ed. Paulus, 2010.

LESSA, Moyana Mariano Robles; CABRAL, Hildeliza Lacerda Tinoco Boechat; SILVESTRE, Gilberto Fachetti. Deepfake: a inteligência artificial e o algoritmo causando riscos à sociedade no ciberespaço. **Revista Jurídica Derecho y Cambio Social**. Ed. nº 61., jul.-set. 2020, pp. 475-487.

LÉVY, P. **O que é virtual**. São Paulo: Ed. 34 Ltda, 1996.

LIMA, Jorge da Cunha; POZZOLI, Lafayette (Orgs.). **Presença de Maritain: testemunhos**. 2. ed. São Paulo: LTR, 2012. 272 p. ISBN 978-85-361-2318-9.

LIMA, Ludmila Lopes; MENEZES, Dayse Rodrigues Alves de; CARDOSO, Larissa de Oliveira. Responsabilidade civil dos influenciadores digitais. **Revista Multidisciplinar do Nordeste Mineiro**, v. 13, n. 1, 2023. DOI: 10.61164/rmnm.v13i1.1986.

LONGHI, João Victor Rozatti. **Responsabilidade civil e redes sociais [recurso eletrônico]: retirada de conteúdo, perfis falsos, discurso de ódio e fake news**. 3. ed. São Paulo: Editora Foco, 2025.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018.

MAIA, R. M.; CURVO, A. C. A Responsabilidade Civil por Danos Materiais nas Redes Sociais. **Revista de Iniciação Científica E Extensão**, 8(1), 48–57, 2025. Recuperado de https://reicen.emnuvens.com.br/revista/article/view/236

MARÇAL, Carolina Hespanhol Pinheiro. **A responsabilidade civil dos influenciadores digitais que fazem publicidade de plataformas digitais de jogos de azar e apostas online à luz do ordenamento jurídico brasileiro**. 2023. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Presbiteriana Mackenzie, São Paulo. Orientador: André Pagani de Souza. Disponível em: https://dspace.mackenzie.br/items/6fee84c9-38c6-411b-af30-f020d12ba537. Acesso em: 15 fev. 2024.

MARQUES, Claudia Lima; MIRAGEM, Bruno. **O novo direito privado e a proteção dos vulneráveis**. São Paulo: RT, 2012.

MAXIMILIANO, Carlos. **Comentários à Constituição brasileira de 1891**. Brasília: Senado Federal, Conselho Editorial, 2005.

MELO JÚNIOR, José Eustáquio de; OLIVEIRA, Gustavo Paschoal Teixeira de Castro. Contributos da Logística para a elaboração do marco legal da Inteligência Artificial no Brasil. **Revista de Informação Legislativa: RIL**, Brasília, DF, v. 60, n. 237, pp. 99-114, jan./mar. 2023. Disponível

em: https://www12.senado.leg.br/ril/edicoes/60/237/ril_v60_n237_p99. Acesso em: 15 dez. 2025.

MICHELETTI, Miquéias. **LGPD: o abismo entre a teoria e a prática**. 1. ed. São Paulo: Ed. do Autor, 2021.

NISHIYAMA, Adolfo Mamoru; DENSA, Roberta. A Proteção dos Consumidores Hipervulneráveis: os Portadores de Deficiência, os Idoso, as Crianças e os Adolescentes. **Revista de Direito do Consumidor**, São Paulo, v. 76, p. 13-45, out./dez. 2010.

NOHARA, Irene Patrícia. Desafios da Ciberdemocracia diante do fenômeno das fake news: regulação estatal em face dos perigos da desinformação. In: RAIS, Diogo. **Fake News: a conexão entre a desinformação e o direito**. 2. ed. São Paulo: Revista dos Tribunais, 2020.

NORMANDO, Priscila. Um breve estudo sobre o conceito de responsabilidade. **Intuitio**, 5(2), 249-265, 2012. Porto Alegre: PUCRS. ISSN 1983-4012.

OLIVEIRA NETO, Olavo de. **Comentários à Lei de Contravenções Penais**. São Paulo: Ed. Revista dos Tribunais, 1994.

Phishing, malware, spoofing e ransomware: ameaças que chegam por email. [S. l.]: **CompuWorks**, 2024. Disponível em: https://compuworks.pt/phishing-malware-spoofing-e-ransomware-4-ameacas-que-chegam-por-email/. Acesso em: 23 dez. 2025.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018**. São Paulo: Saraiva Educação, 2018.

PINHEIRO, Victor Sales. **A crise da cultura e a ordem do amor: ensaios filosóficos**. São Paulo: É Realizações, 2021.

POZZOLI, Lafayette. **Maritain e o Direito**. São Paulo: Loyola, 2001.

Primeira-ministra da Itália pede € 100 mil em indenização após ser vítima de deepfake pornográfico. **CNN**, 2024. Disponível em: https://www.cnnbrasil.com.br/internacional/primeira-ministra-da-italia-pede-e-100-mil-em-indenizacao-apos-ser-vitima-de-deepfake-pornografico/. Acesso em: 15 dez. 2025.

QUEIROZ, Paulo. **Curso de Direito Penal - Parte Geral**. v. 1. 8. ed. rev. atual. e ampl. Salvador: JusPodivm, 2012.

REVISTA DE DIREITO ADMINISTRATIVO. Rio de Janeiro: Fundação Getúlio Vargas, v. 261, 2012. Quadrimestral. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/8856/7678. Acesso em: 01 set. 2024.

RIBEIRO, S. S. H. P. Sobre repovoar narrativas: o trabalho dos influenciadores digitais a partir de uma abordagem sociotécnica. **Civitas - Revista de Ciências Sociais**, v. 21, n. 2, p. 271–281, maio 2021.

ROCHA, Carlos. **Algoritmos das Redes Sociais e Seitas Políticas: Reflexões sobre Tecnologia, Democracia e Sociedade**. São Paulo: Pimenta Cultural, 2024.

ROMANINI, Anderson Vinícius; MIELLI, Renata Vicentini. Mentiras, discurso de ódio e desinformação violaram a liberdade de expressão nas eleições de 2018. In: COSTA, Cristina; BLANCO, Patrícia. **Liberdade de expressão: questões da atualidade**. São Paulo: ECA-USP, 2019.

ROSA, Ana Cristina. Desinformação e eleições: a comunicação como instrumento estratégico. In: RAIS, Diogo. **Fake news: a conexão entre a desinformação e o direito**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. n.p. Disponível em: https://proview.thomsonreuters.com/title.html?redirect=true&titleKey=rt%2Fmonografias%2F156970600%2Fv2.5&titleStage=F&titleAcct=i0adc41900000015b364ba976eee27f33#sl=p&eid=b4f8b515abd8a3cc1534ffd1815763dd&eat=%5Bereid%3D%22b4f8b515abd8a3cc1534ffd1815763dd%22%5D&pg=RB-2.1&psl=&nvgS=false. Acesso em: 05 set. 2024.

ROSA, António Machuco. As origens históricas da Internet: uma comparação com a origem dos meios clássicos de comunicação ponto a ponto. **Estudos em Comunicação**, n. 11, p. 89-116, maio 2012. Disponível em: https://repositorio-aberto.up.pt/bitstream/10216/74026/2/76286.pdf. Acesso em: 02 mar. 2012.

RUEDIGER, M.A. et al. **Bots e o Direito eleitoral brasileiro: eleições 2018**. Policy paper 3. Rio de Janeiro: FGV DAPP, 2019. p. 07.

RUFINO, A. F.; TABOSA, H. R.; NUNES, J. V. Redes sociais: surgimento e desenvolvimento dos micro-bloggings. In: CONGRESSO DE CIÊNCIAS DA COMUNICAÇÃO NA REGIÃO NORDESTE, 11., 2009, Teresina. **Anais...** Teresina: Intercom, 2009. 1 CD-ROM. Disponível em: https://repositorio.ufc.br/bitstream/riufc/22674/1/2010_eve_arufino.pdf. Acesso em: 03 abr. 2025.

RUSSELL, Stuart J. **Inteligência artificial**. Tradução: Regina Célia Simille. Rio de Janeiro: Elsevier, 2013.

SANTOS, G. B.; EDLER, G. O. B. Oversharenting: A Superexposição da Imagem das Crianças e Adolescentes nas Redes Sociais e a Responsabilidade Civil dos Pais. **Revista Ibero-Americana De Humanidades, Ciências E Educação**, 8(6), 852–869, 2022. https://doi.org/10.51891/rease.v8i6.5973

SANTOS, Rodrigo Otávio dos. Algoritmos, engajamento, redes sociais e educação. **Acta Educ.**, Maringá, v. 44, e52736, 2022. Disponível em: http://educa.fcc.org.br/scielo.php?script=sci_arttext&pid=S2178-52012022000100208&lng=pt&nrm=iso. Acesso em 06 maio 2022. Epub 01-Maio-2022. https://doi.org/10.4025/actascieduc.v44i1.52736.

SARLET, Ingo. Liberdade de expressão e biografias não autorizadas — notas sobre a ADI 4.815. **Consultor Jurídico**. 19 de junho de 2015. Disponível em: https://www.conjur.com.br/2015-jun-19/direitos-fundamentais-liberdade-expressao-biografias-nao-autorizadas/. Acesso em: 18 maio 2025.

SARTORI, Giovanni. **Homo videns: televisão e pós-pensamento**. São Paulo: Companhia das Letras, 1999.

SCHREIBER, Anderson. Marco Civil da Internet: avanço ou retrocesso? A responsabilidade civil por danos derivado do conteúdo gerado por terceiro. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (org.). **Direito e Internet III: Marco Civil da Internet, Lei nº 12.965/2014**. Tomo II. São Paulo: Quartier Latin, 2015. p. 291.

SEGURADO, Rosemary; LIMA, Carolina Silva Mandú de; AMENI, Cauê S. Regulamentação da internet: perspectiva comparada entre Brasil, Chile, Espanha, EUA e França. **História, Ciências, Saúde – Manguinhos**. Rio de Janeiro, v.22, supl.,

SEIXAS, R. A retórica da pós-verdade: o problema das convicções. **Revista Eletrônica de Estudos Integrados em Discurso e Argumentação**, v. 18, n. 1, 2019. Disponível em: https://doi.org/10.17648/eidea-18-2197. Acesso em: 15 out. 2025.

SERRO, Bruna Manhago. Da responsabilidade civil dos provedores de aplicações frente à Lei 12.965/2014: análise doutrinária e jurisprudencial. **Anais do 3º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da**

**sociedade em rede**, Santa Maria/RS, UFSM, 27 a 29 maio 2015. ISSN 2238-9121. p. 1-15.

SETENARESKI, Ligia; PERES, Leticia M.; BONA, Luis C. E.; DUARTE JR., Elias P. Panorama mundial da regulação da neutralidade da rede. **Revista Internet e Sociedade**, fev. 2020. Disponível em: https://revista.internetlab.org.br/panorama-mundial-da-regulacao-da-neutralidade-da-rede/. Acesso em: 22 out. 2025.

SIEBERT, S.; PEREIRA, I. V. A pós-verdade como acontecimento discursivo. **Ling. (dis)curso**, v. 20, n. 2, p. 239-249, maio-ago. 2020. Disponível em: https://doi.org/10.1590/1982-4017/200201-00-00. Acesso em: 15 out. 2025.

SILVA, C. R. M.; TESSAROLO, F. M. Influenciadores digitais e as redes sociais enquanto plataformas de mídia. In: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 39., 2016, São Paulo. **Anais...** São Paulo: Intercom, 2016. Disponível em: https://portalintercom.org.br/anais/nacional2016/resumos/R11-2104-1.pdf. Acesso em: 03 abr. 2025.

SILVA, Lucas Gonçalves da; CARVALHO, Mariana Amaral. Direito ao esquecimento na sociedade da informação: análise dos direitos fundamentais no meio ambiente digital. **Revista Brasileira de Direitos e Garantias Fundamentais**, Maranhão, v. 3, n. 2, p. 66-86, jul./dez. 2017.

SILVA, Lucas Gonçalves da; MELO, Bricio Luis da Anunciação. A Lei Geral de Proteção de Dados como instrumento de concretização da autonomia privada em um mundo cada vez mais tecnológico. **Revista Jurídica**, Curitiba, v. 3, n. 56, p. 341-362, 2019.

SILVA, Lucas Gonçalves da; NASCIMENTO, Reginaldo Felix. Colonialismo de dados: o apagar das vozes no conhecimento social. **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 24, n. 3, p. 73-105, set./dez. 2023. DOI: https://doi.org/10.18759/rdgf.v24i3.2296.

SILVA, Lucas Gonçalves da; SANTOS, Elaine Celina Afra da Silva. O aumento das “fake news” durante a propaganda eleitoral e sua possível influência no resultado do pleito. **Revista Brasileira de Direitos e Garantias Fundamentais**, Goiânia, v. 5, n. 1, p. 1-19, jan./jun. 2019. e-ISSN 2526-0111.

SILVA, Lucas Gonçalves da; SOUZA, Patrícia Verônica Nunes Carvalho Sobral de. O controle social como instrumento de defesa da democracia. **Revista Jurídica**, Curitiba, v. 4, n. 49, p. 207-230, 2017. DOI: 10.6084/m9.figshare.5632144.

SILVA, Lucas Gonçalves da; TAKANO, Camila Cardoso. O constitucionalismo digital e as novas tecnologias da informação e comunicação (TIC). **Revista de Direito, Governança e Novas Tecnologias**, [S. l.], v. 6, n. 1, p. 1-15, jan./jun. 2020.

SILVA, Pedro. A manipulação da informação nas redes sociais: implicações para a democracia. In: PEREIRA, José (Org.). **O impacto das redes sociais na política**. São Paulo: Editora Atlas, 2022. p. 45-67.

SILVA, Roberta Soares da; GUARDIA, Karina Joelma Bacciotti Selingardi. A sociedade de risco global. **DIGE – Direito Internacional e Globalização Econômica**, v. 1, n. 1-Ext, 2019. Edição Extraordinária – Direitos Humanos. Disponível em: https://revistas.pucsp.br/DIGE/article/view/42350. Acesso em: 15 abr. 2025.

SOARES de Almeida, D.; ALVES Coutinho da Silva, R.; de Lima Ferreira, S. Análise acerca da responsabilidade civil dos influenciadores digitais na divulgação de jogos de azar. **Revista Ratio Iuris**, v. 3, n. 1, p. 87–98, 2024. Disponível em: https://periodicos.ufpb.br/index.php/rri/article/view/69047. Acesso em: 17 ago. 2024.

SOARES, R. G. Responsabilidade Civil das Plataformas de Redes Sociais e o Entretenimento Jurídico Atribuído a Elas. **Revista Ibero-Americana De Humanidades, Ciências E Educação**, 9(11), 1744–1757, 2023. https://doi.org/10.51891/rease.v9i11.12510

SOUZA, Clarisse Sieckenius de. **Vida na Era da Hiperconectividade: Resenha de partes selecionadas do livro "The Onlife Manifesto - Being Human in a Hyperconnected Era" (Floridi, 2015)**. Rio de Janeiro: SERG/PUC-Rio, 2021. 15 p. (EMAPS Resenhas, n. 5). Disponível em: https://hcc.inf.puc-rio.br/EMAPS/userfiles/downloads/Resenha-Floridi2015.pdf. Acesso em: 02 abr. 2025.

SOUZA, Q. R.; QUANDT, C. O. Metodologia de análise de redes sociais. In: DUARTE, F.; QUANDT, C.; SOUZA, Q. (Org.). **O tempo das redes**. São Paulo: Perspectiva, 2008, p. 31-63.

SPENCER, Michael K. **Deep Fake, a mais recente ameaça distópica**. Tradução de Gabriela Leite. Disponível em: https://outraspalavras.net/tecnologiaemdisputa/deep-fake-a-ultima-distopia/. Acesso em: 15 dez. 2025.

STRECK, Lenio Luiz. A constituição (ainda) dirigente e o direito fundamental a respostas corretas. **Revista do Instituto de Hermenêutica Jurídica**, Porto Alegre, n. 9, p. 267-287, 2008.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil: análise a partir do Marco Civil da Internet. **Pensar**, Fortaleza, v. 22, n. 1, p. 108–146, jan./abr. 2017. Disponível em: https://doi.org/10.5020/2317-2150.2017.v22n1p108. Acesso em: 12 maio 2025.

TEIXEIRA, Q. de S. Vulnerabilidade digital e a terceira idade. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 11, n. 9, p. 307–316, 2025. Disponível em: https://doi.org/10.51891/rease.v11i9.20876.

TEIXEIRA, Tarcísio. **Marco Civil da Internet comentado**. São Paulo: Almedina, 2016.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, São Paulo, v. 30, n. 86, p. 269–285, jan./abr. 2016. Disponível em: https://doi.org/10.1590/S0103-40142016.00100017. Acesso em: 12 maio 2025.

VALE, Karen Sanny Santos; COIMBRA, Stella Mácia Soares; OLIVEIRA, Igor do Vale. A Responsabilidade Civil dos Influenciadores Digitais pela divulgação de produtos e serviços nas redes sociais. **Revista Jurídica do Nordeste Mineiro**, [S.l.], v. 1, n. 1, 2023. Disponível em: https://jrnm.ojsbr.com/juridica/article/view/349. Acesso em: 15 dez. 2025.

WOJAHN et al. The social vulnerability of the elderly against scams in the digital scope. **Research, Society and Development**, [S. l.], v. 11, n. 11, p. e452111133652, 2022. DOI: 10.33448/rsd-v11i11.33652. Disponível em: https://rsdjournal.org/rsd/article/view/33652. Acesso em: 24 nov. 2025.

WOLKMER, Antônio Carlos (Org.). **Fundamentos do humanismo jurídico no Ocidente**. Barueri: Manole; Florianópolis: Fundação José Arthur Boiteux, 2005.