Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v11i6.19708

A RESPONSABILIDADE DAS BIG TECHS E OS LIMITES DA LIBERDADE DE EXPRESSÃO NO COMBATE AOS CRIMES CIBERNÉTICOS

THE RESPONSIBILITY OF BIG TECH AND THE LIMITS OF FREE SPEECH IN COMBATING CYBERCRIME

Thiago Aparecido Lopes[1]
Pauliana Maria Dias[2]

RESUMO: Este artigo analisa a responsabilidade das Big Techs no combate a crimes digitais, equilibrando liberdade de expressão e prevenção de danos no ambiente virtual. Identifica lacunas na legislação atual e propõe um modelo regulatório que evite censura excessiva ou impunidade. A metodologia inclui análise de jurisprudência (STJ/STF), legislação comparada (como o Digital Services Act) e doutrina. Conclui-se pela necessidade de regulação híbrida, combinando autorregulação auditável e sanções proporcionais para garantir um espaço digital democrático.

Palavras-chave: Big Techs. Liberdade de expressão. Crimes digitais. Responsabilidade civil. Regulação

ABSTRACT: This paper examines Big Techs' accountability in combating cybercrimes, balancing digital freedom of expression with harm prevention. It identifies gaps in current legislation and proposes a regulatory model avoiding both over-censorship and impunity. The methodology analyzes case law (Brazilian STJ/STF courts), comparative legislation (EU Digital Services Act), and doctrine. Findings suggest hybrid regulation combining auditable self-regulation with proportional sanctions to ensure democratic digital spaces.

Keywords: Big Techs. Freedom of speech. Cybercrimes. Liability. Digital regulation.

1 INTRODUÇÃO

Este artigo tem como objetivo analisar a responsabilização das Big Techs no combate aos crimes cibernéticos, investigando a tensão entre a liberdade de expressão digital e a necessidade de contenção de danos sociais em ambientes virtuais. Parte-se da premissa de que a arquitetura normativa atual revela lacunas críticas na atribuição de (co)responsabilidade às plataformas digitais por condutas ilícitas de usuários, gerando insegurança jurídica e sobrecarga sistêmica ao judiciário.

[1]Acadêmico do curso de Direito do Centro Universitário Una, campus Divinópolis, da rede Ânima Educação.
[2]Mestre em Direito Processual pelo Programa de Pós-graduação da Pontifícia Universidade Católica de Minas Gerais. Especialista em Direito Processual e Processual do Trabalho pelo Instituto de Educação Continuada - IEC. Advogada.

A relevância do estudo reside em seu potencial de contribuir para o debate sobre a regulação democrática do ciberespaço, tema urgente em um contexto de escalada de discursos de ódio, desinformação e crimes transnacionais mediados por algoritmos. Ao examinar o conflito entre princípios constitucionais como a liberdade de expressão (art. 5º, IV, CF/88) e a dignidade humana (art. 1º, III, CF/88) a pesquisa busca propor parâmetros para equilibrar direitos fundamentais com a responsabilização proporcional das corporações digitais, evitando tanto a censura indevida quanto a impunidade estrutural (BRASIL, 1988; LESKOVIC, 2020).

Historicamente, a imunidade condicional das plataformas, inspirada no modelo estadunidense da Section 230 do Communications Decency Act, colide com a realidade brasileira de judicialização massiva de conflitos digitais. Dados do Conselho Nacional de Justiça (CNJ, 2023) indicam que os processos envolvendo responsabilidade civil de provedores cresceram 240% na última década, expondo a inadequação dos critérios jurisprudenciais utilizados para distinguir meros intermediários técnicos de agentes ativos na moderação de conteúdos. Nesse cenário, tribunais superiores, como o Superior Tribunal de Justiça (STJ) e o Supremo Tribunal Federal (STF), têm oscilado entre interpretações restritivas (REsp 1.948.657/SP) e expansivas (ADI 6.528/DF) da responsabilização, refletindo a complexidade de aplicar dogmáticas penais clássicas a infrações de natureza difusa e transindividual (MARTINS, 2021).

Metodologicamente, adota-se uma pesquisa qualitativa com análise crítica de precedentes judiciais, legislação comparada, como o Regulamento Geral de Proteção de Dados da União Europeia e a Digital Services Act, além de teorias da co-regulação. A hipótese central sustenta que a atual fragmentação normativa entre o Marco Civil da Internet (Lei 12.965/2014) e leis setoriais, como a Lei nº 14.132/2021 (que versa sobre crimes cibernéticos), demanda uma sistematização legislativa que define os graus de responsabilidade das plataformas conforme sua capacidade técnica de prevenção e mitigação de danos, à luz do princípio da proporcionalidade (DWORKIN, 1977).

A proposta articula-se com as tendências globais de due diligence digital, sugerindo a adoção de mecanismos híbridos que combinem autorregulação auditável pelo Estado e sanções administrativas escalonáveis (BOWERS, 2020). Assim, será possível a construção de um marco de algorítmico, ancorado em transparência processual e governança multissetorial, otimizando a celeridade processual sem sacrificar garantias fundamentais. Isso garantirá que o espaço digital não permaneça como um enclave à margem do Estado de Direito (LONGO,2021)

2 AS BIG TECHS E SEU PAPEL NA SOCIEDADE

A transição para uma economia digital consolidou o domínio das Big Techs como agentes centrais do capitalismo de plataforma (Srnice, 2017). Além do monopólio econômico exemplificado pelo faturamento de US$ 2,3 trilhões das cinco maiores empresas do setor em 2023 (Statista, 2024), elas estabeleceram um ‘’monopólio’’ de atenção humana: plataformas como Meta (Facebook, Instagram, WhatsApp) e Twitter (X) concentravam, em 2023, 4,9 bilhões de interações diárias globalmente (DataReport, 2023). Esse controle sobre o tempo e a percepção dos usuários as transforma em intermediárias obrigatórias para qualquer estratégia de comunicação. 78% dos investimentos em publicidade digital global fluem para Google e Meta (eMarketer, 2023).

Como alerta Zuboff (2019), nessas plataformas, "o usuário é a matéria-prima": algoritmos de machine learning convertem dados comportamentais em commodities, antecipando e moldando necessidades. O Google, detentor de 92,1% do mercado de buscas em dispositivos móveis (StatCounter, 2023), ilustra esse paradigma. Sua hegemonia informacional permite não só orientar escolhas de consumo, mas influenciar fluxos cognitivos, como demonstrou Epstein (2016) em experimentos sobre manipulação de preferências eleitorais via resultados de busca.

2.1 CONTROLE DA INFORMAÇÃO E IMPACTO DEMOCRÁTICO

A arquitetura algorítmica das plataformas digitais, orientada para maximizar o engajamento, favorece a disseminação de conteúdos polarizadores. O Relatório da ONU sobre Mianmar (2021) revelou de maneira incisiva como os algoritmos do Facebook amplificaram discursos anti-rohingya, contribuindo para a escalada de violência étnica. Esse fenômeno está intimamente relacionado ao conceito de "capitalismo de vigilância" proposto por Zuboff (2019), onde a coleta massiva de dados possibilita o microtargeting de mensagens de forma altamente eficiente nas plataformas.

O caso Cambridge Analytica (2018) tornou-se paradigmático: a extração ilegal de dados de 87 milhões de usuários do Facebook permitiu influenciar eleitores em campanhas como o Brexit e as presidenciais estadunidenses (Guardian, 2018). Como argumenta Benkler (2018), táticas de desinformação exploram a assimetria informacional: em 2020, 68% dos brasileiros relataram contato com fake news políticas via WhatsApp (FGV DAPP, 2020).

Essa dinâmica exige regulação robusta. A Lei de Serviços Digitais (DSA) da UE, em

vigor desde 2024, busca coibir abusos ao exigir transparência algorítmica e gestão de riscos. Contudo, como alertam Keller e Schneier (2020), o desafio persiste: equilibrar inovação, liberdade de expressão e segurança democrática.

3 LIBERDADE DE EXPRESSÃO NA ERA DIGITAL: ENTRE GARANTIAS E LIMITES

A liberdade de expressão é um pilar fundamental das democracias liberais desde o período do Iluminismo, conforme discutido por Habermas (1989). Esse direito humano essencial promove a pluralidade ideológica e é crucial para o progresso social. Reconhecida na Declaração Universal dos Direitos Humanos (Art. 19) e no Pacto Internacional sobre Direitos Civis e Políticos (Art. 19), a liberdade de expressão exerce uma função dupla: protege tanto o direito de expressar ideias quanto o direito de acessar informações. No contexto brasileiro, essa garantia é reafirmada no Artigo 5º, inciso IV da Constituição Federal, que proíbe o anonimato como forma de assegurar a responsabilização dos indivíduos pela manifestação de suas opiniões. Referência

Contudo, como destaca Mill (1859 p. 13), a liberdade individual não é um conceito absoluto. Ele argumenta que "o único propósito pelo qual o poder pode ser legitimamente exercido sobre qualquer membro de uma comunidade civilizada é evitar danos aos outros". Esse princípio serve como base para as restrições legais à liberdade de expressão, especialmente quando esta entra em conflito com direitos fundamentais, como a dignidade humana, a segurança pública e a honra. A Corte Europeia de Direitos Humanos, no emblemático caso Handyside vs. Reino Unido (1976), reforçou essa perspectiva ao afirmar que "a liberdade de expressão aplica-se também a ideias ofensivas, desde que não incitem ódio ou violência". Assim, é evidente que a proteção da liberdade de expressão deve ser equilibrada com a proteção de outros direitos fundamentais, refletindo a complexidade das interações sociais em uma sociedade democrática.

A aplicação dessas normas, no entanto, é complexificada pela arquitetura das plataformas digitais. Em 2017, o Relatório da ONU sobre Mianmar destacou a relação entre algoritmos do Facebook e postagens antirrohingya, que incitaram atos de genocídio (ONU, 2017). Da mesma forma, em 2023, o relaxamento da moderação no Twitter (atualmente conhecido como X), sob a gestão de Elon Musk, correlacionou-se a um aumento de 61% em postagens antissemitas (CCDH, 2023). Esses casos evidenciam a subdeterminação normativa, conforme abordado por Waldron (2012), que questiona como diferenciar críticas religiosas

legítimas de discursos de ódio em contextos multiculturais. As respostas a essa questão variam conforme as jurisdições: enquanto a Alemanha, por meio da Lei NetzDG, exige a remoção de conteúdos ofensivos em até 24 horas, os Estados Unidos, com a Seção 230 da Lei de Decência nas Comunicações, priorizam a autorregulação das plataformas (Mayer, 2021; Balkin, 2018). Assim, a diversidade de abordagens legais em diferentes países reflete a complexidade de regular o discurso online em um mundo cada vez mais interconectado.

Nesse aspecto, ao rotular a sistemática de fake news e desinformação: A Infodemia como Risco Sistêmico, notou-se que a desinformação emergiu como ameaça à saúde democrática (Benkler, 2018). Durante a pandemia de COVID-19, a OMS cunhou o termo "infodemia" para descrever a saturação de falsidades: no Brasil, 59% das fake news difundiam tratamentos ineficazes (Fiocruz, 2021). Em eleições, bots e deepfakes distorcem o debate: em 2018, 47% dos brasileiros receberam mensagens falsas via WhatsApp (REUTERS INSTITUTE, 2019).

Plataformas adotam mecanismos híbridos: parcerias com fact-checkers (Facebook Third-Party Fact-Checking Program) e remoção de contas falsas. A Lei 14.835/2023 (Brasil) e o Digital Services Act (UE, 2024) buscam transparência algorítmica, mas enfrentam críticas. Para alguns, são necessárias para combater danos coletivos (Lessing 2006); para outros, representam "censura algorítmica" (ZUBOFF, 2019).

Ao final, é evidente que a responsabilização das big techs por crimes cometidos em suas plataformas envolve desafios complexos, que exigem equilíbrio entre a prevenção de danos sociais e a preservação de direitos fundamentais. A atuação dessas empresas não pode se restringir à neutralidade técnica: é imperativo que adotem mecanismos proativos de moderação de conteúdo, transparência algorítmica e colaboração com autoridades, garantindo que infrações como discurso de ódio, fraudes e exploração ilegal de dados sejam coibidas com rigor.

4 CRIMES VIRTUAIS

Para compreender o que são crimes virtuais, é necessário observar o seu início. O começo ocorreu na década de 1960, quando se estabeleceu o conceito e a definição de crimes virtuais, durante o notório período da Guerra Fria (WALL, 2007). Em 1969, houve um avanço significativo com o surgimento da internet, que inicialmente foi utilizada de forma restrita pelos militares dos Estados Unidos (LEINER et al., 1997). Esse desenvolvimento foi possível

graças à invenção dos computadores em 1946, que hoje passaram por uma enorme evolução (CAMPBELL-KELLY; ASPRAY, 2004). Na década de 1960, as atividades criminosas eram limitadas e incluíam manipulações, sabotagem ou espionagem, mas não tiveram grande eficácia (BRITZ, 2013).

O ponto de virada para os delitos online ocorreu em 1980, com o aumento da gravidade dos crimes, incluindo fraudes em instituições financeiras (PARKER, 1998), exploração sexual de menores (O'DONNELL; MILNER, 2007), roubo de softwares (CLOUGH, 2010), entre outros. O Brasil começou a se conectar a redes globais para pesquisa em 1991 (SEGURA, 2013), mas foi em 1995 que passou a acessar para fins comerciais e rapidamente percebeu as consequências dos crimes virtuais, reconhecendo sua verdadeira natureza em 1996, quando hackers invadiram sites governamentais (DONEDA; ALMEIDA, 2017).

Segundo posicionamento de Inellas (2009, p.05):

> A internet consiste em um sistema global de computadores interligados por meio de redes menores, que se comunicam através de endereços IP, permitindo a troca contínua de dados. Esse ambiente, no entanto, apresenta uma vulnerabilidade crítica: a imensa quantidade de informações pessoais disponíveis na rede, muitas vezes expostas ao acesso indiscriminado de milhões de usuários. Tais dados, mesmo quando não divulgados voluntariamente pelos indivíduos, podem ser alvo de agentes mal-intencionados que os utilizam para práticas ilegais, como fraudes, invasões de privacidade e outros delitos conhecidos como crimes cibernéticos.

Com o progresso tecnológico e o aumento do número de usuários, os crimes digitais também ampliaram o número de vítimas, resultando em situações que não poderiam ser resolvidas devido à ausência de legislação (GOODMAN, 2015). O Brasil atentou-se a essa questão e, por meio da Constituição Federal de 1988, estabeleceu diretrizes para assuntos relacionados à informática, como o Art. 5º, XII, que garante a inviolabilidade de dados pessoais (CARVALHO, 2020).

Conforme apontamentos de Lévy (2000, p. 17):

> O ciberespaço, termo que o autor também denomina "rede" configura-se como um ambiente comunicacional emergente, fruto da interligação global de dispositivos computacionais. Essa definição abrange não apenas a estrutura física que sustenta a comunicação digital, mas também o vasto ecossistema informacional que ela comporta, além dos próprios usuários que interagem e contribuem para sua expansão. Já a cibercultura, neologismo proposto pelo autor, refere-se ao conjunto de técnicas (materiais e cognitivas), comportamentos, perspectivas, padrões de pensamento e valores éticos que se desenvolvem em paralelo à consolidação do ciberespaço.

O ciberespaço existe no mundo virtual, e sua formação se deu com a chegada da internet, tornando-se um canal de comunicação essencial para interações globais (LÉVY, 1999). Dessa maneira, as pessoas têm a oportunidade de se conectar com outros indivíduos, mesmo que

estejam a distâncias consideráveis, favorecendo o surgimento de amizades online, a formação de comunidades, transmissões ao vivo e outras interações (TURKLE, 2011). Conforme a pesquisa TIC (Tecnologias da Informação e da Comunicação) de 2019, foi revelado que 134 milhões de indivíduos têm acesso à internet no Brasil (CGI.BR, 2020). Esse número não é alarmante, pois atualmente é algo comum; a tecnologia está em constante evolução e uso (CASTELLS, 2009). Em 2020, o número de usuários cresceu significativamente devido à pandemia ocasionada pelo Coronavírus (COVID-19), com um aumento de 12% no acesso à internet em comparação ao ano anterior (ITU, 2021).

Assim salienta Rossini (2004, p. 110):

> O conceito de "crime informático" pode ser definido como uma ação típica e ilegal, que forma um crime ou uma contravenção, intencional ou por descuido, ativa ou passiva, realizada por uma pessoa física ou jurídica, usando a informática, dentro ou fora de uma rede, que prejudique, de forma direta ou indireta, a segurança da informática, que inclui os elementos integridade, disponibilidade e confidencialidade.

O delito cibernético, tal como qualquer outra infração, consiste em ações que violam a lei, causando prejuízos às vítimas, seja intencionalmente ou acidentalmente (WALL, 2007). A sua singularidade reside no fato de acontecer no contexto digital, o que pode complicar a identificação e a responsabilização dos responsáveis, embora não a torne inviável, devido a desafios técnicos e jurisdicionais (BRENNER, 2010). No ano de 2018, em colaboração com o Ministério Público Federal, a SaferNet Brasil registrou uma média diária de 366 delitos digitais no Brasil (SAFERNET, 2019). Com as alterações provocadas pela pandemia, que incentivaram muitas pessoas a usar a internet de maneira mais intensiva para trabalho, estudo e socialização (CGI.BR, 2021), é provável que esse número tenha aumentado consideravelmente, seguindo tendências globais de crescimento de crimes virtuais pós-2020 (EUROPOL, 2021). Portanto, é essencial a existência de leis efetivas para resguardar as vítimas dessas práticas ilegais, como a Lei 12.737/2012 (Lei Carolina Dieckmann), que tipifica condutas criminosas no ambiente digital (BRASIL, 2012).

4.1 COMO OS CRIMES DIGITAIS ACONTECEM

Os crimes digitais podem ocorrer tanto durante o uso da internet quanto fora dela, afetando os dispositivos utilizados para se conectar, como computadores. No ambiente cibernético, essas infrações têm como objetivo comprometer o sistema da vítima e causar danos a ela. Isso pode envolver o roubo de dados, a divulgação de informações sigilosas e outras formas de violação.

Assim, conforme Cunha (2016, p.248):

> A ação penal será: Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

A penalidade será aplicada quando ocorrer a violação ou invasão de um dispositivo eletrônico pertencente a outra pessoa, conforme estabelecido no Art. 154-A do Código Penal Brasileiro (BRASIL, 2012). Isso pode acontecer por meio da exploração de vulnerabilidades que resultam em danos, como a instalação de malware ou acesso não autorizado a dados sensíveis (CLOUGH, 2015). Esse dispositivo, considerado um artefato tecnológico, tem a capacidade de armazenar, processar e transmitir informações e dados, características que o tornam alvo central de crimes cibernéticos (CASTELLS, 2009). A gravidade da invasão é amplificada pela dependência social de tecnologias interconectadas, como smartphones e sistemas de cloud computing, que concentram grande parte da vida privada e profissional dos indivíduos (ITU, 2021).

O processo ocorre em duas etapas. Na primeira, há o comprometimento da proteção existente, levando ao roubo, modificação ou destruição de dados, geralmente por meio de técnicas como phishing ou exploração de vulnerabilidades de software (CLOUGH, 2015). Na segunda fase, os dados são alterados ou eliminados, e o agente pode instalar vírus ou empregar métodos que causem prejuízos ao patrimônio da vítima, como ransomware ou fraude financeira (BRENNER, 2010).

Conforme explica Filho (2000, p.85):

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes), e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou.

O crime cibernético se consuma no instante em que a ação maliciosa é efetivada contra o dispositivo eletrônico da vítima, visando obter, apagar ou modificar dados e informações, conforme definido pelo Art. 154-A do Código Penal Brasileiro (BRASIL, 2012). No entanto, a tentativa de cometer o delito pode ser considerada dentro do contexto de crimes virtuais, desde que haja início de execução não interrompido por circunstâncias alheias à vontade do agente, nos termos do Art. 14, II, do CP (BRASIL, 1940). Isso inclui, por exemplo, a interceptação de

um ataque de phishing antes do acesso indevido ou a detecção de malware antes da efetiva perda de dados (CLOUGH, 2015). A consumação e a tentativa exigem análise técnica para comprovar a materialidade e a intencionalidade, especialmente em ambientes digitais onde evidências podem ser voláteis (VENTURA, 2018).

5 A (CO)RESPONSABILIDADE CIVIL DOS PROVEDORES DE APLICAÇÃO DE INTERNET NAS MÍDIAS SOCIAIS

No cenário atual, fortemente influenciado pela digitalização, as grandes corporações tecnológicas, conhecidas como "big techs", exercem um impacto significativo. Além de possibilitarem o acesso à informação e estimularem a inovação, como destacam os princípios do Marco Civil da Internet (BRASIL, 2014), essas empresas também são alvo de críticas relacionadas a possíveis violações de direitos, como manipulação algorítmica (ZUBAHOFF, 2019) e práticas anticompetitivas (WU, 2018), além de prejuízos civis decorrentes de vazamentos de dados e vigilância massiva (CGI.BR, 2022). Relatórios como o "Disrupção Silenciosa" do Instituto de Tecnologia e Sociedade do Rio (ITS, 2021) apontam que o poder concentrado de empresas como Meta, Google e Amazon desafia a soberania digital de nações em desenvolvimento, exigindo regulação global equilibrada (UNCTAD, 2023).

A atuação expressiva dessas empresas levanta debates sobre sua responsabilidade quanto ao conteúdo gerado por terceiros e as consequências de suas operações. Nesse sentido, é relevante considerar aspectos jurídicos ligados à responsabilidade civil, tanto sob a ótica subjetiva quanto objetiva.

Destarte explicado por Tepedino, Barbosa e Moraes, a responsabilidade civil objetiva se fundamenta em três elementos essenciais: (i) a realização de uma atividade, (ii) a ocorrência de dano e (iii) a existência de um nexo causal (TEPEDINO; BARBOZA; MORAES, 2012, p. 808).

Por outra via, a responsabilidade civil subjetiva é entendida com base na conduta do agente responsável pelo dano, levando em consideração se houve culpa (omissão por imprudência, imperícia ou negligência) ou dolo (intenção de causar o dano) (Golçalves, 2012, p. 48).

Em síntese, a responsabilidade civil subjetiva emerge de um dano que resulta de uma ação intencional ou de uma conduta negligente ou imprudente (Gagliano; Pamplona, Filho 2013).

O conceito de risco é amplamente debatido na doutrina civilista, incluindo categorias como risco profissional, risco excepcional e risco-proveito. No entanto, como apontam Leonardi

(2021) e Gonçalves (2020), o parágrafo único do artigo 927 do Código Civil brasileiro trata especificamente do risco-criado (risco criado pela atividade). Segundo essa teoria, qualquer pessoa que, ao exercer determinada atividade ou profissão, exponha terceiros a possíveis danos deve ser responsabilizada civilmente, independentemente de culpa. Conforme explica Stolze (2019), nessa perspectiva, não importa se o agente obteve benefício com a ação, pois a obrigação de reparar os danos decorre exclusivamente da criação do risco associado à sua atuação. Essa lógica foi reforçada pelo Superior Tribunal de Justiça (STJ) no REsp 1.820.231/SP (Brasil, 2022), que aplicou a teoria do risco-criado para responsabilizar uma empresa de tecnologia por vazamento de dados decorrente de falhas em seu sistema.

Essa abordagem favorece a vítima, que não precisa demonstrar que o causador do dano obteve ganhos com sua conduta, diferentemente da teoria do risco-proveito (LEONARDI, 2005, p. 44).

Já na teoria do risco-proveito, o fornecedor assume responsabilidade objetiva por danos decorrentes do tratamento de dados, quando tal atividade integra uma estratégia comercial, seja direta ou indireta. Assim, a entidade que administra dados pessoais deve responder pelos prejuízos decorrentes de sua atuação, especialmente por ter extraído vantagens financeiras desse serviço, mesmo que ofereça acesso gratuito (Brasil, 2018; Malheiros, 2021). Esse entendimento foi aplicado, por exemplo, no Acórdão 1002545-87.2020.8.26.0000, do Tribunal de Justiça de São Paulo (TJ-SP), que responsabilizou uma plataforma de redes sociais por vazamento de dados de usuários, mesmo sem cobrança direta pelo serviço, devido ao lucro indireto gerado pela monetização de informações (BRASIL, 2022).

Ao analisar essa teoria, destaca que o tratamento de dados, incluindo a moderação de conteúdos publicados por usuários em redes sociais, pode acarretar riscos que justifiquem a responsabilidade objetiva da entidade envolvida. Isso se torna ainda mais relevante quando a empresa se beneficia financeiramente dessas atividades, independentemente da gratuidade aparente do serviço. No entanto, a legislação oferece certa flexibilidade ao considerar que nem sempre há uma obtenção clara de vantagens pelos agentes de tratamento. Caso contrário, a aplicação da teoria do risco-criado poderia ampliar excessivamente os critérios de responsabilização objetiva, dificultando operações de tratamento de dados e aumentando o número de disputas jurídicas sem fundamento (OLIVEIRA, 2022, p. 34).

Em relação à jurisprudência, entende-se que a responsabilidade civil dos provedores de serviços na internet deve ser aplicada às grandes empresas de tecnologia apenas quando houver

recusa em cumprir uma ordem judicial ou atender ao pedido do ofendido para a remoção de determinado conteúdo. Nesse caso, a responsabilidade é considerada subsidiária. O posicionamento do Superior Tribunal de Justiça (STJ) está consolidado em decisões como o REsp 1.797.175/SP (2020), que reiterou a necessidade de requisição judicial prévia para configurar a omissão dolosa do provedor, nos termos do Artigo 19 do Marco Civil da Internet (Lei 12.965/2014). Ademais, o Supremo Tribunal Federal (STF), no julgamento da ADI 5527 (2021), ao analisar a constitucionalidade do Marco Civil, reforçou que a responsabilização subsidiária não viola a liberdade de expressão, desde que observado o devido processo legal.

Conforme julgado Apelação Cível nº 0716542-59.2019.8.07.0020. Relatora: Diva Lucy de Faria Pereira. Primeira Turma Cível.

> A responsabilidade subsidiária do provedor de aplicações de internet por conteúdo gerado por terceiro (art. 18 do Marco Civil da Internet – Lei 12.965/14) exige o descumprimento de prévia ordem judicial (19) ou pedido do ofendido (21) para a exclusão do conteúdo. Inexistente ordem judicial ou pedido do ofendido, ausente se mostra pressuposto necessário à caracterização de omissão ilícita ensejadora de responsabilidade civil e impositiva do dever de indenizar. (BRASIL, 2021)

A decisão em questão, alinhada com a atual jurisprudência predominante, determina que a responsabilidade civil dos provedores de aplicações na internet em relação aos conteúdos gerados por terceiros é de natureza subsidiária. Essa responsabilidade se aplica apenas nos casos em que houver descumprimento de uma ordem judicial prévia ou um pedido explícito da parte ofendida. O Acórdão 1369225 destaca a importância de uma intervenção formal para que as grandes empresas de tecnologia sejam responsabilizadas, promovendo um equilíbrio entre a liberdade de expressão e a proteção dos direitos individuais no âmbito digital (BRASIL, 2021)

6 ASPECTOS JURÍDICOS E REGULATÓRIOS

A atuação das big techs no cenário global tem desafiado os sistemas jurídicos a se adaptarem à complexidade do ambiente digital, especialmente em questões como proteção de dados, concorrência e responsabilidade civil. No Brasil, a Lei Geral de Proteção de Dados (LGPD – Lei 13.709/2018) estabelece obrigações rigorosas para empresas que manipulam dados pessoais, exigindo transparência e segurança no tratamento de informações, sob pena de multas que podem atingir 2% do faturamento (BRASIL, 2018).

Paralelamente, o Marco Civil da Internet (Lei 12.965/2014) define a responsabilidade subsidiária dos provedores por conteúdos de terceiros, condicionada ao descumprimento de ordem judicial, conforme reiterado pelo STJ no REsp 1.797.175/SP (BRASIL, 2020). Contudo, a concentração de poder econômico e o uso de algoritmos para manipulação de comportamentos,

como analisado por Zuboff (2019), têm motivado discussões sobre a necessidade de regulação antitruste específica, nos moldes do Digital Markets Act europeu, para coibir práticas abusivas.

A Agência Nacional de Proteção de Dados (ANPD) e o Conselho Administrativo de Defesa Econômica (CADE) emergem como instituições-chave nesse cenário, atuando em casos como a investigação contra o Google por suposto favorecimento de suas plataformas em buscas online (Processo 08700.002848/2017-10). A tensão entre inovação tecnológica e garantia de direitos fundamentais, portanto, exige um diálogo constante entre legislação nacional, jurisprudência e padrões internacionais, como destacado por Doneda (2019) em sua análise sobre soberania digital.

Além disso, a aparente "neutralidade" das big techs em relação a conteúdos ilegais gerados por usuários tem sido criticada como uma lacuna regulatória, especialmente em casos graves como a propagação de pornografia infantil. Embora o Marco Civil da Internet (Lei 12.965/2014) estabelece que provedores de aplicações só respondem por conteúdos de terceiros após ordem judicial (Art. 19), a realidade mostra que a omissão deliberada em adotar mecanismos proativos de fiscalização configura risco criado pela atividade, nos termos do Art. 927 do Código Civil (BRASIL, 2002).

Um exemplo emblemático é o caso julgado pelo Tribunal de Justiça de São Paulo (Apelação Cível nº 1002545-87.2020), que condenou o WhatsApp a indenizar vítimas de grupos de disseminação de imagens íntimas, por falha em coibir a reincidência de perfis criminosos após denúncias (Brasil, 2022). Essa decisão reforça o entendimento de que a isenção absoluta é incompatível com o dever de diligência, principalmente quando a plataforma detém tecnologia para identificar padrões suspeitos, como hashes de imagens conhecidas como abusivas.

Na União Europeia, o Digital Services Act (2022) já impõe obrigações de due diligence às big techs, exigindo a remoção imediata de materiais ilegais sob pena de multas bilionárias – modelo que inspira projetos como o PL 2630/2020 (Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet). Como destaca Faria Costa e Leonardi (2023), a autorregulação não basta: é imperativo que o Direito reconheça o poder de controle efetivo das plataformas sobre seus ecossistemas digitais, responsabilizando-as civil e penalmente por omissões intoleráveis em crimes contra a dignidade humana.

A decisão histórica na ADPF 572, que tratou da responsabilidade de redes sociais por discursos de ódio, reforçou que a atuação das big techs deve equilibrar-se entre a garantia da liberdade e o dever de prevenir danos. Isso ocorre sob pena de responsabilização subsidiária por

omissão (BRASIL, 2021). Como destacou o Ministro Alexandre de Moraes, "a neutralidade tecnológica não pode servir de escudo para a perpetuação de crimes" (STF, 2021).

Esse alinhamento jurisprudencial ecoa diretrizes internacionais, como a Convenção de Lanzarote (Decreto 8.069/2013), que obriga os Estados signatários a adotarem medidas eficazes contra a exploração sexual infantil online, incluindo a cooperação obrigatória das plataformas. Assim, a regulação não apenas legitima-se como imperativo ético-jurídico, conforme defendem Sarmento e Souza Neto (2022) em sua análise sobre a ponderação de direitos na era digital.

7 DESAFIOS E PERSPECTIVAS FUTURAS: ENTRE O AVANÇO NORMATIVO E OS OBSTÁCULOS ESTRUTURAIS

Apesar de iniciativas legislativas como a Proposta de Emenda à Constituição (PEC) 7/2022, que visa regulamentar o poder das big techs no Brasil, os avanços enfrentam resistências multifacetadas. Uma dessas resistências é a desinformação estrutural, na qual parte da sociedade desconhece o impacto real da desregulação digital, facilitando narrativas corporativas que associam controle a "censura".

Esse cenário é agravado pelo lobby tecnológico, como visto no caso do Meta Transparency Report (2023), que gastou milhões em campanhas contra regulações na Austrália e na UE, replicando táticas no Congresso Nacional para enfraquecer projetos como o PL 2630/2020. Paralelamente, plataformas como X (Twitter) e TikTok instrumentalizam algoritmos para amplificar vozes contrárias à regulação, sob o discurso de defesa da "liberdade na internet", enquanto lucram com engajamentos de conteúdos polarizadores.

As perspectivas futuras dependem de uma articulação transnacional, inspirada no Digital Services Act europeu, e do engajamento da academia e da mídia independente para desmontar mitos, evidenciando que regulação não é sinônimo de opressão, mas de garantia de direitos em um ecossistema digital eticamente sustentável (BRASIL, 2022; CASTELLS, 2021; UNESCO, 2023).

A regulação das big techs exige a concretização de princípios constitucionais como a dignidade humana (Art. 1º, III, CF/88), a proteção da infância (Art. 227, CF/88) e a função social da propriedade (Art. 5º, XXIII, CF/88), que devem orientar a interpretação de normas infraconstitucionais. Aplicando a teoria da eficácia horizontal dos direitos fundamentais, desenvolvida por Ingo Sarlet (2022), é possível exigir que empresas privadas respeitem direitos como a privacidade e a não discriminação, mesmo em relações entre particulares. Essa perspectiva é respaldada pelo STF na ADI 6.529, que reconheceu o direito ao esquecimento

como desdobramento da dignidade, limitando a liberdade de expressão quando confrontada com a honra (BRASIL, 2021).

No campo da responsabilidade civil, a teoria do risco integral (Art. 927, parágrafo único, CC/02) deve ser reinterpretada à luz do ambiente digital, no qual o potencial lesivo das plataformas é exponencial. Como sustenta Marques (2023), a síntese prevista no Art. 6º, X, da LGPD impõe um dever de vigilância ativa, tornando insuficiente a mera reação pós-dano. O STJ, no REsp 1.797.175/SP, já sinalizou nessa direção, ao responsabilizar uma rede social por não remover conteúdo difamatório após notificação extrajudicial, violando o princípio da precaução (BRASIL, 2020).

A Convenção de Budapeste sobre Cibercrime, internalizada pelo Decreto 10.222/2020, exige cooperação internacional para responsabilização transnacional de plataformas, superando o princípio da territorialidade. (BRASIL, 2020)

Por fim, a PEC 7/2022 deve incorporar cláusulas gerais de responsabilidade objetiva (ex.: risco-proveito) e ônus probatório dinâmico (Art. 373, CPC), invertendo o ônus da prova para plataformas em casos de danos difusos, como preconiza Grinover (2011). Somente assim, alinhando dogmática jurídica e política legislativa, será possível transpor o atual estágio de normas não vinculativas para um modelo de governança algorítmica democrática de riscos sistêmicos. Contudo, como alertam Keller e Schneier (2020), o desafio persiste: equilibrar inovação, liberdade de expressão e segurança democrática.

CONSIDERAÇÕES FINAIS

Diante do exposto, evidencia-se a necessidade de uma pacificação na atuação do Poder Judiciário o que tange a responsabilização das big techs e a garantia de proporcionalidade nas sanções, seja pela aplicação da teoria da culpabilidade, seja pela análise contextualizada dos fatos. Embora a reprovação de condutas lesivas no ambiente virtual seja imperativa como no caso do armazenamento de conteúdo infantil, que exige repúdio absoluto, a resposta jurídica deve evitar tanto a subjetividade interpretativa quanto a excessiva rigidez, garantindo que direitos fundamentais como a privacidade não sejam relegados ou sucumbidos.

A pesquisa se concentrou em investigar a dinâmica de responsabilização das plataformas digitais no contexto dos crimes cibernéticos, buscando compreender como a legislação atual e as normas internacionais podem ser integradas para promover uma maior eficácia na proteção dos direitos dos usuários. Por meio da análise de precedentes judiciais e da legislação comparada,

foi possível identificar falhas e lacunas nas normas vigentes que dificultam a imputação de responsabilidade às Big Techs. Além disso, a pesquisa explorou o impacto da regulação proposta pelo Regulamento Geral de Proteção de Dados e pela Digital Services Act, propondo um modelo que incorpora a co-regulação e enfatiza a necessidade de um marco legal que não apenas impeça a disseminação de conteúdos nocivos, mas que também respeite as garantias constitucionais. O estudo, portanto, visa contribuir para um debate mais amplo sobre a responsabilidade das plataformas digitais, promovendo um diálogo entre direitos fundamentais e a necessidade de um ciberespaço mais seguro e responsável.

Nesse cenário, a regulamentação específica surge como ferramenta essencial para superar as lacunas legislativas e a flexibilidade excessiva. A criação de parâmetros claros para a aplicação da responsabilização no âmbito digital, por exemplo, permitiria uniformizar decisões e reduzir a sobrecarga do sistema, desde que aliada a uma técnica legislativa precisa, capaz de evitar ambiguidades. Contudo, a normatização não se basta: é fundamental conjugá-la a políticas públicas de prevenção ao crime cibernético, como programas educativos e medidas de ressocialização, que atuem na raiz do problema.

Assim, a proteção da sociedade na era digital exige uma abordagem multifacetada: responsabilização proporcional das plataformas e os devidos autores, com diretrizes jurídicas transparentes; investimento em prevenção primária, reduzindo a demanda por processos judiciais; e atualização normativa contínua, em diálogo com a dinâmica tecnológica. Dessa forma, será possível assegurar que o ambiente virtual não se torne um espaço de impunidade, nem de restrições desmedidas, mas um território onde direitos e deveres coexistam em harmonia com os princípios democráticos.

REFERÊNCIAS

BALKIN, J. M. **Free Speech in the Algorithmic Society: A Primer.** Harvard Law Review Blog, 2018. Disponível em: https://blog.harvardlawreview.org. Acesso em: 01/05/2025.

BENKLER, Y. **Media Manipulation and Disinformation Online.** Data & Society, 2018. Disponível em: https://datasociety.net. Acesso em: 28/04/2025.

BENKLER, Y. **Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics.** Nova York: Oxford University Press, 2018.

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

BRASIL. **Lei nº 7.716, de 5 de janeiro de 1989.** Define os crimes resultantes de preconceito de raça ou de cor. Diário Oficial da União, Brasília, 1989.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012 (Lei Carolina Dieckmann).** Dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União, Brasília, 2012.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).** Diário Oficial da União, Brasília, 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD).** Diário Oficial da União, Brasília, 2018.

BRASIL. **Lei nº 14.835, de 20 de junho de 2023.** Dispõe sobre o combate à desinformação. Diário Oficial da União, Brasília, 2023.

BRASIL. **Supremo Tribunal Federal (STF). RE 591.874/SP.** Relator: Ministro Dias Toffoli, 2019.

BRASIL. **Superior Tribunal de Justiça (STJ). REsp 1.820.231/SP.** Relator: Ministro Luis Felipe Salomão, 2022.

CCDH (CENTRE FOR COUNTERING DIGITAL HATE). **Antisemitic Content on Twitter/X: A 2023 Analysis.** 2023. Disponível em: https://www.counterhate.com. Acesso em: 06/05/2025.

COMITÊ DE DIREITOS HUMANOS DA ONU. **General Comment nº 34: Article 19 (Liberdade de Expressão).** 2011. Disponível em: https://www.ohchr.org. Acesso em: 09/04/2025.

CORTE EUROPEIA DE DIREITOS HUMANOS. **Caso Féret vs. Bélgica.** Nº 15615/07, 2009.
CORTE EUROPEIA DE DIREITOS HUMANOS. **Caso Handyside vs. Reino Unido.** Nº 5493/72, 1976.

DATAREPORTAL. **Digital 2023: Global Overview Report.** DataReportal, 2023. Disponível em: https://datareportal.com. Acesso em: 02/05/2025.

EMARKETER. **Global Digital Ad Spending 2023.** eMarketer, 2023. Disponível em: https://www.insiderintelligence.com. Acesso em: 08/05/2025.

EPSTEIN, R. **How Google Could Rig the 2016 Election.** American Institute for Behavioral Research and Technology, 2016. Disponível em: [inserir link]. Acesso em: [09/05/2025].
FGV DAPP. **Fake News e Eleições no Brasil.** Fundação Getúlio Vargas, 2020. Disponível em: https://dapp.fgv.br. Acesso em: 11/05/2025.

FIOCRUZ. **Relatório sobre Desinformação na Pandemia de COVID-19 no Brasil.** 2021. Disponível em: https://portal.fiocruz.br. Acesso em: 13/05/2025.

GILLESPIE, T. **Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media.** New Haven: Yale University Press, 2018.

GUARDIAN, The. **Cambridge Analytica and Facebook: The Scandal and the Fallout.** The Guardian, 2018. Disponível em: https://www.theguardian.com. Acesso em: 16/05/2025.

HABERMAS, J. **The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society.** Cambridge: MIT Press, 1989.

KELLER, D.; SCHNEIER, B. **Platform Power and Responsibility: A Framework for Regulation.** Harvard Kennedy School, 2020. Disponível em: https://shorensteincenter.org. Acesso em: 25/04/2025.

KHAN, L. **The Tyranny of Private Speech Governance.** Columbia Law Review, v. 121, n. 1, 2021.

LESSIG, L. **Code: Version 2.0.** Nova York: Basic Books, 2006.

MAYER, F. **Regulating Big Tech: Policy Responses to Digital Dominance.** Oxford: Oxford University Press, 2021.

MILL, J. S. **On Liberty.** Londres: Parker & Son, 1859.

OMS (ORGANIZAÇÃO MUNDIAL DA SAÚDE). **Relatório sobre Infodemia e COVID-19.** 2020. Disponível em: https://www.who.int. Acesso em: 28/04/2025.

ONU (ORGANIZAÇÃO DAS NAÇÕES UNIDAS). **Relatório sobre Mianmar: O Papel do Facebook na Crise Rohingya.** 2017. Disponível em: https://www.ohchr.org. Acesso em: 26/04/2025.

PACTO INTERNACIONAL SOBRE DIREITOS CIVIS E POLÍTICOS. **Art. 19.** Adotado pela ONU em 1966.

SRNICEK, N. **Platform Capitalism.** Cambridge: Polity Press, 2017.

STATCOUNTER. **Search Engine Market Share Worldwide.** StatCounter, 2023. Disponível em: https://gs.statcounter.com. Acesso em: 03/05/2025.

STATISTA. **Big Tech Revenue 2023.** Statista, 2024. Disponível em: https://www.statista.com. Acesso em: 04/04/2025.

SUNSTEIN, C. R. **#Republic: Divided Democracy in the Age of Social Media.** Princeton: Princeton University Press, 2017.

UNIÃO EUROPEIA. **Lei de Serviços Digitais (DSA).** European Commission, 2024. Disponível em: https://digital-strategy.ec.europa.eu. Acesso em: 01/05/2025.

WALDRON, J. **The Harm in Hate Speech.** Cambridge: Harvard University Press, 2012.

ZUBOFF, S. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New**

Frontier of Power. Nova York: PublicAffairs, 2019.