

IX ENCONTRO VIRTUAL DO CONPEDI

**DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS
II**

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydêe Dal Farra Napolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFRSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Ednilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Educação Jurídica

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR

Prof. Dr. Rubens Beçak - USP - SP

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - MS

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial

Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG

Prof. Dr. Rogério Borba - UNIFACVEST - SC

D597

Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Clarisse Inês de Oliveira; Valter Moura do Carmo – Florianópolis: CONPEDI, 2026.

Inclui bibliografia

ISBN: 978-65-5274-591-0

Modo de acesso: www.conpedi.org.br em publicações

Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Direito. 3. Governança e novas tecnologias. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34



IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

APRESENTAÇÃO

Entre os dias 22 e 26 de junho de 2026, o Conselho Nacional de Pesquisa e Pós-Graduação em Direito realizou o IX Encontro Virtual do CONPEDI, que teve como tema “Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos”. Com a Instituição Toledo de Ensino de Bauru como parceira institucional, o evento reuniu pesquisadoras, pesquisadores, docentes e discentes vinculados a instituições de ensino e programas de pós-graduação de diferentes regiões do país, proporcionando um amplo espaço de apresentação, discussão e circulação da produção científica jurídica.

A programação, composta por palestra científica, painéis, Grupos de Trabalho de artigos e Grupos de Trabalho de pôsteres, permitiu o exame de temas relacionados aos desafios sociais, institucionais e democráticos que marcam o atual cenário jurídico. Ao favorecer o intercâmbio entre pesquisadores com distintas formações e perspectivas teóricas, o Encontro reafirmou a importância da pesquisa jurídica para a compreensão das transformações pelas quais passam o Estado, as instituições e as relações sociais.

Nesse contexto, o Grupo de Trabalho “Direito, Governança e Novas Tecnologias II”, coordenado por Clarisse Inês de Oliveira e Valter Moura do Carmo, reuniu dezenove trabalhos que discutiram os impactos da digitalização e da inteligência artificial sobre o Direito, a Administração Pública, o sistema de justiça, a democracia e o exercício dos direitos fundamentais.

Administração Pública, especialmente em atividades relacionadas à implementação de políticas públicas e à concessão de benefícios. O autor sustentou que o monitoramento e a avaliação não devem ocupar posição meramente gerencial, mas constituir mecanismos permanentes de preservação da legalidade, da accountability e da legitimidade democrática das decisões estatais automatizadas.

Na sequência, o artigo “Letramento digital na assessoria jurídica popular: introduzindo noções de algoritmo e inteligência artificial aos assistidos do Núcleo de Prática Jurídica”, de Clarisse Inês de Oliveira e Patrícia Garcia dos Santos, tratou da necessidade de promover o letramento digital dos jurisdicionados atendidos pelos Núcleos de Prática Jurídica. As autoras destacaram que o conhecimento mínimo acerca do funcionamento dos algoritmos e dos limites do emprego da inteligência artificial na advocacia e no Poder Judiciário constitui condição para uma participação consciente dos assistidos na condução de suas demandas.

O trabalho “Inclusão digital e serviços notariais: limites e potencialidades da plataforma e-Notariado à luz do constitucionalismo digital”, de Lígia Maria Silva Quaresma e José Carlos Francisco dos Santos, analisou a digitalização dos serviços notariais e as dificuldades enfrentadas pelos usuários da plataforma e-Notariado. Os autores compreenderam a inclusão digital como direito instrumental ao exercício da cidadania e de outros direitos, destacando a necessidade de ações de capacitação, particularmente em favor das pessoas idosas e daquelas que se encontram em situação de vulnerabilidade.

Em “Hermenêutica algorítmica e o dever de fundamentação das decisões judiciais”, Marcos Vinicius Conaciani de Souza e Flávio Luís de Oliveira investigaram a compatibilidade entre o emprego de sistemas algorítmicos no processo decisório judicial e o dever constitucional de fundamentação. Os autores defenderam que o uso dessas ferramentas deve ser acompanhado de mecanismos de transparência, explicabilidade e auditabilidade, além de um regime de responsabilidade compartilhada entre magistrados, tribunais e desenvolvedores.

decisões automatizadas sobre os direitos da personalidade, a privacidade, a igualdade e a autonomia informacional. O estudo questionou a suficiência dos modelos tradicionais de responsabilidade civil para o enfrentamento dos riscos algorítmicos e ressaltou a importância da supervisão humana, da prevenção de danos e da rastreabilidade das decisões.

As repercussões das novas tecnologias sobre a democracia e o processo eleitoral foram objeto do trabalho “Deep fakes e os riscos à democracia no contexto eleitoral: análise da insuficiência do ordenamento jurídico brasileiro e das alternativas regulatórias”, de Luiz Felipe de Farias Leite Borges e Glaucia Maria de Araújo Ribeiro. Os autores analisaram a capacidade dos conteúdos sintéticos de manipular a opinião pública e comprometer a integridade eleitoral, propondo uma resposta regulatória que articule atuação estatal, responsabilidade das plataformas e instrumentos tecnológicos de transparência e rastreabilidade.

Em “Golpe do ‘falso advogado’: estelionato digital, responsabilidade institucional e os limites da publicidade processual na era do processo eletrônico”, Murillo Silva da Rosa e Catarina Ribeiro Bragança Marques examinaram uma modalidade de fraude baseada na utilização de dados verdadeiros retirados de processos judiciais eletrônicos. O artigo discutiu a tensão entre publicidade processual e proteção de dados pessoais, bem como as responsabilidades dos tribunais e das instituições diante de golpes que atingem, sobretudo, pessoas idosas e outros indivíduos em situação de vulnerabilidade.

A proteção da infância no ambiente digital foi discutida no artigo “ECA Digital e monetização algorítmica da infância: governança de plataformas, proteção integral e responsabilidade digital”, de Andre Canuto Bezerra e Júlia Terra Nova dos Santos. Os autores abordaram a conversão da imagem, da rotina e dos dados de crianças e adolescentes em ativos econômicos, questionando se o ECA Digital oferece instrumentos suficientes para enfrentar o sharenting comercial, a publicidade direcionada, o impulsionamento pago e os sistemas de recomendação que favorecem a exploração econômica da exposição infantil.

Em “Controle e consumo na era digital: explorando o regime da informação no capitalismo através das perspectivas de Byung-Chul Han”, Andrezza Damasceno Machado, Felipe Ryuji Coimbra Miyamoto e Felipe Yasuhiro Mira Coimbra Miyamoto analisaram as transformações do capitalismo digital a partir dos conceitos de psicopolítica e infocracia. Os autores refletiram sobre a forma como a coleta e o tratamento de dados permitem influenciar comportamentos, orientar o consumo e produzir uma percepção de liberdade inserida em estruturas cada vez mais sofisticadas de controle.

O artigo “Constitucionalismo digital e equidade algorítmica: como combater os efeitos discriminatórios decorrentes do (mau) uso da inteligência artificial”, de Gabriella do Carmo Pantoja Duarte, abordou a reprodução de padrões discriminatórios por sistemas de inteligência artificial treinados com bases de dados enviesadas. A autora ressaltou que a alimentação humana dos sistemas pode perpetuar estereótipos e desigualdades históricas, razão pela qual defendeu mecanismos de rastreabilidade, supervisão humana, auditabilidade, explicabilidade e avaliação de impactos.

Em “Inteligência artificial: capitalismo de plataforma, desafios éticos e regulatórios no Brasil contemporâneo”, Irineu Francisco Barreto Junior discutiu a inteligência artificial no contexto do capitalismo de plataforma e da Sociedade da Informação. O estudo abordou a monetização de dados, a vigilância digital, as bolhas informacionais, a opacidade algorítmica e seus efeitos sobre a democracia, a privacidade e a autodeterminação informativa, defendendo a construção de parâmetros éticos e de um modelo regulatório policêntrico.

O trabalho “Chatbots sonham com advogados elétricos? Sobre regulamentação da inteligência artificial no contexto de crítica social”, de Bruno Gadelha Xavier e Amanda Schmid, examinou casos envolvendo interações entre usuários vulneráveis e sistemas automatizados de conversação. Os autores analisaram falhas dos mecanismos de segurança diante de sinais de sofrimento psicológico, automutilação e comportamento suicida, discutindo as dificuldades de imputação de responsabilidade civil e penal às empresas

No trabalho “A metamorfose do mediador judicial na Justiça 4.0: vulnerabilidade, datificação e democracia”, Juliana de Oliveira Sampaio Souto Queiroga e José Alexandre Ricciardi Sbizzera analisaram criticamente os efeitos da digitalização sobre a mediação judicial. Os autores destacaram que a submissão da atividade a metas, métricas e protocolos padronizados pode converter o mediador em gestor de fluxos institucionais, comprometendo as dimensões ética, relacional e democrática da mediação, particularmente em conflitos familiares marcados por vulnerabilidades.

Em “A memória de Funes: do direito ao esquecimento à gradação de remédios contra a hiperexposição algorítmica”, Thamires Ribas Lopes Smith, Rodrigo Plack Ferreira e Cláudio Augusto Diana Terra partiram do conto de Jorge Luis Borges para refletir sobre uma sociedade digital que registra e recupera indefinidamente acontecimentos da vida das pessoas. À luz do Tema 786 do Supremo Tribunal Federal, o estudo examinou os instrumentos jurídicos que permanecem disponíveis contra a circulação desproporcional e descontextualizada de informações, propondo uma gradação entre contextualização, desindexação e exclusão.

O artigo “Inclusão e exclusão digital no Brasil: o papel ambivalente da conectividade e novas tecnologias no acesso ao Direito”, de Jamerson Lima dos Santos, abordou as diferentes dimensões da exclusão digital e seus efeitos sobre o exercício da cidadania e o acesso à justiça. O autor demonstrou que a simples disponibilização de serviços digitais não assegura acesso efetivo, sobretudo quando persistem obstáculos relacionados à infraestrutura, ao custo da conectividade e à ausência de habilidades para utilização das tecnologias.

Encerrando o conjunto de pesquisas, o trabalho “A possibilidade do desenvolvimento da ação comunicativa entre adolescentes na era digital”, de Samira Bonfim Bernardi, analisou as relações comunicativas estabelecidas por adolescentes nas plataformas digitais a partir da teoria de Jürgen Habermas e do princípio da proteção integral. A autora reconheceu que esses ambientes ampliam as possibilidades de expressão e participação, mas observou que a

As discussões também evidenciaram a ambivalência que acompanha as novas tecnologias. Os mesmos instrumentos capazes de ampliar a eficiência administrativa, facilitar o acesso a serviços e favorecer a circulação de informações podem aprofundar desigualdades, reproduzir discriminações, intensificar formas de controle e expor a pessoa a riscos ainda não inteiramente alcançados pelas categorias jurídicas tradicionais. Essa constatação afasta tanto a aceitação acrítica da inovação quanto sua rejeição automática, impondo uma análise atenta aos contextos em que as tecnologias são desenvolvidas e utilizadas.

Os coordenadores agradecem aos autores pela qualidade das pesquisas apresentadas e pela contribuição aos debates realizados durante o Grupo de Trabalho. É necessário um agradecimento especial à monitora do Grupo de Trabalho, Maria Eduarda, pela dedicação, organização e apoio prestado durante a condução das apresentações e dos debates.

Espera-se que os artigos reunidos nestes anais contribuam para o aprofundamento das reflexões sobre Direito, governança e novas tecnologias e para a formulação de respostas institucionais que permitam aproveitar os benefícios da inovação sem desconsiderar os riscos que ela pode representar para a dignidade humana, a igualdade, a democracia e os direitos fundamentais.

Boa leitura!

Profa. Dra. Clarisse Inês de Oliveira

Universidade Federal Fluminense

Prof. Dr. Valter Moura do Carmo

Escola Superior da Magistratura Tocantinense (ESMAT)

**DEEP FAKES E OS RISCOS À DEMOCRACIA NO CONTEXTO ELEITORAL:
ANÁLISE DA INSUFICIÊNCIA DO ORDENAMENTO JURÍDICO BRASILEIRO E
DAS ALTERNATIVAS REGULATÓRIAS**

**DEEPFAKES E RISCOS À DEMOCRACIA NO CONTEXTO ELEITORAL: A
INSUFICIÊNCIA DO ORDENAMENTO JURÍDICO BRASILEIRO DIANTE DA
DESINFORMAÇÃO DIGITAL**

**Luiz Felipe de Farias Leite Borges ¹
Glaucia Maria de Araújo Ribeiro**

Resumo

O avanço das tecnologias de inteligência artificial generativa ampliou significativamente a capacidade de produção e disseminação de conteúdos sintéticos, especialmente os chamados deepfakes, gerando novos desafios para a proteção da democracia e dos direitos fundamentais no ambiente digital. Nesse contexto, o presente artigo analisa os impactos jurídicos e democráticos decorrentes da utilização de deepfakes em cenários de desinformação digital, com ênfase nos riscos ao processo eleitoral e na insuficiência do ordenamento jurídico brasileiro diante da velocidade de circulação desses conteúdos. A pesquisa possui natureza qualitativa, desenvolvida a partir de revisão bibliográfica e análise normativa, com enfoque na Constituição Federal, no Marco Civil da Internet e na Lei Geral de Proteção de Dados. O estudo demonstra que os mecanismos jurídicos atualmente existentes apresentam limitações estruturais, especialmente por estarem predominantemente orientados à reparação posterior do dano, revelando dificuldades na adoção de respostas preventivas eficazes. Além disso, verifica-se que a rápida evolução das ferramentas de inteligência artificial amplia os riscos de manipulação da opinião pública e de comprometimento da integridade democrática, sobretudo em períodos eleitorais. Ao final, propõe-se a adoção de um modelo regulatório híbrido, baseado na articulação entre atuação estatal, responsabilidade das plataformas digitais e utilização de mecanismos tecnológicos de transparência e rastreabilidade, com o objetivo de fortalecer a proteção dos direitos fundamentais sem inviabilizar a liberdade de expressão e a inovação tecnológica.

resulting from the use of deepfakes in scenarios of digital disinformation, with emphasis on the risks posed to electoral processes and on the insufficiency of the Brazilian legal system in addressing the rapid circulation of such content. The research adopts a qualitative approach, developed through bibliographic review and normative analysis, focusing on the Federal Constitution, the Brazilian Civil Rights Framework for the Internet and the General Data Protection Law. The study demonstrates that the legal mechanisms currently available present structural limitations, especially because they are predominantly oriented toward post-damage reparation, revealing difficulties in adopting effective preventive responses. Furthermore, the rapid evolution of artificial intelligence tools increases the risks of public opinion manipulation and the compromise of democratic integrity, particularly during electoral periods. Finally, the article proposes the adoption of a hybrid regulatory model based on the articulation between state action, platform responsibility and technological mechanisms of transparency and traceability, aiming to strengthen the protection of fundamental rights without undermining freedom of expression and technological innovation.

Keywords/Palabras-claves/Mots-clés: Deepfakes, Artificial intelligence, Digital disinformation, Democracy, Regulation

1 INTRODUÇÃO

O desenvolvimento recente das tecnologias de inteligência artificial, especialmente aquelas voltadas à geração de conteúdos sintéticos, têm produzido impactos significativos nas estruturas sociais, comunicacionais e jurídicas contemporâneas. Dentre essas inovações, destacam-se os chamados *deepfakes*, conteúdos audiovisuais manipulados por algoritmos capazes de simular, com elevado grau de verossimilhança, a imagem, a voz ou o comportamento de indivíduos reais. Tal fenômeno intensifica a complexidade do ambiente informacional contemporâneo, na medida em que dificulta a distinção entre conteúdos autênticos e artificiais.

A evolução acelerada dessas tecnologias, impulsionada pelo avanço dos modelos de inteligência artificial generativa, amplia exponencialmente os riscos associados à desinformação digital. Em períodos eleitorais, tais riscos assumem especial relevância, uma vez que a circulação de conteúdos manipulados pode influenciar a formação da opinião pública, comprometer a lisura do processo eleitoral e fragilizar a confiança nas instituições democráticas. A utilização de *deepfakes* no contexto político potencializa a disseminação de informações falsas com aparência de veracidade, dificultando sua identificação e mitigação em tempo adequado.

Para além dos impactos coletivos, observa-se também a incidência direta sobre direitos fundamentais, como a honra, a imagem e a privacidade. Nesse cenário, evidencia-se uma tensão crescente entre a liberdade de expressão e a necessidade de proteção contra abusos decorrentes do uso indevido da tecnologia. Tal tensão revela limites importantes do ordenamento jurídico, especialmente diante da velocidade com que as inovações tecnológicas se desenvolvem, em contraste com o caráter historicamente mais lento e reativo das respostas jurídicas.

O ordenamento jurídico brasileiro dispõe de instrumentos relevantes para a tutela desses direitos, a exemplo da Constituição Federal de 1988, do Marco Civil da Internet e da Lei Geral de Proteção de Dados. Todavia, tais mecanismos mostram-se, em grande medida, insuficientes diante das especificidades dos deep fakes. Isso ocorre porque, em sua maioria, operam de forma posterior à ocorrência do dano, revelando-se incapazes de prevenir a disseminação inicial de conteúdos manipulados, especialmente em ambientes digitais caracterizados pela alta velocidade de propagação da informação.

Nesse contexto, emerge não apenas uma lacuna normativa, mas também uma limitação estrutural do modelo jurídico tradicional, que privilegia a reparação em detrimento da

prevenção. A ausência de mecanismos eficazes de atuação preventiva contribui para a ampliação dos riscos sistêmicos associados aos deep fakes, inclusive com potencial de impacto sobre a própria estabilidade do ordenamento jurídico e a integridade do regime democrático, sobretudo em anos eleitorais.

Diante desse cenário, o presente artigo busca responder ao seguinte problema de pesquisa: em que medida o ordenamento jurídico brasileiro é suficiente para enfrentar os riscos decorrentes da disseminação de deep fakes no contexto eleitoral, especialmente considerando a ausência de mecanismos preventivos eficazes? Parte-se da hipótese de que os instrumentos jurídicos atualmente disponíveis mostram-se insuficientes para lidar com a complexidade e a velocidade desse fenômeno, exigindo a construção de soluções regulatórias mais integradas e orientadas à prevenção.

O objetivo geral do trabalho consiste em analisar criticamente os limites do ordenamento jurídico brasileiro no enfrentamento dos deep fakes, com especial atenção aos riscos ampliados em períodos eleitorais, bem como propor alternativas regulatórias capazes de mitigar tais impactos sem comprometer a liberdade de expressão. Para tanto, adota-se uma metodologia de natureza qualitativa, com abordagem dedutiva, baseada na análise bibliográfica e documental, incluindo legislação nacional e referenciais teóricos relevantes.

Para o desenvolvimento da pesquisa, o artigo está estruturado em três seções. Inicialmente, examina-se o fenômeno dos deep fakes, seu funcionamento e seus impactos na desinformação digital. Em seguida, analisa-se a resposta do ordenamento jurídico brasileiro, com ênfase na proteção dos direitos fundamentais e nas limitações dos mecanismos atualmente existentes. Por fim, discutem-se alternativas regulatórias possíveis, com a proposição de um modelo jurídico que privilegie mecanismos preventivos e preserve o equilíbrio entre liberdade de expressão e proteção da democracia.

2 DEEP FAKES E DESINFORMAÇÃO DIGITAL

O avanço das tecnologias de inteligência artificial tem promovido transformações significativas na forma como a informação é produzida, disseminada e consumida na sociedade contemporânea. Nesse cenário, a emergência dos chamados deep fakes representa um marco relevante, ao introduzir novas possibilidades de manipulação de conteúdos audiovisuais com elevado grau de sofisticação. Tais tecnologias não apenas ampliam os desafios relacionados à veracidade da informação, como também reconfiguram as dinâmicas da desinformação digital, especialmente em ambientes caracterizados pela rápida circulação de conteúdos, como as plataformas online.

A análise dos deep fakes exige, portanto, uma abordagem que considere simultaneamente seus fundamentos tecnológicos e suas implicações sociais e jurídicas. Nesse contexto, torna-se essencial compreender o funcionamento dessas ferramentas, bem como seus impactos na intensificação da desinformação e nos riscos associados ao processo democrático, em especial em períodos eleitorais, nos quais a manipulação informacional pode produzir efeitos relevantes sobre a formação da opinião pública.

2.1 Conceito e funcionamento dos deep fakes

Os chamados deep fakes constituem uma das mais recentes aplicações da inteligência artificial generativa, sendo caracterizados pela produção de conteúdos audiovisuais sintéticos capazes de reproduzir, com elevado grau de verossimilhança, a imagem, a voz e os comportamentos de indivíduos reais. O termo decorre da combinação entre “deep learning”, técnica de aprendizado profundo baseada em redes neurais artificiais, e “fake”, indicando a natureza artificial dos conteúdos produzidos.

Do ponto de vista técnico, os deep fakes são desenvolvidos, em grande medida, por meio de modelos generativos, especialmente redes adversariais generativas (Generative Adversarial Networks – GANs), que operam a partir da interação entre dois sistemas: um gerador, responsável pela criação de conteúdos sintéticos, e um discriminador, incumbido de avaliar sua autenticidade. Esse processo iterativo permite o aprimoramento contínuo dos resultados, tornando os conteúdos progressivamente mais realistas e difíceis de serem identificados como falsos.

A evolução dessas tecnologias tem sido acompanhada pela ampliação do acesso às ferramentas de criação, muitas vezes disponibilizadas por meio de plataformas digitais de fácil utilização. Essa democratização do uso da inteligência artificial contribui para a disseminação dos deep fakes em larga escala, reduzindo barreiras técnicas e permitindo sua utilização por indivíduos sem conhecimento especializado.

Embora existam aplicações legítimas para essas tecnologias, como na indústria do entretenimento, na produção audiovisual e em contextos educacionais, sua utilização em cenários de manipulação informacional representa um desafio significativo. A capacidade de simular falas, expressões e comportamentos de indivíduos reais pode ser explorada para fins ilícitos, como fraude, difamação e disseminação de conteúdos enganosos.

A principal característica dos deep fakes reside em seu elevado grau de realismo, que compromete a capacidade de distinção entre conteúdos autênticos e artificiais. Essa dificuldade é potencializada pelo avanço contínuo dos modelos de inteligência artificial, que

incorporam técnicas cada vez mais sofisticadas de simulação, tornando os conteúdos praticamente indistinguíveis da realidade em determinadas situações.

Nesse contexto, os deepfakes devem ser compreendidos não apenas como uma inovação tecnológica, mas como um fenômeno que reconfigura as dinâmicas contemporâneas de produção e circulação da informação. Seus impactos ultrapassam o âmbito técnico, alcançando dimensões sociais e jurídicas relevantes, especialmente no que se refere à confiança nas informações e à integridade das interações digitais.

2.2 A intensificação da desinformação na era da inteligência artificial

A desinformação não constitui um fenômeno recente, estando historicamente associada à circulação de conteúdos enganosos com o objetivo de influenciar percepções, comportamentos e decisões coletivas. Contudo, a incorporação de tecnologias de inteligência artificial no processo de produção de conteúdos representa uma mudança qualitativa significativa nesse cenário, ampliando o alcance, a sofisticação e o potencial de impacto das informações falsas.

Nesse contexto, os deep fakes emergem como uma evolução das tradicionais formas de desinformação, na medida em que superam limitações anteriores relacionadas à qualidade e à credibilidade dos conteúdos manipulados. Diferentemente das chamadas fake news, que frequentemente se baseiam em textos ou imagens de fácil contestação, os conteúdos gerados por inteligência artificial apresentam um grau de realismo capaz de induzir o erro mesmo em observadores atentos. Essa característica compromete os mecanismos tradicionais de verificação, baseados na análise visual ou contextual das informações.

A intensificação da desinformação na era da inteligência artificial também está diretamente relacionada ao funcionamento das plataformas digitais, especialmente aquelas estruturadas a partir de modelos de negócios baseados na maximização do engajamento. Os sistemas de recomendação algorítmica, ao priorizarem conteúdos capazes de gerar maior interação, tendem a amplificar materiais que despertam emoções intensas, independentemente de sua veracidade. Como resultado, conteúdos manipulados, incluindo deep fakes, podem alcançar ampla disseminação em curto espaço de tempo, potencializando seus efeitos nocivos.

Além disso, a velocidade de circulação dessas informações dificulta a atuação de mecanismos tradicionais de contenção, como a verificação jornalística ou a resposta institucional. Em muitos casos, a identificação de um conteúdo como falso ocorre apenas após sua ampla difusão, momento em que seus efeitos já se encontram consolidados no imaginário

coletivo. Tal dinâmica evidencia uma assimetria entre a capacidade tecnológica de produção e disseminação de conteúdos e os instrumentos disponíveis para sua contenção.

Outro aspecto relevante refere-se ao impacto da desinformação sobre a confiança social. A proliferação de conteúdos sintéticos contribui para a criação de um ambiente de incerteza, no qual a própria noção de verdade passa a ser questionada. Esse fenômeno, frequentemente associado à chamada “crise da verdade”, compromete não apenas a credibilidade das informações falsas, mas também a confiabilidade de conteúdos legítimos, gerando um cenário de descrédito generalizado.

Nesse sentido, a inteligência artificial não apenas amplia a escala da desinformação, mas também altera sua natureza, tornando-a mais sofisticada, difícil de detectar e potencialmente mais danosa. Os deep fakes, enquanto expressão desse novo paradigma, evidenciam a necessidade de reavaliação dos instrumentos jurídicos e institucionais existentes, especialmente diante de contextos em que a circulação de informações exerce papel central na formação da opinião pública, como ocorre nos processos democráticos.

2.3 Deep Fakes e riscos ao processo eleitoral

A utilização de deep fakes no contexto eleitoral representa uma das manifestações mais preocupantes da desinformação digital contemporânea, na medida em que potencializa a manipulação da opinião pública e compromete a integridade do processo democrático. Em ambientes nos quais a informação desempenha papel central na formação da vontade do eleitor, a circulação de conteúdos falsificados com aparência de autenticidade pode produzir efeitos significativos e, por vezes, irreversíveis.

Os deep fakes possibilitam a criação de declarações fictícias atribuídas a candidatos, a simulação de comportamentos comprometedores ou a distorção de discursos, criando narrativas que podem influenciar diretamente a percepção do eleitorado. Tais práticas são particularmente sensíveis em períodos eleitorais, nos quais a dinâmica de circulação de informações é intensificada e o tempo para verificação e contestação é reduzido.

Além disso, a viralização desses conteúdos em plataformas digitais amplia seu alcance e dificulta sua contenção. A lógica de disseminação baseada no engajamento favorece a circulação de materiais sensacionalistas, independentemente de sua veracidade, o que contribui para a amplificação dos efeitos dos deep fakes. Em muitos casos, mesmo após a identificação de um conteúdo como falso, sua repercussão inicial já produziu impactos relevantes na formação da opinião pública.

Outro fator que agrava esse cenário é a assimetria temporal entre a produção e disseminação dos conteúdos manipulados e a atuação dos mecanismos institucionais de controle. A resposta jurídica, frequentemente dependente de provocação e de trâmites processuais, tende a ocorrer de forma posterior à consolidação dos efeitos do conteúdo, revelando-se insuficiente para evitar danos em tempo adequado.

Para além dos impactos imediatos, os deep fakes também contribuem para a erosão da confiança no próprio sistema informacional. A multiplicação de conteúdos sintéticos gera um ambiente de incerteza, no qual a autenticidade das informações passa a ser constantemente questionada. Esse fenômeno compromete não apenas a credibilidade de conteúdos falsos, mas também de informações verídicas, dificultando o exercício crítico por parte do eleitor.

Nesse contexto, os deep fakes configuram um risco estrutural à democracia, na medida em que afetam diretamente os pressupostos de transparência, confiabilidade e liberdade de escolha que fundamentam o processo eleitoral. A capacidade de manipulação informacional em larga escala evidencia a necessidade de reavaliação dos instrumentos jurídicos existentes, especialmente no que se refere à criação de mecanismos preventivos capazes de mitigar tais riscos antes da ocorrência de danos irreversíveis.

Como advertiu Goffredo da Silva Telles Júnior, “o Estado de Direito é o Estado da legitimidade” (TELLES JÚNIOR, 2003, p. 63), razão pela qual a circulação massiva de conteúdos manipulados capazes de comprometer a formação livre da vontade popular representa risco direto à estabilidade democrática e à própria confiança institucional.

Dessa forma, a análise dos impactos dos deep fakes no processo eleitoral reforça a necessidade de uma abordagem jurídica que ultrapasse o modelo tradicional, centrado na reparação posterior, e avance no desenvolvimento de estratégias regulatórias orientadas à prevenção, à transparência e à proteção da integridade democrática.

3 LIMITES DO ORDENAMENTO JURÍDICO BRASILEIRO

A análise dos impactos dos deep fakes no contexto da desinformação digital, especialmente em períodos eleitorais, impõe a necessidade de examinar a resposta do ordenamento jurídico brasileiro diante desse fenômeno. Embora existam instrumentos normativos relevantes voltados à proteção de direitos fundamentais e à regulação do ambiente digital, a complexidade e a velocidade das transformações tecnológicas evidenciam limitações estruturais do modelo jurídico vigente.

O Direito brasileiro, tradicionalmente orientado à reparação de danos após sua ocorrência, enfrenta dificuldades para lidar com situações em que a prevenção se mostra

essencial, como no caso da disseminação de conteúdos manipulados em larga escala. Nesse cenário, torna-se necessário analisar, de forma crítica, os direitos fundamentais afetados, os instrumentos jurídicos disponíveis e as insuficiências do modelo atual frente aos desafios impostos pelos deep fakes.

3.1 Direitos fundamentais afetados

A disseminação de deep fakes impacta diretamente um conjunto relevante de direitos fundamentais, especialmente aqueles relacionados à proteção da personalidade e à garantia das liberdades individuais. Dentre esses direitos, destacam-se a honra, a imagem, a privacidade e a autodeterminação informativa, todos assegurados pela Constituição Federal de 1988.

A manipulação de conteúdos audiovisuais por meio de inteligência artificial pode gerar representações falsas capazes de comprometer a reputação de indivíduos, expondo-os a situações de constrangimento, descrédito ou dano moral. Nesse contexto, a violação do direito à honra e à imagem assume contornos particularmente graves, uma vez que os deep fakes são dotados de elevado grau de realismo, dificultando sua contestação imediata.

Além disso, a utilização indevida de dados biométricos, como imagens faciais e padrões de voz, levanta questões relevantes no âmbito da privacidade e da proteção de dados pessoais. A criação de conteúdos sintéticos a partir de informações reais pode ocorrer sem o consentimento dos titulares, configurando uma violação à autodeterminação informativa e aos princípios que regem o tratamento de dados.

Paralelamente, a análise dos direitos fundamentais afetados pelos deep fakes exige a consideração da liberdade de expressão, igualmente protegida pela Constituição. A circulação de informações e a livre manifestação do pensamento constituem pilares essenciais do regime democrático, o que impõe limites à atuação estatal no controle de conteúdos.

Nesse sentido, evidencia-se uma tensão entre, de um lado, a necessidade de proteção contra abusos decorrentes do uso indevido da tecnologia e, de outro, a preservação da liberdade de expressão. A solução dessa tensão demanda uma abordagem equilibrada, capaz de evitar tanto a omissão regulatória quanto a imposição de restrições excessivas à circulação de informações.

Assim, os deep fakes evidenciam um cenário de colisão de direitos fundamentais, no qual se torna necessário ponderar valores constitucionais em conflito, considerando a proporcionalidade e a adequação das medidas jurídicas adotadas. Tal contexto reforça a

complexidade do tema e a necessidade de desenvolvimento de respostas jurídicas mais sofisticadas e compatíveis com a realidade tecnológica contemporânea.

3.2 Instrumentos jurídicos existentes

O ordenamento jurídico brasileiro dispõe de um conjunto de instrumentos normativos que, ainda que não tenham sido concebidos especificamente para enfrentar os desafios impostos pelos *deep fakes*, podem ser mobilizados na tutela de direitos afetados por essa tecnologia. Dentre esses instrumentos, destacam-se normas constitucionais, civis e regulatórias voltadas à proteção da personalidade, à responsabilização por danos e à disciplina do ambiente digital.

No plano constitucional, a Constituição Federal de 1988 assegura a inviolabilidade da honra, da imagem, da vida privada e da intimidade, estabelecendo fundamentos essenciais para a proteção dos indivíduos contra abusos decorrentes da manipulação informacional. Além disso, a Constituição também garante a liberdade de expressão, o que impõe a necessidade de equilíbrio entre a proteção contra conteúdos ilícitos e a preservação do livre fluxo de informações.

No âmbito infraconstitucional, o Marco Civil da Internet (Lei nº 12.965/2014) representa um dos principais diplomas voltados à regulação do ambiente digital no país. Entre seus dispositivos, destaca-se o regime de responsabilidade dos provedores de aplicação, que, em regra, condiciona a responsabilização à existência de ordem judicial para remoção de conteúdo. Tal modelo foi concebido com o objetivo de proteger a liberdade de expressão e evitar a censura privada, mas apresenta limitações quando aplicado a situações que demandam respostas rápidas, como no caso dos *deep fakes*.

Outro instrumento relevante é a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que estabelece princípios e regras para o tratamento de dados pessoais, incluindo dados sensíveis e biométricos. A utilização de imagens, vídeos e áudios para a criação de conteúdos sintéticos pode configurar tratamento indevido de dados pessoais, especialmente quando realizada sem consentimento do titular. Nesse sentido, a LGPD oferece fundamentos importantes para a responsabilização de agentes que utilizem dados de forma ilícita na produção de *deep fakes*.

Adicionalmente, o ordenamento jurídico brasileiro prevê mecanismos de responsabilização civil por danos morais e materiais decorrentes de violações aos direitos da personalidade, bem como dispositivos penais que podem ser aplicados em situações específicas, como crimes contra a honra ou fraudes. Tais instrumentos, embora relevantes, operam predominantemente a partir de uma lógica reativa, baseada na identificação do dano e na posterior atribuição de responsabilidade.

No contexto eleitoral, também se observam normas voltadas à proteção da lisura do processo democrático, incluindo regras sobre propaganda eleitoral e combate à desinformação. Contudo, a aplicação dessas normas a conteúdos gerados por inteligência artificial ainda enfrenta desafios interpretativos e operacionais, especialmente diante da dificuldade de identificação e comprovação da manipulação.

Dessa forma, embora o ordenamento jurídico brasileiro disponha de instrumentos relevantes para a tutela dos direitos afetados pelos deep fakes, a aplicação desses mecanismos revela limitações práticas, especialmente no que se refere à velocidade de resposta e à eficácia na contenção de danos em ambientes digitais de alta circulação informacional. Tais limitações indicam a necessidade de uma análise mais aprofundada acerca da suficiência do modelo jurídico vigente, o que será desenvolvido na seção seguinte.

3.3 Insuficiência do modelo jurídico atual

Apesar da existência de instrumentos normativos relevantes para a tutela dos direitos afetados pelos deep fakes, o ordenamento jurídico brasileiro apresenta limitações significativas diante das especificidades desse fenômeno. Tais limitações decorrem não apenas da ausência de regulamentação específica voltada à inteligência artificial e aos conteúdos sintéticos, mas também de características estruturais do próprio modelo jurídico tradicional, historicamente orientado à reparação posterior do dano.

No contexto dos deep fakes, a lógica predominantemente reativa do Direito revela-se insuficiente. A dinâmica de circulação de conteúdos em ambientes digitais ocorre em velocidade incompatível com os mecanismos convencionais de resposta institucional. Em muitos casos, quando medidas judiciais são adotadas para remoção de conteúdos ou responsabilização dos envolvidos, os materiais manipulados já atingiram ampla disseminação,

produzindo impactos relevantes sobre a opinião pública e, por vezes, efeitos irreversíveis sobre a reputação dos indivíduos e sobre o próprio debate democrático.

Essa insuficiência torna-se ainda mais evidente em períodos eleitorais, nos quais a circulação de informações ocorre de forma intensificada e o tempo assume papel determinante. Um conteúdo manipulado disseminado às vésperas de uma eleição pode influenciar significativamente a percepção do eleitorado antes mesmo da verificação de sua falsidade. Nesses casos, a posterior remoção do conteúdo ou eventual responsabilização civil mostram-se incapazes de restaurar integralmente os danos produzidos.

Além disso, a estrutura normativa atualmente existente apresenta dificuldades operacionais relevantes no que se refere à identificação dos responsáveis pela criação e disseminação dos deep fakes. A utilização de perfis anônimos, redes descentralizadas e mecanismos automatizados de compartilhamento dificulta a rastreabilidade dos conteúdos e compromete a efetividade das medidas jurídicas tradicionais.

Outro aspecto relevante diz respeito ao próprio modelo de responsabilização previsto no Marco Civil da Internet, cuja lógica condicionada à ordem judicial, embora voltada à proteção da liberdade de expressão, pode revelar-se inadequada em situações que exigem respostas céleres e preventivas. A demora inerente ao procedimento judicial contribui para a manutenção e propagação dos conteúdos ilícitos, ampliando seus efeitos nocivos.

Paralelamente, a ausência de mecanismos preventivos específicos evidencia uma lacuna importante no enfrentamento dos deep fakes. O ordenamento jurídico brasileiro ainda carece de instrumentos voltados à identificação prévia de conteúdos sintéticos, à transparência algorítmica e à imposição de deveres preventivos às plataformas digitais. Como resultado, a atuação estatal tende a ocorrer apenas após a consolidação dos danos, reduzindo significativamente a eficácia da tutela jurídica.

A insuficiência do modelo atual também se relaciona à crescente assimetria entre o avanço tecnológico e a capacidade regulatória do Estado. A evolução acelerada das ferramentas de inteligência artificial amplia continuamente a sofisticação dos deep fakes, enquanto os instrumentos jurídicos permanecem dependentes de estruturas concebidas para uma realidade tecnológica distinta. Tal cenário evidencia um descompasso entre a complexidade dos riscos contemporâneos e os mecanismos disponíveis para sua contenção.

Dessa forma, verifica-se que o ordenamento jurídico brasileiro, embora disponha de instrumentos relevantes para proteção de direitos fundamentais, ainda não apresenta respostas plenamente adequadas aos desafios impostos pelos deep fakes. A predominância de mecanismos reativos, a ausência de estratégias preventivas eficazes e as limitações operacionais da responsabilização tradicional demonstram a necessidade de desenvolvimento de soluções regulatórias mais compatíveis com a dinâmica das tecnologias de inteligência artificial e com os riscos estruturais que estas representam para a democracia digital.

4 ALTERNATIVAS REGULATÓRIAS PARA O ENFRENTAMENTO DOS DEEP FAKES

A insuficiência dos mecanismos jurídicos tradicionais diante dos desafios impostos pelos deep fakes evidencia a necessidade de desenvolvimento de estratégias regulatórias mais compatíveis com a dinâmica das tecnologias de inteligência artificial e com os riscos estruturais associados à desinformação digital. Nesse contexto, o debate regulatório contemporâneo tem buscado construir soluções capazes de equilibrar a proteção dos direitos fundamentais, a preservação da liberdade de expressão e a integridade do ambiente democrático.

A complexidade do fenômeno impede a adoção de respostas simplificadas ou exclusivamente repressivas. Os deep fakes envolvem simultaneamente questões tecnológicas, jurídicas, sociais e econômicas, exigindo abordagens multidimensionais e integradas. Assim, torna-se necessário analisar os diferentes modelos regulatórios possíveis, bem como seus limites e potencialidades, especialmente no contexto do processo eleitoral e da circulação massiva de informações em plataformas digitais.

4.1 Modelos regulatórios possíveis

O enfrentamento dos deep fakes tem sido objeto de debates regulatórios em diferentes países, revelando a inexistência de um modelo único ou plenamente consolidado. Em linhas gerais, as propostas existentes podem ser agrupadas em três grandes perspectivas: a regulação estatal, a autorregulação das plataformas digitais e os modelos híbridos de governança.

A primeira abordagem consiste na adoção de mecanismos regulatórios estatais voltados à criação de normas específicas para inteligência artificial e conteúdos sintéticos. Nesse modelo, o Estado assume papel central na definição de obrigações, limites e

responsabilidades aplicáveis aos agentes envolvidos na produção e disseminação de deep fakes. Entre as medidas frequentemente discutidas estão a exigência de identificação de conteúdos manipulados, a previsão de sanções para usos ilícitos e a criação de deveres de diligência para plataformas digitais.

A principal vantagem dessa abordagem reside na possibilidade de estabelecimento de parâmetros jurídicos uniformes e vinculantes, capazes de conferir maior segurança jurídica e previsibilidade regulatória. Contudo, a adoção de modelos excessivamente restritivos pode gerar riscos à liberdade de expressão e à livre circulação de informações, especialmente diante da dificuldade de delimitação precisa entre conteúdos ilícitos, sátiras, manifestações artísticas e usos legítimos da inteligência artificial.

A segunda perspectiva baseia-se na autorregulação das plataformas digitais, atribuindo às empresas responsáveis pelos ambientes virtuais o dever de desenvolver políticas internas de monitoramento, identificação e remoção de conteúdos manipulados. Nesse modelo, as próprias plataformas passam a estabelecer mecanismos de controle, incluindo sistemas automatizados de detecção, políticas de rotulagem e restrições à disseminação de conteúdos potencialmente enganosos.

Embora a autorregulação apresente maior flexibilidade e capacidade de adaptação às rápidas transformações tecnológicas, ela também suscita preocupações relevantes. A ausência de controle democrático direto sobre as decisões das plataformas pode ampliar a concentração de poder privado sobre o fluxo informacional, além de gerar riscos de arbitrariedade e falta de transparência nos critérios de moderação de conteúdo.

Diante das limitações dos modelos puramente estatais ou exclusivamente privados, ganha destaque a adoção de modelos híbridos de governança, que buscam integrar instrumentos regulatórios públicos com mecanismos tecnológicos e políticas de autorregulação supervisionada. Essa abordagem parte do reconhecimento de que os desafios impostos pelos deep fakes não podem ser solucionados apenas por meio da atuação estatal ou empresarial isolada, exigindo cooperação entre diferentes atores institucionais.

Os modelos híbridos permitem a combinação entre deveres legais mínimos, transparência algorítmica, mecanismos preventivos e soluções tecnológicas de identificação de conteúdos sintéticos. Além disso, possibilitam maior flexibilidade regulatória, preservando

espaço para inovação tecnológica sem afastar a necessidade de proteção dos direitos fundamentais e da integridade democrática.

Nesse contexto, a adoção de mecanismos regulatórios preventivos assume especial relevância, sobretudo em períodos eleitorais, nos quais os impactos da desinformação podem comprometer diretamente a legitimidade do processo democrático. A construção de respostas regulatórias adequadas exige, portanto, uma abordagem equilibrada, capaz de compatibilizar inovação, liberdade de expressão e proteção institucional em um ambiente digital marcado pela rápida evolução tecnológica.

4.2 Responsabilidade das plataformas e transparência algorítmica

A centralidade das plataformas digitais na circulação de informações atribui a esses agentes papel relevante no enfrentamento dos riscos associados aos deep fakes. Redes sociais, serviços de compartilhamento de vídeos e demais ambientes digitais operam como principais vetores de disseminação de conteúdos manipulados, especialmente em contextos de elevada circulação informacional, como os períodos eleitorais. Nesse cenário, o debate acerca da responsabilidade das plataformas digitais assume importância crescente no âmbito jurídico e regulatório.

O modelo atualmente predominante no ordenamento jurídico brasileiro, especialmente a partir do Marco Civil da Internet, estrutura-se sobre a lógica da responsabilização condicionada à ordem judicial. Embora tal sistema tenha sido concebido para proteger a liberdade de expressão e evitar práticas de censura privada, sua aplicação aos casos envolvendo deep fakes revela limitações práticas relevantes, sobretudo diante da velocidade de propagação dos conteúdos.

A dinâmica de disseminação dos deep fakes em plataformas digitais ocorre, frequentemente, em ritmo incompatível com o tempo necessário para a obtenção de decisões judiciais. Em muitos casos, o conteúdo manipulado alcança ampla repercussão antes mesmo da adoção de medidas de remoção, reduzindo significativamente a eficácia das respostas institucionais posteriores. Essa realidade evidencia a necessidade de reflexão acerca do papel preventivo das plataformas na contenção de danos informacionais.

Nesse contexto, tem ganhado relevância a discussão sobre a imposição de deveres de diligência às plataformas digitais, especialmente no que se refere à identificação e limitação

da circulação de conteúdos sintéticos potencialmente lesivos. Tais deveres podem envolver mecanismos de detecção automatizada, políticas de rotulagem de conteúdos gerados por inteligência artificial e procedimentos mais céleres de resposta diante de situações de risco elevado.

A adoção de medidas preventivas, contudo, não se mostra isenta de controvérsias. A ampliação das responsabilidades das plataformas suscita preocupações relacionadas à liberdade de expressão, à possibilidade de remoções excessivas e à concentração de poder privado sobre a moderação do discurso público. O risco de decisões automatizadas equivocadas ou de critérios opacos de moderação evidencia a necessidade de estabelecimento de parâmetros transparentes e compatíveis com as garantias constitucionais.

Nesse sentido, a transparência algorítmica assume papel fundamental. Os sistemas de recomendação e distribuição de conteúdo utilizados pelas plataformas influenciam diretamente o alcance e a visibilidade das informações circulantes no ambiente digital. A ausência de clareza acerca dos critérios utilizados por esses sistemas dificulta a compreensão dos mecanismos de amplificação da desinformação e reduz a possibilidade de controle social e institucional sobre seus impactos.

A implementação de deveres de transparência pode contribuir para maior responsabilização das plataformas, permitindo a identificação de práticas que favoreçam a circulação de conteúdos manipulados ou potencialmente danosos. Além disso, mecanismos de auditoria e prestação de contas podem fortalecer a legitimidade das políticas de moderação e reduzir riscos de arbitrariedade.

No contexto dos deep fakes, a transparência algorítmica também se relaciona à necessidade de identificação clara de conteúdos produzidos ou alterados por inteligência artificial. A rotulagem de conteúdos sintéticos surge, nesse cenário, como uma alternativa capaz de ampliar a capacidade de verificação por parte dos usuários, reduzindo os riscos de manipulação informacional sem impor restrições absolutas à circulação de conteúdos.

Dessa forma, a discussão sobre responsabilidade das plataformas e transparência algorítmica revela-se essencial para o desenvolvimento de estratégias regulatórias mais eficazes no enfrentamento dos deep fakes. A construção de mecanismos preventivos e transparentes mostra-se particularmente relevante em contextos eleitorais, nos quais a

velocidade de circulação das informações pode produzir impactos significativos sobre a formação da opinião pública e sobre a integridade democrática.

4.3 Mecanismos preventivos e soluções tecnológicas

A insuficiência das respostas jurídicas tradicionalmente orientadas à reparação posterior do dano evidencia a necessidade de desenvolvimento de mecanismos preventivos voltados à contenção dos riscos associados aos deep fakes. Em um ambiente digital caracterizado pela rápida circulação de informações, a adoção de medidas exclusivamente repressivas mostra-se limitada, especialmente diante da velocidade com que conteúdos manipulados podem alcançar ampla disseminação e influenciar a formação da opinião pública.

Nesse contexto, as soluções tecnológicas assumem papel relevante no enfrentamento preventivo da desinformação produzida por inteligência artificial. Entre as alternativas discutidas no âmbito regulatório e técnico, destacam-se os sistemas de identificação de conteúdos sintéticos, mecanismos de rastreabilidade digital e ferramentas automatizadas de detecção de manipulações audiovisuais.

A rotulagem de conteúdos produzidos ou alterados por inteligência artificial surge como uma das medidas preventivas mais debatidas atualmente. Tal mecanismo consiste na identificação explícita de conteúdos sintéticos, permitindo que os usuários tenham ciência acerca da utilização de inteligência artificial na criação ou modificação do material visual ou sonoro. A adoção de sistemas de rotulagem pode contribuir para ampliar a transparência informacional e reduzir os riscos de manipulação indevida da percepção pública.

Além disso, mecanismos de rastreabilidade digital, como marcas d'água (watermarks) e certificações de autenticidade, têm sido apontados como alternativas capazes de auxiliar na verificação da origem e integridade dos conteúdos. Essas ferramentas permitem a identificação de alterações realizadas em materiais audiovisuais, fortalecendo a capacidade de detecção de manipulações e contribuindo para a preservação da confiabilidade informacional.

Paralelamente, o desenvolvimento de sistemas automatizados de detecção de deep fakes representa uma estratégia complementar de prevenção. Tais ferramentas utilizam inteligência artificial para identificar inconsistências em expressões faciais, padrões vocais ou elementos visuais que indiquem manipulação sintética. Contudo, a eficácia desses mecanismos enfrenta limitações decorrentes da própria evolução tecnológica dos modelos generativos, que se tornam progressivamente mais sofisticados e difíceis de detectar.

Outro aspecto relevante refere-se à necessidade de adoção de políticas preventivas por parte das plataformas digitais. A implementação de protocolos específicos para períodos eleitorais, sistemas de resposta rápida e mecanismos de redução de alcance de conteúdos suspeitos pode contribuir para minimizar os impactos da desinformação sem impor restrições absolutas à circulação de informações.

Todavia, a utilização de soluções tecnológicas no enfrentamento dos deep fakes também suscita preocupações relevantes. A adoção de mecanismos automatizados de controle pode gerar riscos relacionados a erros de identificação, remoções indevidas e limitações excessivas à liberdade de expressão. Além disso, a dependência de sistemas automatizados amplia debates acerca da transparência, da supervisão humana e da legitimidade das decisões algorítmicas.

Nesse sentido, os mecanismos preventivos não devem ser compreendidos como soluções autônomas ou suficientes por si mesmas, mas como instrumentos complementares a estratégias regulatórias mais amplas. A combinação entre medidas jurídicas, deveres de transparência e soluções tecnológicas mostra-se essencial para a construção de um modelo de enfrentamento mais eficaz e proporcional aos desafios impostos pelos deep fakes.

Assim, a adoção de estratégias preventivas representa um elemento central para a proteção da integridade democrática no ambiente digital, especialmente em contextos eleitorais, nos quais a velocidade de disseminação da desinformação pode comprometer significativamente a formação livre e consciente da vontade popular.

4.4 Proposta de modelo regulatório híbrido

A complexidade dos desafios impostos pelos deep fakes evidencia a insuficiência de soluções regulatórias isoladas ou exclusivamente orientadas por perspectivas repressivas. A natureza dinâmica da inteligência artificial, associada à velocidade de circulação das informações em ambientes digitais, exige a construção de mecanismos regulatórios capazes de integrar instrumentos jurídicos, soluções tecnológicas e deveres institucionais voltados à prevenção de danos.

Nesse contexto, propõe-se a adoção de um modelo regulatório híbrido, estruturado a partir da articulação entre atuação estatal, responsabilidade das plataformas digitais e utilização de mecanismos tecnológicos de transparência e rastreabilidade. Tal proposta parte do reconhecimento de que os riscos associados aos deep fakes não podem ser enfrentados

adequadamente por um único agente institucional, demandando cooperação entre Estado, empresas de tecnologia e sociedade civil.

O primeiro eixo deste modelo refere-se à atuação estatal na definição de parâmetros normativos mínimos voltados à proteção da integridade democrática e dos direitos fundamentais. Nesse âmbito, destaca-se a necessidade de desenvolvimento de normas específicas relacionadas à utilização de conteúdos sintéticos em contextos eleitorais, especialmente no que se refere à obrigação de identificação de materiais manipulados e à criação de mecanismos céleres de resposta diante de situações de elevado potencial lesivo.

O segundo eixo envolve a ampliação dos deveres de diligência atribuídos às plataformas digitais. Considerando o papel central desses agentes na circulação e amplificação de conteúdos, mostra-se necessária a implementação de políticas preventivas voltadas à identificação, rotulagem e limitação da disseminação de deep fakes potencialmente danosos. Tal atuação, contudo, deve observar critérios transparentes e compatíveis com as garantias constitucionais, evitando práticas arbitrárias ou restrições desproporcionais à liberdade de expressão.

O terceiro eixo consiste na incorporação de soluções tecnológicas voltadas à transparência e rastreabilidade dos conteúdos digitais. Ferramentas de identificação de conteúdos sintéticos, certificação de autenticidade e mecanismos automatizados de detecção podem contribuir para ampliar a capacidade preventiva do sistema regulatório, especialmente em contextos de rápida circulação informacional.

A adoção de um modelo híbrido também permite superar parte das limitações do paradigma jurídico tradicional, excessivamente centrado na reparação posterior do dano. Ao incorporar mecanismos preventivos e estratégias de mitigação em tempo adequado, torna-se possível reduzir os impactos decorrentes da disseminação de conteúdos manipulados antes da consolidação de seus efeitos sobre a opinião pública e sobre o processo democrático.

Além disso, a estrutura híbrida possibilita maior flexibilidade regulatória diante da constante evolução das tecnologias de inteligência artificial. A rápida transformação dos modelos generativos exige mecanismos regulatórios capazes de adaptação contínua, evitando que o Direito permaneça permanentemente em posição de atraso em relação ao desenvolvimento tecnológico.

No contexto eleitoral, a implementação de estratégias preventivas integradas assume relevância ainda maior. A combinação entre monitoramento reforçado, transparência informacional e respostas institucionais céleres pode contribuir para minimizar os riscos de manipulação da vontade popular e preservar a legitimidade do processo democrático.

Dessa forma, a adoção de um modelo regulatório híbrido apresenta-se como alternativa mais adequada para o enfrentamento dos deepfakes, ao combinar proteção dos direitos fundamentais, preservação da liberdade de expressão e fortalecimento da integridade democrática em um cenário marcado pela crescente influência da inteligência artificial sobre a circulação de informações.

5 CONCLUSÃO

O avanço das tecnologias de inteligência artificial generativa, especialmente no que se refere à produção de deep fakes, evidencia a emergência de novos desafios para o Direito contemporâneo, sobretudo no contexto da proteção da democracia e da integridade do processo eleitoral. A crescente sofisticação dos conteúdos sintéticos, associada à velocidade de disseminação proporcionada pelas plataformas digitais, amplia significativamente os riscos relacionados à desinformação e à manipulação da opinião pública.

Ao longo do presente estudo, verificou-se que os deep fakes ultrapassam a dimensão meramente tecnológica, configurando um fenômeno com impactos relevantes sobre direitos fundamentais, como honra, imagem, privacidade e liberdade de expressão. Além disso, observou-se que a utilização desses conteúdos em períodos eleitorais potencializa riscos estruturais ao ambiente democrático, comprometendo a confiabilidade das informações e fragilizando a formação livre e consciente da vontade popular.

A análise do ordenamento jurídico brasileiro demonstrou que, embora existam instrumentos normativos relevantes para a tutela dos direitos afetados pelos deep fakes, os mecanismos atualmente disponíveis apresentam limitações significativas diante da dinâmica contemporânea da desinformação digital. O modelo jurídico vigente permanece predominantemente orientado à reparação posterior do dano, revelando dificuldades em atuar de forma preventiva e em tempo adequado diante da rápida circulação de conteúdos manipulados.

Nesse contexto, confirmou-se a hipótese inicialmente formulada, no sentido de que o ordenamento jurídico brasileiro ainda não dispõe de respostas plenamente suficientes para enfrentar os riscos decorrentes da disseminação de deep fakes, especialmente em cenários eleitorais. A ausência de mecanismos preventivos específicos, aliada às limitações operacionais da responsabilização tradicional, evidencia a necessidade de desenvolvimento de estratégias regulatórias mais compatíveis com a realidade tecnológica contemporânea.

Diante dessas limitações, o trabalho propôs a adoção de um modelo regulatório híbrido, baseado na articulação entre atuação estatal, responsabilidade das plataformas digitais e utilização de soluções tecnológicas de transparência e rastreabilidade. Tal proposta busca equilibrar a proteção dos direitos fundamentais e da integridade democrática com a preservação da liberdade de expressão e da inovação tecnológica, evitando tanto a omissão regulatória quanto intervenções excessivamente restritivas.

Conclui-se, portanto, que o enfrentamento dos deep fakes demanda uma reconfiguração das estratégias jurídicas tradicionalmente adotadas no ambiente digital, com maior ênfase em mecanismos preventivos, deveres de transparência e cooperação institucional. Em um cenário de constante evolução da inteligência artificial, a construção de respostas regulatórias eficazes torna-se essencial não apenas para a proteção individual dos cidadãos, mas também para a preservação da confiança pública e da estabilidade democrática.

REFERÊNCIAS

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2021.

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

BRASIL. Marco Civil da Internet. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014.

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

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Thomson Reuters Brasil, 2021.

LEVY, Pierre. *Cibercultura*. São Paulo: Editora 34, 2010.

MAGRANI, Eduardo. *Democracia conectada: a internet como ferramenta de engajamento político-democrático*. Curitiba: Juruá, 2014.

MARTINS, Guilherme Magalhães. *Responsabilidade civil e mídias digitais*. São Paulo: Revista dos Tribunais, 2020.

MENDES, Laura Schertel. *Proteção de dados pessoais na internet: contexto e perspectivas da Lei Geral de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 2021.

SANTAELLA, Lucia. *A inteligência artificial é inteligente?*. São Paulo: Paulus, 2023.

SUNSTEIN, Cass R. *#Republic: divided democracy in the age of social media*. Princeton: Princeton University Press, 2017.

TELLES JÚNIOR, Goffredo da Silva. *O povo e o poder*. São Paulo: Juarez de Oliveira, 2003.