III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

POLÍTICAS PÚBLICAS E DIREITOS HUMANOS NA ERA TECNOLÓGICA II

P769
Políticas públicas e direitos humanos na era tecnológica II [Recurso eletrônico on-line] organização III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade de Direito de Franca – Franca;

Coordenadores: Manoel Ilson, Marcelo Toffano e Marcelo Fonseca – Franca: Faculdade de Direito de Franca, 2025.

Inclui bibliografia
ISBN: 978-65-5274-371-8
Modo de acesso: www.conpedi.org.br em publicações
Tema: Governança, regulação e o futuro da inteligência artificial.
1. Direito. 2. Políticas Públicas. 3. Tecnologia. 4. Internet. I. III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2025 : Franca, SP).

CDU: 34

III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

POLÍTICAS PÚBLICAS E DIREITOS HUMANOS NA ERA TECNOLÓGICA II

Apresentação

Entre os dias 30 de setembro e 3 de outubro de 2025, a Faculdade de Direito de Franca recebeu o III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet. O evento reuniu acadêmicos, profissionais, pesquisadores e estudantes, promovendo o debate interdisciplinar sobre o impacto das inovações tecnológicas no campo jurídico e nas políticas públicas. A programação envolveu Grupos de Trabalho (GTs) organizados para aprofundar temas específicos, abordando desde o acesso à justiça até as complexidades da regulação tecnológica, com ênfase na adaptação do sistema jurídico aos avanços da inteligência artificial e da automação.

O GT 2 investiga as relações entre políticas públicas, direitos humanos e avanços tecnológicos. Os trabalhos apresentados analisam a influência das novas mídias na formação da opinião pública, os limites da liberdade de expressão e os desafios da proteção de dados. O grupo reflete sobre como o Estado pode promover uma governança digital que garanta a dignidade humana e a inclusão social na era da informação.

A AMEAÇA DAS DEEPFAKES À DEMOCRACIA: DESINFORMAÇÃO, CIBERPOLARIZAÇÃO E OS LIMITES DA LIBERDADE DE EXPRESSÃO

THE THREAT OF DEEPFAKES TO DEMOCRACY: DISINFORMATION, CYBERPOLARIZATION AND THE LIMITS OF FREE SPEECH

Cláudia Gil Mendonça

Resumo

O desenvolvimento das deepfakes, viabilizado pelo avanço da inteligência artificial, introduziu novas ameaças ao Estado Democrático de Direito, especialmente quando tais conteúdos são utilizados para desinformação e manipulação política. Inseridas no contexto da ciberpolarização, essas tecnologias comprometem princípios fundamentais como a integridade dos processos democráticos, a liberdade de expressão e a dignidade da pessoa humana. Nesse contexto, este artigo analisa as implicações jurídicas das deepfakes e os efeitos da ciberpolarização, propondo abordagens regulatórias para mitigar seus impactos, com base em pesquisa qualitativa de cunho dedutivo, sustentada em fontes legislativas, doutrinárias e jurisprudenciais.

Palavras-chave: Deepfake, Ciberpolarização, Estado democrático de direito, Princípios fundamentais

Abstract/Resumen/Résumé

The development of deepfakes, enabled by advances in artificial intelligence, has introduced new threats to the democratic rule of law, especially when such content is used for disinformation and political manipulation. Within the context of cyberpolarization, these technologies compromise fundamental principles such as the integrity of democratic processes, freedom of expression, and human dignity. In this context, this article analyzes the legal implications of deepfakes and the effects of cyberpolarization, proposing regulatory approaches to mitigate their impacts, based on qualitative deductive research supported by legislative, doctrinal, and jurisprudential sources.

Keywords/Palabras-claves/Mots-clés: Deepfake, Cyberpolarization, Democratic rule of law, Fundamental principles

Introdução

A comunicação por meio da internet, embora tenha promovido uma conectividade global sem precedentes, também desencadeou efeitos negativos significativos, dentre os quais se destaca o fenômeno da *deepfake*. Trata-se de conteúdos falsificados, como vídeos e áudios, gerados ou manipulados por algoritmos de inteligência artificial, capazes de simular com alto grau de realismo a aparência e a voz de uma pessoa, criando representações digitais que aparentam ser autênticas (Spencer, 2019, n.p.). Esses materiais contribuem diretamente para a disseminação de notícias falsas (*fake news*).

Quando amplamente divulgadas, as *deepfakes* podem distorcer a percepção da realidade e influenciar indevidamente a opinião pública, afetando inclusive processos democráticos. Ao induzirem as pessoas a decisões baseadas em informações falsas, esses conteúdos potencializam a polarização de debates, fenômeno conhecido como *ciberpolarização*. Tal dinâmica compromete a credibilidade das instituições políticas e enfraquece os pilares fundamentais do Estado Democrático de Direito, tornando as *deepfakes* uma das principais ameaças à integridade da informação e à confiança pública nas democracias contemporâneas.

A velocidade com que essas informações se propagam na internet agrava ainda mais seu impacto, dificultando a identificação, a contenção e a correção de falsidades. Nesse cenário, valores essenciais como a liberdade de expressão, o direito à informação, a participação política e a dignidade humana, todos alicerces do Estado Democrático de Direito, passam a ser colocados em risco.

Desse modo, o uso irresponsável de tecnologias como a *deepfake*, especialmente quando associado ao alcance das redes sociais, compromete a formação de uma opinião pública consciente e bem informada, indispensável ao pleno funcionamento das instituições democráticas.

Diante desse panorama, o presente artigo tem como objetivo demonstrar de que maneira a *deepfake* pode interferir na democracia, analisando suas consequências, os impactos do avanço tecnológico e da disseminação de notícias falsas nas redes sociais, além de examinar a aplicação constitucional das garantias da liberdade de expressão, do direito à informação e da proteção à imagem, a fim de buscar soluções para tal questão.

Para tanto, a abordagem adotada no artigo será baseada nos métodos dedutivo e bibliográfico, com análise legislativa, doutrinária e jurisprudencial sobre o tema.

2. Metodologia

A presente pesquisa possui natureza qualitativa, entendida como um instrumento voltado à exploração e à compreensão dos significados atribuídos por indivíduos ou grupos a determinados problemas sociais ou humanos (Creswell, 2010, p. 43), sempre observando os limites estabelecidos pelos objetivos do estudo.

Para o desenvolvimento do trabalho, utilizou-se a pesquisa bibliográfica, baseada no levantamento de referências teóricas previamente analisadas e publicadas em meios impressos e digitais, como livros, artigos científicos, páginas da internet, entre outros. Além disso, recorreu-se à pesquisa documental, por meio da análise de decisões proferidas pelos tribunais brasileiros, a fim de aprofundar a compreensão da temática abordada.

3. Resultados e Discussão

O avanço das tecnologias digitais no contexto da globalização inaugurou uma nova era na comunicação, caracterizada pela mediação quase onipresente de computadores conectados à internet. A inteligência artificial, outrora limitada ao imaginário da ficção científica, evoluiu ao longo do século XX para se tornar uma realidade concreta, dotada de capacidades complexas, como o uso da linguagem, a resolução de problemas e o aprendizado autônomo (Lavagnoli, 2024, n.p.).

A IA, enquanto ramo da ciência da computação voltado à replicação de capacidades cognitivas humanas por meio de *softwares*, apoia-se em algoritmos, especialmente os de *machine learning* e *deep learning* (Guillou, 2018, n.p.). Esses últimos, ao se estruturarem em redes neurais profundas, são capazes de aperfeiçoar-se com base nos próprios erros, possibilitando o surgimento de tecnologias sofisticadas como as *deepfakes* (Robles-Lessa; Cabral; Silvestre, 2020, n.p.).

Na lição de Michael K. Spencer,

> Deepfakes são, essencialmente, identidades falsas criadas com o Deep Learning [aprendizagem profunda, por meio de uso maciço de dados], por meio de uma técnica de síntese de imagem humana baseada na inteligência artificial. É usada para combinar e sobrepor imagens e vídeos preexistentes e transformá-los em imagens ou vídeos "originais" [...] Essa combinação de vídeos existentes e "originais" resulta em vídeos falsos, que mostram uma ou algumas pessoas realizando ações ou fazendo coisas que nunca aconteceram na realidade (Spencer, 2019, n.p.).

Assim, sendo, trata-se de conteúdos manipulados, como vídeos, áudios e imagens altamente realistas, que simulam pessoas executando ações que jamais ocorreram, frequentemente com fins lesivos. Sua criação foi viabilizada pelas Redes Neurais Generativas

Adversárias (GANs), que tornam as falsificações cada vez mais verossímeis e de difícil detecção (Lima, 2020, n.p.).

O uso das *deepfakes* transita entre fins criativos e aplicações maliciosas, como vingança, chantagem, fabricação de provas falsas e manipulação política. A facilidade de acesso a ferramentas de edição e a ampla disponibilidade de imagens pessoais nas redes sociais tornam qualquer indivíduo um potencial alvo, o que, por consequência, impõe dilemas éticos, jurídicos e de segurança de altíssima complexidade (Westerlund, 2019, n.p.).

Paralelamente, a sociedade contemporânea assiste a uma escalada da desinformação nas plataformas digitais. A confiança indiscriminada do público nas redes sociais, somada à escassa educação midiática, tem impulsionado a propagação de *fake news*, agravada por algoritmos que priorizam conteúdos polarizadores. Nesse ambiente, a linha que separa o real do falso se torna cada vez mais tênue, comprometendo a qualidade do debate público e o funcionamento saudável da democracia.

A comunicação digital, nesse sentido, apresenta-se como instrumento ambíguo: ao mesmo tempo em que promove a inclusão e o acesso à informação, também se converte em meio de manipulação e vulnerabilização. Assim, o fenômeno das *deepfakes* ilustra os perigos de um progresso tecnológico dissociado de parâmetros éticos e normativos, demandando reflexão crítica sobre seus efeitos no Estado Democrático de Direito e a urgente formulação de estratégias regulatórias, educativas e institucionais.

A aceleração comunicacional na sociedade da informação suprimiu barreiras como o segredo, a distância e o estranhamento, tornando as interações simbólicas mais frequentes, mas também mais superficiais (Gatinho; Silveira; Dias, 2024, p. 9-10). Como observa Zygmunt Bauman (2012), integração e fragmentação coexistem no espaço digital: a aproximação promovida pelas redes não dissolve as divergências, mas intensifica a polarização. Já Cass Sunstein (2018) alerta para o risco das "câmaras de eco", onde algoritmos personalizados confinam os usuários a visões semelhantes, reforçando preconceitos e dificultando o encontro com a diferença, elemento vital à democracia deliberativa.

Desse modo, as redes sociais, alimentadas por algoritmos orientados ao engajamento, ampliam esse processo ao criar bolhas informacionais e comunidades ideologicamente homogêneas. Ainda que o autoisolamento digital não seja, por si, negativo, ele propicia a proliferação de rumores, distorções e extremismos (Sunstein, 2018). A internet, portanto, não cria tais fenômenos, mas os potencializa em escala inédita e, a assimetria da esfera pública, antes visível nos meios tradicionais, radicaliza-se no ambiente *online*, que favorece a

“polarização de grupo”, em que interações entre semelhantes levam à adoção de posições ainda mais extremas (Benkler; Faris; Roberts, 2018).

Esse processo configura o que se denomina *ciberpolarização*, ou seja, uma intensificação das divisões políticas e sociais mediada por tecnologias digitais (Robles-Lessa; Cabral; Silvestre, 2020, n.p.). Nesse contexto, as *deepfakes* agravam o quadro ao manipular visual e sonoramente a realidade, forjando narrativas falsas sobre figuras públicas e eventos políticos. Assim, ao minar a confiança pública e alimentar a desinformação, tais conteúdos desestabilizam o discurso racional, essencial à vida democrática (Robles-Lessa; Cabral; Silvestre, 2020, n.p.).

No Brasil, os desafios jurídicos decorrentes das *deepfakes* são expressivos. A manipulação audiovisual sem consentimento atinge direitos fundamentais como a privacidade, a honra e a imagem, gerando danos morais e institucionais de grande magnitude. A legislação brasileira, embora conte com instrumentos como a LGPD, o Código Penal, o Marco Civil da Internet e o Projeto de Lei sobre *fake news*, ainda apresenta lacunas diante da complexidade técnica, da dificuldade de rastreamento dos agentes e da responsabilização das plataformas digitais.

Salienta-se que, em períodos eleitorais, os riscos se agravam, pois, essas tecnologias são empregadas para manipular a opinião pública e comprometer a legitimidade do processo democrático. Nesse contexto, a tensão entre liberdade de expressão e proteção de direitos fundamentais intensifica o debate, pois a livre manifestação do pensamento é um pilar das sociedades democráticas, mas não pode ser confundida com o direito de divulgar falsificações prejudiciais (Andrade, 2022).

Assim, o uso de *deepfakes* exige não apenas responsabilização civil e penal dos envolvidos, mas também o desenvolvimento de normas específicas, penas proporcionais, ferramentas de detecção automatizada e articulação entre setor público, plataformas digitais e academia.

Empresas como Google, Amazon e Facebook já investem em tecnologias capazes de detectar conteúdos manipulados. Pesquisadores têm explorado o uso de *blockchain*, inteligência artificial inversa e padrões visuais para identificar falsificações (Schroepfer, 2019, n.p.). No entanto, a resposta não pode ser apenas tecnológica. A construção de um ecossistema digital saudável requer também a educação midiática da população (Westerlund, 2019, n.p.), pois, a alfabetização digital, especialmente entre os grupos mais vulneráveis, é fundamental para formar uma cidadania crítica e resistente à desinformação.

Face ao exposto, enfrentar os desafios impostos pelas *deepfakes* e pela *ciberpolarização* exige, portanto, uma abordagem multidimensional: aprimoramento legislativo, responsabilidade compartilhada, inovação tecnológica, atuação ética das plataformas e fortalecimento da formação cidadã. A preservação dos direitos fundamentais e a integridade do Estado Democrático de Direito dependem dessa articulação entre regulação, tecnologia e educação crítica.

4. Considerações Finais

A proliferação de *deepfakes* representa uma grave ameaça ao Estado Democrático de Direito, sobretudo quando associada ao fenômeno da *ciberpolarização*. Suas implicações jurídicas são vastas e preocupantes, abrangendo desde a manipulação de processos eleitorais e violação da privacidade até a difamação de figuras públicas e o enfraquecimento da confiança coletiva nas instituições democráticas.

Para salvaguardar os fundamentos do Estado de Direito, torna-se imperativa a formulação de legislações específicas que assegurem a responsabilização não apenas dos indivíduos que produzem esse tipo de conteúdo, mas também das plataformas que facilitam sua disseminação. Tal arcabouço normativo deve ser acompanhado de esforços coordenados de cooperação internacional e de promoção da educação midiática, a fim de mitigar os impactos deletérios dessa tecnologia sobre a esfera pública.

Em síntese, as *deepfakes* podem ser utilizadas para forjar áudios ou vídeos com conteúdo difamatório, atentando contra a honra e a imagem de indivíduos. Nesses casos, as vítimas têm o direito de buscar reparação por danos morais e acionar os responsáveis com base em crimes contra a honra, como calúnia, difamação ou injúria, contudo o desafio reside na velocidade e na complexidade das inovações tecnológicas. Além disso, quando envolverem o uso indevido de dados pessoais, as *deepfakes* podem, ainda, configurar infrações à Lei Geral de Proteção de Dados Pessoais (LGPD), que disciplina o tratamento de informações sensíveis no ordenamento jurídico brasileiro.

A identificação técnica dessas manipulações é um processo complexo, o que torna essencial a colaboração entre autoridades públicas, especialistas em cibersegurança e instituições de pesquisa para o desenvolvimento de mecanismos eficazes de detecção e rastreamento. Nesse sentido, busca-se aprimorar as tecnologias capazes de reconhecer padrões característicos das manipulações digitais promovidas por IA, como os traços gerados por redes neurais artificiais.

Contudo, o enfrentamento da desinformação e da *ciberpolarização* é um fenômeno dinâmico, que exige respostas igualmente evolutivas. A construção de um ambiente digital mais resiliente e informado pressupõe a articulação permanente entre Estado, sociedade civil, setor tecnológico e mídia.

No Brasil, uma abordagem jurídica robusta, atualizada e tecnicamente orientada é indispensável para assegurar a proteção da privacidade, coibir práticas difamatórias e delimitar com clareza as esferas de responsabilidade civil e penal. Para além da regulação normativa, torna-se imprescindível fomentar a consciência crítica da população e investir no desenvolvimento e na adoção de tecnologias de verificação e autenticação de conteúdos, pois, somente através de uma atuação multissetorial e integrada, será possível enfrentar os riscos impostos pelas *deepfakes* e preservar a integridade das instituições democráticas.

Referências Bibliográficas

ANDRADE, Otávio Morato. **Governamentalidade algorítmica: democracia em risco?** São Paulo: Dialética, 2022.

BAUMAN, Zygmunt. **Globalização: as consequências humanas**. Trad. Marcus Penchel. Rio de Janeiro: Zahar, 2012.

BENKLER, Yochai; FARIS, Robert; ROBERTS, Hal. **Network propaganda: manipulation, disinformation, and radicalization in American politics**. Nova Iorque: Oxford University Press, 2018.

CRESWELL, J. W. W. **Projeto de pesquisa**: métodos qualitativo, quantitativo e misto. 2. ed. Porto Alegre: Bookman, 2010.

GATINHO, Gislaine Fernanda Carvalho; SILVEIRA, Túlio Belchior Mano da; DIAS, José Wanderley Dallas Reis. Consequências jurídicas da ciberpolarização do deepfake face ao estado democrático de direito. **Revista Contribuciones a Las Ciencias Sociales**, São José dos Pinhais, v.17, n.10, p. 01-23, 2024. Disponível em: https://ojs.revistacontribuciones.com/ojs/index.php/clcs/article/view/12175/7174. Acesso em: 25 jun. 2025.

GUILLOU, Pierre. **Qual é o princípio de funcionamento de um algoritmo de inteligência artificial?** Medium, 2018. Disponível em: https://medium.com/@pierre_guillou/qual-%C3%A9-o-principio-de-funcionamento-de-um-algoritmo-de-intelig%C3%AAncia-artificial-d68619ce2b4. Acesso em: 24 jun. 2025.

LAVAGNOLI, Silvia. **Como surgiu a Inteligência Artificial?** OPENCADD, 2024. Disponível em: https://www.opencadd.com.br/blog/como-surgiu-a-inteligencia-artificial. Acesso em: 24 jun. 2025.

LIMA, Ramalho. **Deepfake: o que é e como funciona?** Techmundo, 2020. Disponível em: https://www.tecmundo.com.br/internet/206706-deepfake-funciona.htm. Acesso em: 24 jun. 2025.

ROBLES-LESSA, Moyana Mariano; CABRAL, Hildeliza Lacerda Tinoco Boechat; SILVESTRE, Gilberto Fachetti. Deepfake: a inteligência artificial e o algoritmo causando riscos à sociedade no ciberespaço. **Revista Jurídica Derecho y Cambio Social**, n. 61, jul-set, 2020. Disponível em: https://www.academia.edu/43394704/Deepfake_a_intelig%C3%AAncia_artificial_e_o_algoritmo_causando_riscos_%C3%A0_sociedade_no_ciberespa%C3%A7o_Deepfake_artificial_intelligence_and_algorithm_causing_risks_to_society_in_cyberspace_. Acesso em: 24 jun. 2025.

SCHROEPFER, Mike. **Creating a dataset and a challenge for deepfakes**. Meta, 2019. Disponível em: https://ai.meta.com/blog/deepfake-detection-challenge/. Acesso em: 25 jun. 2025.

SPENCER, Michael K. **Deep Fake, a mais recente ameaça distópica**. Outras palavras, 2019. Disponível em: https://outraspalavras.net/tecnologiaemdisputa/deep-fake-a-ultima-distopia/. Acesso em: 24 jun. 2025.

SUNSTEIN, Cass R. **Republic: divided democracy in the age of social media**. 3. ed. Princeton Oxford: Princeton University Press, 2018.

WESTERLUND, Mika. The Emergence of Deepfake Technology: A Review. **Technology Innovation Management Review**, vol. 9, issue 11, nov., 2019. Disponível em: https://timreview.ca/sites/default/files/article_PDF/TIMReview_November2019%20-%20D%20-%20Final.pdf. Acesso em: 25 jun. 2025.