JUSTIÇA ELEITORAL E DESINFORMAÇÃO AUTOMATIZADA: REFLEXÕES SOBRE DEEPFAKES E SEGURANÇA DEMOCRÁTICA

ELECTORAL JUSTICE AND AUTOMATED DISINFORMATION: REFLECTIONS ON DEEPFAKES AND DEMOCRATIC SECURITY

Débora Coelho Nunes Campos
Graduanda em Direito pelo Centro Universitário Unidade de Ensino Superior Dom Bosco - UNDB, São Luís - Maranhão.
deboracampos.direito@gmail.com

Emilly Beatriz Andrade Silva
Graduanda em Direito pelo Centro Universitário Unidade de Ensino Superior Dom Bosco - UNDB, São Luís - Maranhão.
emillybeatriz2004@hotmail.com

Kalyne Laura Aguiar de Alencar
Graduanda em Direito pelo Centro Universitário Unidade de Ensino Superior Dom Bosco - UNDB, São Luís - Maranhão.
kalynealencar.drt@gmail.com

Kassandra Kelly Cunha Santos
Bolsista vinculada à Fundação de Amparo à Pesquisa e ao Desenvolvimento Científico e Tecnológico do Maranhão (FAPEMA). Graduanda em Direito do Centro Universitário Dom Bosco. - UNDB, São Luís - Maranhão.
cunhaslz09slz@gmail.com

Josanne Cristina Ribeiro Ferreira Façanha
Doutora e Mestra em Políticas Públicas pela Universidade Federal do Maranhão (UFMA). Doutora em Ciências Jurídicas e Sociais pela Universidad del Museo Social Argentino (UMSA), Professora Adjunto I da Universidade Estadual do Maranhão, campus São Luís/MA, Advogada, Professora permanente do Programa de Mestrado em Estudos Criminológicos (PPGEC/UEMA).
jocrf_2009@hotmail.com.

RESUMO: O presente artigo analisa a crescente utilização de ferramentas de desinformação automatizada, com ênfase nas tecnologias de *deepfakes* e, no contexto da Justiça Eleitoral brasileira. A rápida evolução da inteligência artificial generativa tem intensificado a manipulação audiovisual e a disseminação de notícias falsas, impactando diretamente a integridade do processo democrático, especialmente em períodos eleitorais. A pesquisa apresenta caráter descritivo e exploratório, fundamentando-se em revisão doutrinária, análise de normas do Tribunal Superior Eleitoral (TSE) e estudos técnicos do setor de tecnologia. Os resultados indicam que, apesar de iniciativas como o Programa de Enfrentamento à Desinformação e parcerias com plataformas digitais, permanecem desafios significativos relacionados à detecção de conteúdos sintéticos, à responsabilização de agentes automatizados e à proteção da liberdade de expressão. Conclui-

se que a Justiça Eleitoral necessita aprimorar mecanismos regulatórios, fortalecer estratégias de transparência e investir em educação midiática, adotando medidas preventivas e de responsabilização capazes de mitigar os impactos de *deepfakes* e assegurar a segurança do processo eleitoral em um ambiente digital cada vez mais complexo.

PALAVRAS-CHAVE: *Deepfakes*; Democracia; Desinformação Automatizada; Justiça Eleitoral; Segurança Digital.

ABSTRACT: This article examines the increasing use of automated disinformation tools, with an emphasis on deepfake technologies within the context of the Brazilian Electoral Justice system. The rapid advancement of generative artificial intelligence has intensified audiovisual manipulation and the spread of false information, directly affecting the integrity of the democratic process, especially during electoral periods. The research adopts a descriptive and exploratory approach, grounded in doctrinal review, analysis of regulations issued by the Superior Electoral Court (TSE), and technical studies from the technology sector. The findings indicate that, despite initiatives such as the Anti-Disinformation Program and partnerships with digital platforms, significant challenges remain regarding the detection of synthetic content, the accountability of automated agents, and the protection of freedom of expression. The study concludes that the Electoral Justice must improve regulatory mechanisms, strengthen transparency strategies, and invest in media literacy, adopting preventive and accountability measures capable of mitigating the impacts of deepfakes and ensuring the security of the electoral process in an increasingly complex digital environment.

KEYWORDS: Automated Disinformation;. Deepfake; Democracy. Digital Security; Electoral Justice.

INTRODUÇÃO

A rápida evolução tecnológica das últimas décadas provocou transformações profundasna produção, disseminação e consumo de informação, impactando de forma significativa as dinâmicas da comunicação social e da esfera pública. Nesse contexto, a expansão das redes sociais e das plataformas digitais não apenas ampliou o alcance das mensagens, como também acelerou sua circulação, permitindo que conteúdos atinjam milhares de usuários em tempo real, muitas vezes sem que haja mecanismos eficazes de verificação de sua veracidade. Dessa forma, essas mudanças repercutiram de maneira particularmente intensa na seara política, ao reconfigurar a interação entre eleitores, candidatos e instituições públicas, tornando o ambiente informativo mais volátil, permeável à manipulação e suscetível à propagação de conteúdos enganosos, o que impõe desafios inéditos à transparência e à legitimidade dos processos democráticos.

Diante desse cenário político, surge um fenômeno particularmente preocupante, o uso de *deepfakes*[1] no contexto eleitoral, sendo estes conteúdos audiovisuais sintéticos produzidos por meio de inteligência artificial, capazes de reproduzir de forma realista imagens, vozes e

[1] Conteúdos digitais manipulados com o uso de inteligência artificial, capazes de substituir rostos, vozes ou expressões de forma realista em vídeos, áudios ou imagens, fazendo parecer que alguém disse ou fez algo que nunca aconteceu.

gestos de indivíduos. Tais ferramentas permitem criar, substituir, omitir ou manipular conteúdos multimídia de maneira persuasiva, podendo influenciar a percepção do eleitorado, distorcer narrativas políticas e comprometer a confiança nas instituições eleitorais. Nesse sentido, a Justiça Eleitoral brasileira encontra-se diante de desafios inéditos, pois, embora exista um arcabouço normativo destinado a coibir a utilização desses conteúdos, a sua eficácia prática ainda é limitada frente à sofisticação tecnológica e à disseminação rápida e segmentada de informações falsas.

Nesse sentido, reconhecendo a gravidade do problema, o Tribunal Superior Eleitoral promulgou a Resolução nº 23.732, de 27 de fevereiro de 2024, que altera a Res.-TSE nº 23.610/2019, dispondo sobre a propaganda eleitoral. Essa norma veda expressamente a utilização de conteúdos sintéticos produzidos por inteligência artificial para criar, substituir, suprimir, combinar ou modificar imagens e sons, e impõe ao responsável pela propaganda o dever de informar de forma clara, destacada e acessível que o material foi manipulado artificialmente, indicando a tecnologia empregada. Todavia, apesar da clareza normativa, a aplicação efetiva dessa medida enfrenta entraves significativos, sobretudo relacionados à identificação, rastreamento e responsabilização dos conteúdos, especialmente quando disseminados em plataformas privadas ou por meio de mecanismos automatizados, o que evidencia a necessidade de medidas complementares e integradas.

Desse modo, o problema central que orienta esta pesquisa consiste em compreender como a Justiça Eleitoral pode assegurar a integridade do processo democrático diante da proliferação de desinformação automatizada, em especial *deepfakes*, considerando as limitações tecnológicas, jurídicas e institucionais atualmente existentes. Estudos prévios têm investigado a propagação de notícias falsas e as estratégias de combate à desinformação, mas há lacunas importantes quanto à análise específica de conteúdos sintéticos sofisticados, à eficácia das normas vigentes e à preparação do eleitor para lidar com informações manipuladas digitalmente. Assim, torna-se evidente que o conhecimento acumulado sobre *fake news* tradicionais não se aplica automaticamente a esse fenômeno, exigindo abordagem multidimensional que articule tecnologia, direito e educação midiática.

Em vista disso, a relevância deste estudo é clara, uma vez que compreender os impactos das *deepfakes* sobre o processo eleitoral é essencial para o fortalecimento da segurança democrática e para a formulação de políticas públicas mais eficazes. A pesquisa visa preencher lacunas existentes na literatura, analisando criticamente a aplicação da Resolução nº 23.732/2024, discutindo suas limitações práticas e propondo reflexões sobre estratégias integradas de prevenção, detecção e responsabilização. Além disso, objetiva-se contribuir para o debate acadêmico e institucional acerca da proteção da integridade do processo eleitoral em um ambiente digital em constante transformação, de modo a assegurar que a evolução tecnológica seja orientada em prol da transparência e da legitimidade democrática.

Especificamente, os objetivos deste trabalho consistem em: analisar de forma aprofundada a atuação da Justiça Eleitoral diante da disseminação de conteúdos sintéticos e automatizados, avaliando os mecanismos legais, técnicos e institucionais empregados para identificar,

regular e mitigar os efeitos desses conteúdos sobre a integridade do processo democrático e a formação da opinião pública; identificar os desafios tecnológicos, jurídicos e institucionais envolvidos na detecção e responsabilização de *deepfakes*, considerando tanto a evolução das técnicas de manipulação digital quanto as lacunas normativas e operacionais que podem comprometer a eficácia da Justiça Eleitoral; examinar os impactos potenciais de conteúdos sintéticos e automatizados sobre a legitimidade, transparência e integridade do processo eleitoral, avaliando como sua disseminação pode influenciar a percepção pública, o comportamento do eleitorado e a confiança nas instituições democráticas; e propor recomendações estratégicas para o aprimoramento de políticas públicas, marcos regulatórios digitais e programas educativos voltados à alfabetização midiática do eleitorado, de modo a fortalecer a resiliência da sociedade frente à manipulação de informações, garantindo maior transparência, responsabilização e participação consciente no processo democrático.

Com isso, pretende-se oferecer uma reflexão crítica e aprofundada sobre a interface entre tecnologia, direito e democracia, apresentando subsídios concretos para que os avanços digitais sejam empregados de modo a fortalecer, e não a fragilizar, a segurança e a confiança no sistema eleitoral brasileiro. Para atingir esse propósito, o estudo organiza-se em seis seções interdependentes, que se articulam de forma progressiva, consolidando as principais reflexões e propostas deste trabalho.

METODOLOGIA

A presente pesquisa adota uma abordagem descritiva e exploratória, voltada a compreender de que forma a Justiça Eleitoral brasileira tem enfrentado a disseminação de desinformação automatizada, com ênfase no uso de *deepfakes*, e de que maneira tais práticas impactam a segurança democrática. Buscou-se, portanto, articular os fundamentos teóricos, as normas institucionais e os desafios práticos que permeiam a regulação, detecção e responsabilização de conteúdos sintéticos no contexto eleitoral.

O caráter descritivo da pesquisa justifica-se pela intenção de apresentar, de maneira sistematizada, os principais conceitos, princípios e fundamentos jurídicos que orientam a atuação da Justiça Eleitoral, especialmente no que se refere à Resolução nº 23.732/2024, bem como mapear as iniciativas já implementadas para mitigar os efeitos da desinformação digital. Por sua vez, a dimensão exploratória decorre da escassez de estudos específicos sobre *deepfakes* aplicados ao contexto eleitoral brasileiro, exigindo uma investigação voltada à identificação e análise das estratégias, lacunas e desafios ainda existentes.

Para alcançar os objetivos propostos, foram utilizados procedimentos metodológicos múltiplos. Em primeiro lugar, realizou-se uma pesquisa bibliográfica, com base no Scielo, Google Acadêmico e Portal de Periódicos da Capes, utilizando as palavras-chave *"deepfake"*, *"desinformação política"* e *"processo democrático"*, "*fake news* nas eleições". Foram priorizadas publicações entre 2018 e 2025, nacionais e internacionais, que tratam da intersecção

entre tecnologia, comunicação e regulação eleitoral. O corpus teórico resultante incluiu autores como Aggio (2020), Bachur (2021), Beiguelman (2020), Kaufman (2018), Sunstein (2018), Gomes (2024) e Tavares (2024), além de artigos recentes que abordam o impacto das mídias digitais e da inteligência artificial sobre a integridade democrática.

A análise documental concentrou-se em atos normativos e institucionais do Tribunal Superior Eleitoral (TSE) publicados entre 2020 e 2024, especialmente as Resoluções nº 23.714/2022 e nº 23.732/2024, além de relatórios e comunicados oficiais do Programa Permanente de Enfrentamento à Desinformação (PPED) e do Centro Integrado de Enfrentamento à Desinformação e Defesa da Democracia (CIEDDE), bem como legislações como o Código Penal, a Lei nº 12.965/2014 e a Lei nº 13.709/2018. Também foram examinadas publicações oficiais e notas informativas divulgadas no portal do TSE e em Tribunais Regionais Eleitorais, como o TRE-RJ (2025), com o objetivo de identificar as medidas de prevenção e resposta institucional adotadas.

No campo empírico, foram selecionados três casos representativos de *deepfakes* no contexto político brasileiro, escolhidos por sua ampla repercussão midiática, identificados em sites de notícias como CNN Brasil, Folha de S.Paulo e Justiça Eleitoral e pela relevância para o debate sobre a integridade do processo eleitoral: o vídeo falso de Renata Vasconcellos com pesquisa adulterada; o *deepfake* de William Bonner chamando candidatos de "bandidos"; e o áudio manipulado atribuído a Ciro Gomes, sobre suposta fraude eleitoral.

A investigação aplicou o método de análise de conteúdo, para examinar tanto as narrativas midiáticas quanto as respostas institucionais. As categorias de análise adotadas incluíram: *autoria e intencionalidade, tecnologia empregada, repercussão pública, impacto político-eleitoral e respostas normativas e comunicacionais*. Além disso, procedeu-se a uma análise crítica de casos e experiências nacionais e internacionais sobre combate à desinformação em contextos eleitorais, com foco na aplicação de tecnologias de detecção de *deepfakes* e na eficácia normativa.

Dessa forma, a metodologia empregada buscou integrar fontes de informação teóricas, normativas, técnicas e práticas, possibilitando uma compreensão crítica e contextualizada sobre os desafios e estratégias da Justiça Eleitoral frente à desinformação automatizada. Com isso, pretende-se fornecer subsídios para o debate acadêmico e institucional acerca da proteção da integridade do processo eleitoral, da segurança democrática e da eficácia das políticas públicas voltadas à regulação e mitigação desse fenômeno.

1. PERCURSO HISTÓRICO DA DESINFORMAÇÃO: DOS MEIOS TRADICIONAIS ÀS TECNOLOGIAS DIGITAIS

A propaganda política, enquanto instrumento de influência social e construção de narrativas de poder, não constitui fenômeno recente no contexto brasileiro. Desde o Brasil Império, é possível identificar práticas voltadas à formação e direcionamento da opinião pública, em um

ambiente posteriormente associado ao fenômeno da chamada "politicagem"[2]. Nesse período, a circulação de panfletos, folhetins e manifestos desempenhava papel central na difusão de ideias e na legitimação das autoridades constituídas.

Com o advento do Estado Novo, a atuação do governo de Getúlio Vargas consolidou de forma ainda mais robusta a cultura propagandística no país, conhecida como populismo. Por meio de estratégias comunicacionais organizadas e institucionalizadas, o varguismo elevou a propaganda a um instrumento de controle social e construção da identidade nacional, reforçando ideais nacionalistas e moldando percepções coletivas (Capelato, 1999). Dessa forma, observa-se que a manipulação informacional e a persuasão política atravessam a história brasileira, adequando-se aos meios de comunicação de cada época e demonstrando continuidade entre formas tradicionais e as modernas dinâmicas de desinformação.

A virada digital representa uma ruptura: o surgimento das redes sociais, aliado ao acesso massificado à internet, descentralizou a produção e circulação de informações. Se antes a manipulação dependia de estruturas estatais ou midiáticas, agora qualquer indivíduo ou grupo pode produzir, replicar e impulsionar conteúdos falsos em larga escala. A automatização, com uso de *bots* e algoritmos, ampliou o impacto dessas práticas, criando mecanismos capazes de direcionar narrativas e manipular o debate público. Dessa forma, Aggio menciona:

> A crescente popularidade da comunicação em redes sociais digitais é uma espécie de sonho realizado de todo e qualquer líder político que encampem a máxima populista clássica da representação direta e genuína das vontades do povo sem as intermediações tradicionais que, nessa mesma retórica, são caracterizados como agentes que distorcem, corrompem, quando não sequestram, efetivamente, qualquer possibilidade de estabelecimento de uma relação honesta, transparente e verdadeira entre políticos e "o povo" (Aggio, 2020, p. 03)

Nos últimos anos, o desenvolvimento de tecnologias de inteligência artificial inaugurou uma nova etapa: a desinformação sintética. Diferente de erros ou imprecisões não intencionais, a desinformação é estruturada estrategicamente, muitas vezes aproveitando vulnerabilidades cognitivas, vieses de confirmação e a rápida circulação de conteúdos em ambientes digitais. Nesse sentido, estudos indicam que, em bolhas de opinião política nas redes sociais, os usuários tendem a ser influenciados pela intensa carga emocional que acompanha as mensagens, desativando o processamento crítico do conteúdo e validando informações com base em sentimentos, e não em evidências (Bachur, 2021).

No contexto político, ela se manifesta na forma de notícias falsas, rumores, teorias conspiratórias e conteúdos manipulados, comprometendo o debate público, corroendo a confiança nas instituições e ameaçando a integridade de processos democráticos. A crescente sofisticação tecnológica, especialmente com o uso de inteligência artificial, intensifica seu alcance e potencial de impacto, tornando a compreensão e o combate à desinformação desafios centrais para a sociedade contemporânea.

[2] Termo utilizado para designar práticas políticas distorcidas, movidas por interesses pessoais, corporativos ou partidários, em detrimento do interesse público e do bem comum.

Compreender a trajetória histórica da desinformação política e suas transformações ao longo do tempo permite perceber como práticas antigas de manipulação evoluíram para formas cada vez mais sofisticadas, impulsionadas pelo avanço tecnológico. Nesse contexto, surge uma nova fronteira de desafios para a democracia: os *deepfakes*, capazes de gerar conteúdos audiovisuais hiper-realistas que ameaçam a confiança pública e a integridade dos processos eleitorais. Assim, o próximo capítulo examina a relação entre *deepfakes*, tecnologia e impactos sobre a integridade democrática, buscando compreender os riscos e as implicações desses novos mecanismos de desinformação automatizada.

2. DEEPFAKES, TECNOLOGIA E IMPACTOS SOBRE A INTEGRIDADE DEMOCRÁTICA

Ao longo das últimas décadas, a trajetória da evolução tecnológica tem se caracterizado por um ritmo acelerado e contínuo, propiciando o surgimento de inovações que impactam de maneira significativa diversos setores da sociedade. Nesse contexto, os avanços na produção e na automação de sistemas inteligentes têm possibilitado que algoritmos de aprendizado de máquina e inteligência artificial realizem tarefas complexas com maior precisão e eficiência, sem necessariamente uma intervenção humana especializada, tornando esses comandos popularizados, promovendo transformações profundas em áreas como indústria, comunicação e entretenimento.

Ademais, o surgimento de conceitos emergentes, como é o caso das *deepfakes*, objeto da presente pesquisa, evidencia tanto o potencial inovador dessas tecnologias quanto os desafios éticos que delas decorrem, ao permitir a criação de conteúdos altamente realistas e manipulados, o que suscita questionamentos acerca de privacidade, veracidade da informação e segurança digital. Dessa forma, observa-se que a convergência entre automação, inteligência artificial e novas tecnologias redefine de maneira constante os limites entre realidade e simulação, exigindo reflexão crítica sobre seu impacto social e ético.

Nesse sentido, o conceito de *deepfakes* surgiu em novembro de 2017 na plataforma Reddit, conhecida por suas discussões temáticas. Originalmente, o termo era o apelido de um usuário e também nomeava um fórum dedicado ao uso de tecnologias de aprendizado profundo para substituir os rostos de atrizes pornográficas pelos de celebridades. Embora esse grupo tenha sido removido da plataforma no início de 2018, essa prática continuou a se expandir e se consolidar (Beiguelman, 2020).

Dessa forma, esse fenômeno emergiu a partir do desenvolvimento de algoritmos de inteligência artificial baseados em aprendizado profundo (*deep learning*), um subcampo do aprendizado de máquina que se caracteriza pelo uso de redes neurais compostas por múltiplas camadas, capazes de processar informações de maneira estruturada e executar tarefas complexas. Nesse contexto, conforme aponta a pesquisadora Dora Kaufman em seu estudo *Deep Learning: a Inteligência Artificial que domina a vida do século XXI* (2018), essa abordagem, inspirada no

funcionamento do cérebro humano, permite que sistemas computacionais identifiquem padrões, realizem reconhecimento de imagens, traduzem diferentes idiomas e operem veículos de forma autônoma, aprimorando seu desempenho progressivamente à medida que analisam grandes volumes de dados, sem depender de programação manual detalhada.

É válido ressaltar que a produção de conteúdos audiovisuais sintéticos a partir de inteligência artificial ultrapassa o campo das simples montagens ou edições tradicionais. Trata-se de uma tecnologia capaz de processar grandes volumes de dados visuais e sonoros, identificando padrões complexos de expressões, movimentos e características vocais para gerar sequências inéditas com forte aparência de autenticidade (Beiguelman, 2020). Essa sofisticação técnica permite simular situações que nunca ocorreram, conferindo elevado grau de persuasão aos materiais produzidos, podendo ser realizada por qualquer pessoa.

Diante disso, quando aplicada no contexto democrático, tal tecnologia assume contornos particularmente críticos. Desse modo, a elaboração intencional de conteúdos enganosos pode influenciar percepções eleitorais, prejudicar reputações políticas e difundir narrativas falsas com grande alcance em um curto espaço de tempo. Nesse cenário, ao instalar dúvidas sobre o que é real ou fabricado, a manipulação digital enfraquece a confiança do público nas instituições responsáveis pela condução do processo eleitoral e compromete o debate informado, essencial para a deliberação coletiva.

Além disso, a circulação de representações forjadas intensifica a polarização social. Assim, reforça discursos extremados e dificulta a construção de consensos, componentes indispensáveis ao funcionamento equilibrado das instituições democráticas. Ademais, tais práticas podem impactar negativamente a participação cidadã, sobretudo quando informações fraudulentas relacionadas ao processo eleitoral passam a ser percebidas como legítimas, desmotivando o engajamento do eleitorado e gerando descrença generalizada.

Dessa forma, as aplicações dessa tecnologia colocam em risco dimensões basilares das democracias contemporâneas, como a integridade informacional, a lisura dos pleitos e a liberdade de formação da vontade política. Dessa forma, ao desafiar esses pilares, a produção audiovisual sintética não apenas altera o cenário comunicacional, como também repercute diretamente na qualidade das escolhas coletivas (Tavares, 2024).

Assim, os *deepfakes* configuram um desafio que ultrapassa o campo tecnológico e incide diretamente sobre dinâmicas políticas, sociais e institucionais. Desse modo, compreender seus mecanismos e impactos torna-se essencial para o desenvolvimento de estratégias preventivas que mitiguem a desinformação automatizada e resguardem a confiança pública nos processos eleitorais.

Além disso, o estudo crítico desse fenômeno contribui para identificar lacunas regulatórias, aperfeiçoar métodos de detecção e responsabilização e orientar políticas públicas que integrem tecnologia, direito e educação na proteção da integridade democrática. Portanto, ao reconhecer a complexidade desse cenário, reforça-se a necessidade de respostas coordenadas que assegurem a preservação dos valores das democracias hodiernas.

3. A JUSTIÇA ELEITORAL E O ENFRENTAMENTO ÀS AMEAÇAS DIGITAIS

O Direito Eleitoral constitui ramo especializado do Direito Público responsável por disciplinar os institutos, normas e procedimentos que asseguram o exercício do direito fundamental ao sufrágio, garantindo a materialização da soberania popular e a legitimidade do processo democrático (Gomes, 2020). Seu escopo envolve não apenas a regulamentação das etapas do pleito e a definição das regras de acesso aos cargos políticos, mas também a proteção da integridade do voto e da representatividade popular.

Nesse contexto, a Justiça Eleitoral brasileira consolidou-se como instituição central na preservação da legitimidade do processo democrático, desempenhando papel que transcende a mera organização das eleições. Em cenário marcado por transformações tecnológicas aceleradas, por novos fluxos comunicacionais e pelo avanço de práticas ilícitas sofisticadas, como a desinformação automatizada e a manipulação digital de narrativas públicas, torna-se indispensável analisar como o sistema eleitoral nacional se estrutura para garantir a integridade do voto e a estabilidade institucional. Assim, a atuação da Justiça Eleitoral evolui de um modelo predominantemente reativo e normativo para um paradigma preventivo, estratégico e integrado, que combina ações normativas, fiscalizadoras e tecnológicas.

3.1 ESTRATÉGIAS DA JUSTIÇA ELEITORAL DE ENFRENTAMENTO DAS AMEAÇAS DIGITAIS

A Resolução TSE nº 23.610/2019, posteriormente editada pela Resolução nº 23.732/2024 (Brasil, 2024b), constitui marco normativo no enfrentamento à propaganda política excessiva, estabelecendo o que é permitido ou proibido durante o período eleitoral. Entre seus avanços, destacam-se a proibição de *deepfakes* e conteúdos sintéticos que manipulem a percepção do eleitor, a obrigatoriedade de informar o uso de inteligência artificial nas propagandas, a limitação do uso de robôs para comunicação automatizada e a responsabilização das plataformas digitais pela remoção imediata de conteúdos que disseminem desinformação, discurso de ódio ou antidemocráticas, racistas e homofóbicas.

Ademais, a Resolução n.º 23.714/2022 (Brasil, 2022b) surge com o objetivo específico de regulamentar o enfrentamento à desinformação no processo eleitoral brasileiro, estabelecendo diretrizes para a prevenção, fiscalização e responsabilização de conteúdos falsos ou manipulativos que possam comprometer a integridade das eleições.

Além das normas estabelecidas, devido aos embates digitais à democracia, observa-se uma ampliação significativa de iniciativas que visam mitigar riscos democráticos e proteger o eleitor contra interferências indevidas, criação de estruturas especializadas, como o Programa Permanente de Enfrentamento à Desinformação (PPED), instituído pela Portaria-TSE nº 510, de 4 de agosto de 2021 (Brasil, 2021), com a finalidade de mitigar os efeitos nocivos de informações falsas relacionadas à própria Justiça Eleitoral, ao sistema eletrônico de votação e às etapas do processo eleitoral, excluindo, porém, conteúdos direcionados a candidatos e partidos,

salvo quando capazes de comprometer a integridade e a legitimidade do pleito.

Em complemento, a Portaria TSE nº 282/2022 instituiu o Programa de Fortalecimento da Imagem da Justiça Eleitoral (PROFI) (Brasil, 2022a), destinado a promover a confiança social na idoneidade das eleições e a reforçar a percepção de imparcialidade, profissionalismo e relevância institucional da Justiça Eleitoral.

Outrossim, o Centro Integrado de Enfrentamento à Desinformação e Defesa da Democracia (CIEDDE) atua de forma articulada com tribunais regionais, órgãos de fiscalização, plataformas digitais e entidades de checagem de fatos, buscando monitorar conteúdos falsos e coordenar respostas rápidas às ameaças ao ambiente eleitoral. Além disso, o centro desempenha papel educativo e de conscientização, promovendo campanhas para fortalecer a confiança da sociedade na Justiça Eleitoral e na lisura das eleições, contribuindo para a defesa da democracia em um contexto de crescente vulnerabilidade informacional.

Juntos, esses programas consolidam uma atuação preventiva, educativa e institucional, reafirmando o compromisso do Tribunal Superior Eleitoral com a proteção da democracia em um ambiente comunicacional crescentemente vulnerável à manipulação informacional. Ocorre, entretanto, que essa demanda recente ainda enfrenta obstáculos para sua plena consolidação, seja pela velocidade das inovações tecnológicas, seja pelas complexidades do ecossistema digital. Tais limitações evidenciam a necessidade de reflexão crítica sobre os instrumentos regulatórios e as soluções tecnológicas disponíveis, abrindo caminho para a análise aprofundada dos desafios regulatórios e tecnológicos que impactam a atuação da Justiça Eleitoral no enfrentamento da desinformação.

4. DESAFIOS REGULATÓRIOS E TECNOLÓGICOS

4.1 LIMITES PRÁTICOS DA DETECÇÃO DE DEEPFAKES

A rápida evolução das tecnologias de inteligência artificial tem proporcionado tanto benefícios quanto desafios inéditos, especialmente no campo da informação digital. No contexto da desinformação automatizada, um dos aspectos mais delicados é a detecção de *deepfakes*. Atualmente, existem algoritmos e sistemas baseados em IA projetados para identificar manipulações digitais, como as técnicas fundamentadas em Redes Neurais Convolucionais (CNNs).

Nesse sentido, o autor Servian (2025) destaca que essas redes se tornaram a base de muitos métodos de detecção, pois são capazes de aprender automaticamente padrões visuais complexos em imagens e vídeos, diferenciando elementos sutis. Modelos como *XceptionNet, ResNet101 e Faster R-CNN* analisam detalhes imperceptíveis ao olho humano, como bordas, texturas e contrastes, para identificar alterações. Em vídeos, essas redes também podem examinar sinais biológicos, como o pulso detectado por variações na cor da pele, os quais *deepfakes* geralmente

não conseguem reproduzir com fidelidade. Apesar de eficazes, essas técnicas ainda enfrentam desafios significativos, uma vez que a rápida evolução das falsificações de *deepfakes* geradas por Redes Adversariais Generativas (GANs) cria um cenário de constante adaptação mútua entre criadores e detectores, caracterizando uma verdadeira corrida tecnológica. O processo de treinamento adversarial das GANs, que envolve a interação entre um gerador e um discriminador, é projetado para aprimorar continuamente o realismo das amostras sintéticas, tornando-as cada vez mais difíceis de distinguir do conteúdo autêntico (Langguth et al, 2021 apud Servian, 2025).

Além disso, os detectores de *deepfakes* também são vulneráveis a estratégias adversariais (Langguth et al, 2021 apud Servian, 2025), que consistem em pequenas alterações, frequentemente imperceptíveis ao olho humano, aplicadas a imagens ou vídeos para induzir o modelo a classificá-los erroneamente, por exemplo, considerando um *deepfake* como autêntico. Assim, cada avanço tecnológico voltado à criação de falsificações realistas tende a desafiar e superar os métodos existentes de identificação, tornando o processo de verificação cada vez mais complexo e incerto.

A detecção de *deepfakes* e outras falsificações digitais requer investimento contínuo em pesquisa, sobretudo em instituições públicas, visando reduzir a dependência de soluções externas e garantir autonomia tecnológica. Entretanto, a implementação dessas ferramentas enfrenta obstáculos práticos relevantes. O elevado custo para desenvolver e manter sistemas de detecção de alto desempenho constitui um desafio, uma vez que soluções eficazes demandam grande poder computacional, muitas vezes inacessível para órgãos públicos menores. Além disso, a rapidez na disseminação de vídeos e imagens falsificados torna a agilidade na detecção outro ponto crítico: identificar conteúdos manipulados antes que se tornem virais é essencial para mitigar seus efeitos, mas a velocidade com que esses materiais se espalham dificulta a resposta imediata, tornando o combate à desinformação uma tarefa complexa e sujeita a constante atualização tecnológica.

Dessa forma, embora os avanços tecnológicos representem uma ferramenta promissora no combate à desinformação digital, ainda estamos diante de um cenário em que a detecção automática de *deepfakes* é falível e insuficiente. O risco de erro, somado à velocidade de disseminação desses conteúdos nas redes sociais, torna evidente a necessidade de estratégias complementares, como o monitoramento, a cooperação entre instituições e plataformas, e a promoção da alfabetização midiática. Assim, mais do que confiar apenas nos algoritmos, o enfrentamento desse fenômeno exige uma abordagem integrada, multidisciplinar e contínua, capaz de equilibrar inovação tecnológica com responsabilidade social e política.

4. 2 IMPLICAÇÕES JURÍDICAS E ELEITORAIS DAS DEEPFAKES

Outro ponto importante que merece destaque é que, no Brasil, ainda permanecem lacunas jurídicas no combate às *deepfakes*, uma vez que não há legislação específica que criminalize ou regule o uso dessas tecnologias. As normas existentes, como o Código Penal (Brasil,1940), o Marco Civil da Internet (Lei nº 12.965/2014) (Brasil, 2014) e a Lei Geral de Proteção de Dados

(Lei nº 13.709/2018 – LGPD) (Brasil, 2018), oferecem princípios gerais de responsabilidade das plataformas digitais e normas para a proteção digital e da privacidade, mas não oferecem uma resposta específica aos desafios trazidos pelos *deepfakes*, assim há extrema necessidade de uma norma específica, mais rigorosa, voltada para essa tecnologia. Tavares (2024) assinala que, no contexto eleitoral, os *deepfakes* configuram uma ameaça concreta à integridade do processo democrático, pois comprometem a percepção pública da veracidade e manipulam a vontade popular por meio da distorção da imagem de figuras públicas.

Nesse sentido, exemplos recentes reforçam o potencial de impacto das *deepfakes* nas eleições brasileiras. Foi no ano de 2022, o caso mais conhecido envolvendo um vídeo manipulado foi o da jornalista Renata Vasconcellos que mostrava falsamente uma pesquisa de intenção de votos, atribuindo liderança a Jair Bolsonaro, quando, na realidade, Luiz Inácio Lula da Silva liderava (Folha de S. Paulo, 2022). Outros casos incluíram *deepfakes* de William Bonner, supostamente chamava os candidatos à presidência de "bandidos", e um áudio manipulado em que o candidato Ciro Gomes (CNN Brasil, 2022) acusava fraude eleitoral com a ciência das Forças Armadas (Brasil, 2022). Esses exemplos evidenciam o impacto potencial das *deepfakes* na manipulação.

Um entrave prático é a atribuição de autoria e responsabilidade. Identificar quem criou, compartilhou ou impulsionou um *deepfake* é uma tarefa complexa, especialmente diante da fronteira entre o dolo humano e a automação algorítmica. Além disso, a volatilidade das provas digitais evidencia um vazio normativo que demanda reflexão doutrinária e atualização legislativa (Do Norte Filho; Vieira; Rodrigues, 2025). Deste modo, a responsabilidade não recai apenas sobre o autor original da falsificação, mas nos usuários que compartilham o conteúdo e nas plataformas que o hospedam ou distribuem também podem contribuir para a propagação do material. Esse cenário levanta questões jurídicas delicadas sobre responsabilidade solidária, ainda em debate, pois envolve equilibrar a proteção à liberdade de expressão com a necessidade de responsabilização por danos causados pela opinião pública.

Assim, apesar da existência de normas legais e das resoluções específicas do Tribunal Superior Eleitoral (TSE), como a nº 23.610/2019 e sua atualização 23.732/2024, esses desafios ainda persistem. O avanço tecnológico voltado à criação de *deepfakes* realistas tendem a superar os métodos tradicionais de identificação, tornando o processo de verificação cada vez mais sofisticado e incerto. Além disso, a atribuição de autoria e responsabilidade se mostra complexa, agravada pela velocidade de criação e disseminação desses conteúdos, o que exige ferramentas avançadas e constante atualização das técnicas de detecção.

Logo, a educação e conscientização da população surgem como estratégias essenciais para reduzir a vulnerabilidade do eleitorado à desinformação. O enfrentamento das *deepfakes* no período eleitoral exige, portanto, uma abordagem integrada que combine inovação tecnológica, regulação eficaz e participação cidadã, garantindo a preservação da confiança no processo democrático.

5. IMPACTOS SOBRE A DEMOCRACIA E A SOCIEDADE

O avanço das tecnologias de inteligência artificial e o crescimento dos conteúdos sintéticos, como os *deepfakes*, ultrapassam em muito a dimensão meramente técnica e alcançam o alicerce do funcionamento das democracias contemporâneas. Ao manipularem informações e abalar a confiança da população nas instituições, essas práticas reconfiguram o espaço público, modificam as formas de debate político e comprometem tanto a formação da opinião pública quanto a legitimidade das decisões coletivas. Trata-se de uma mutação estrutural na esfera da comunicação, na qual os parâmetros clássicos de racionalidade e verdade perdem força diante de narrativas fabricadas e emocionalmente persuasivas.

Em primeiro lugar, a desinformação automatizada desencadeia uma verdadeira crise de confiança institucional. Em um ambiente digital hiperconectado, os indivíduos são diariamente expostos a um volume massivo de informações, oriundas de múltiplas fontes, sem que existam filtros confiáveis ou mecanismos universais de verificação. Como consequência, a fronteira entre o verdadeiro e o falso se torna difusa, criando um cenário propício à manipulação e à descredibilidade de instituições públicas, veículos de imprensa e autoridades democráticas. Essa perda de confiança mina um dos pilares centrais da democracia: a crença na legitimidade e na imparcialidade das instituições que o sustentam.

Nesse cenário, os *deepfakes* reforçam o fenômeno conhecido como "pós-verdade", em que as emoções e crenças pessoais ganham mais peso do que os fatos. Isso enfraquece o debate racional e compromete a base da democracia, que depende de cidadãos bem informados para escolher de forma consciente.

Como explicam Carvalho Júnior, Carvalho e Sousa (2024):

> "Com o advento da Inteligência Artificial Restrita (IAR), um sistema de máquinas com cognição de nível humano e capacidade de definir metas de forma autônoma, há uma necessidade imperiosa de se avançar na análise dos perigos potenciais para a democracia contemporânea. Isso implica em focar não apenas na análise da tecnologia em si, mas também considerar sua inserção em estruturas econômicas, políticas e sociais."

Ao destacar esse ponto, o autor alerta que o problema da desinformação e dos *deepfakes* não está apenas em sua criação, mas em como essas ferramentas podem ser usadas para manipular o discurso público, interferir na formação da vontade do eleitor e comprometer a legitimidade democrática. Assim, compreender o impacto da IA exige uma visão sistêmica, que considere seus efeitos éticos, sociais e institucionais, e não apenas o aspecto tecnológico.

Ora, os impactos atingem a legitimidade eleitoral. Quando conteúdos falsos são atribuídos a candidatos ou instituições, o processo de escolha do eleitor fica vulnerável à manipulação. A decisão de voto, que deveria refletir a vontade livre e consciente do cidadão, passa a ser influenciada por informações distorcidas.

Outro efeito preocupante é o aumento da polarização social. A circulação de *deepfakes*

reforça estereótipos e alimenta discursos de ódio, intensificando a radicalização política. As redes sociais, ao priorizarem conteúdos que geram engajamento, acabam amplificando mensagens sensacionalistas e divisivas. Isso cria verdadeiras "bolhas digitais", nas quais grupos passam a consumir apenas informações que confirmam suas próprias visões, o que dificulta o diálogo e enfraquece o senso de comunidade.

Esse fenômeno está relacionado ao que Pariser (2012) chama de "filtro invisível", mecanismo pelo qual os algoritmos selecionam o que o usuário vê, com base em suas preferências, reforçando apenas opiniões semelhantes. De forma semelhante, Sunstein (2018) explica que esse processo leva à "polarização de grupo", quando pessoas com ideias parecidas se reúnem em ambientes fechados e passam a adotar posições cada vez mais radicais. Nesses espaços, a emoção substitui a razão, e a troca de ideias dá lugar à confirmação do que já se acredita. Assim, a combinação entre tecnologia, algoritmos e desinformação cria um terreno propício à intolerância e à perda do diálogo democrático.

No campo jurídico e institucional, os desafios são igualmente grandes. A falta de uma legislação específica sobre conteúdos sintéticos dificulta a responsabilização de quem cria ou divulga essas manipulações, enquanto a velocidade com que elas se espalham torna insuficientes os mecanismos tradicionais de controle. Diante disso, o Direito precisa se adaptar ao ambiente digital, buscando equilibrar a regulação dessas práticas sem violar direitos fundamentais como a liberdade de expressão e o acesso à informação. Além disso, a desinformação automatizada afeta a educação midiática. O problema não está apenas na ausência de leis, mas na falta de preparo da população para reconhecer conteúdos falsos.

Em síntese, os impactos dos *deepfakes* e da desinformação automatizada são multidimensionais. Enfrentar esse desafio requer mais do que novas leis ou tecnologias: é preciso investir em educação, cultura e ética digital, de modo a reconstruir a confiança, estimular o pensamento crítico e promover uso responsável da informação pela democracia.

6. RESULTADOS, DISCUSSÕES E LIMITAÇÕES

Os resultados desta pesquisa evidenciam que a Justiça Eleitoral brasileira tem adotado um conjunto de medidas cada vez mais estruturadas para combater a desinformação e seus efeitos sobre o processo democrático, especialmente diante do avanço das tecnologias de inteligência artificial e da disseminação dos *deepfakes*. Tais ações demonstram uma evolução institucional significativa, ainda que permeada por desafios relacionados à velocidade tecnológica e à necessidade de integração entre diferentes setores.

Conforme a Justiça Eleitoral, o combate à desinformação foi um dos principais temas de destaque do primeiro semestre de 2024, reforçando o compromisso do Tribunal Superior Eleitoral (TSE) com a proteção da integridade das eleições. A matéria destaca que o órgão intensificou parcerias com plataformas digitais, universidades e agências de checagem, consolidando um modelo de atuação preventiva e cooperativa no enfrentamento às notícias falsas e à manipulação

de informações relacionadas ao processo eleitoral (Brasil, 2024).

Segundo o próprio TSE, as ações incluíram o fortalecimento do Programa Permanente de Enfrentamento à Desinformação (PPED) e do Centro Integrado de Enfrentamento à Desinformação e Defesa da Democracia (CIEDDE), criados para monitorar conteúdos suspeitos e coordenar respostas rápidas em parceria com os Tribunais Regionais Eleitorais (TREs). Essas iniciativas também tiveram caráter educativo, buscando orientar o eleitor sobre como identificar e denunciar informações falsas, um passo essencial para reduzir o impacto das *fake news e deepfakes* sobre a opinião pública.

Além disso, em 1º de abril de 2024, data simbolicamente escolhida por coincidir com o "Dia da Mentira", o TSE lançou uma ampla campanha de enfrentamento à desinformação, atualizando normas e reforçando diretrizes sobre o uso de inteligência artificial, *deepfakes* e robôs de comunicação em propagandas eleitorais (Brasil, 2024c). Nessa ocasião, o Tribunal reafirmou o papel central da Resolução nº 23.732/2024, que proíbe expressamente o uso de conteúdos sintéticos para manipular imagens, vozes e vídeos de candidatos, como estabelece a obrigação de identificar publicamente materiais gerados por inteligência artificial.

De acordo com o então presidente da Corte, ministro Alexandre de Moraes, a medida busca "garantir que o uso de novas tecnologias se dê de forma ética, transparente e responsável, sem comprometer a confiança do eleitor nem o equilíbrio da disputa" (Brasil, 2024c). Essa postura demonstra uma mudança de paradigma: a Justiça Eleitoral passa de uma atuação predominantemente reativa, centrada em punições, para um modelo preventivo, pedagógico e colaborativo, que combina regulação, conscientização e inovação tecnológica.

Os impactos dessas políticas começam a aparecer nos dados institucionais. Segundo relatórios do TSE, entre junho e outubro de 2024, o Sistema de Alerta de Desinformação (SIADE) recebeu mais de 5.200 registros de denúncias relacionadas a conteúdos falsos sobre as eleições, dos quais cerca de 2.100 foram encaminhados às plataformas digitais para análise e remoção. Esses números revelam não apenas o volume de tentativas de manipulação, mas também a capacidade operacional do Tribunal em responder rapidamente às ameaças digitais (Brasil, 2024a).

Do ponto de vista qualitativo, as ações também têm repercutido positivamente na percepção pública sobre a credibilidade do sistema eleitoral. Pesquisas internas mencionadas nas próprias comunicações do TSE apontam que a confiança no processo eletrônico de votação cresceu após a intensificação das campanhas de esclarecimento, especialmente entre os eleitores mais jovens. Isso indica que a combinação entre transparência institucional, comunicação direta e educação digital pode ser uma estratégia eficiente para conter a influência da desinformação automatizada.

Em âmbito regional, observa-se que os Tribunais Regionais Eleitorais também têm desempenhado papel importante nesse processo. Um exemplo disso foi a palestra "A responsabilidade do impacto das informações nas eleições", promovida pela Escola da Magistratura do Estado do Rio de Janeiro (EMERJ) e pela Escola Judiciária Eleitoral Desembargador Roberto Felinto (EJE/TRE-RJ), em 21 de outubro de 2025, que discutiu os

riscos da desinformação, o uso de inteligência artificial e o papel das redes sociais no processo democrático (Brasil, 2025).

Na ocasião, a desembargadora Maria Helena Pinto, diretora da EJE/TRE-RJ, destacou que "a desinformação sempre existiu, mas agora ela se aprimorou e cresceu, sendo divulgada de forma tão próxima à realidade que muitas vezes o eleitor não consegue distinguir o falso do verdadeiro". A ministra do TSE Estela Aranha, que participou do evento, acrescentou que a polarização política intensificada pelas redes sociais e pelo ecossistema da desinformação exige uma atuação combinada de tecnologia, direito e educação midiática.

Esses exemplos reforçam que o enfrentamento da desinformação no Brasil vai além da esfera normativa: envolve um esforço educativo e cultural em nível nacional e regional, integrando magistrados, instituições públicas e sociedade civil.

Apesar dos avanços, o cenário ainda impõe desafios significativos. O primeiro deles é tecnológico: os algoritmos de detecção de *deepfakes* e os mecanismos de rastreamento de desinformação ainda não acompanham a velocidade com que novas falsificações são produzidas e disseminadas nas redes. Outro desafio é jurídico, já que o país ainda não dispõe de legislação penal específica para responsabilizar autores de conteúdos sintéticos, o que exige da Justiça Eleitoral uma constante interpretação adaptativa das normas já existentes, como o Código Eleitoral e o Marco Civil da Internet.

Por fim, permanece o desafio educacional e social. Combater a desinformação não depende apenas de ferramentas tecnológicas ou de resoluções judiciais: requer um eleitor mais crítico, consciente e preparado para reconhecer manipulações. A alfabetização midiática promovida pelo TSE e pelos TREs, portanto, desponta como uma das medidas mais eficazes e sustentáveis para fortalecer a democracia.

CONSIDERAÇÕES FINAIS

Deste modo, com base em todo o levantamento histórico, tecnológico e jurídico apresentado, é possível concluir que a desinformação política no Brasil é um fenômeno de longa duração, que se adapta às mudanças nos meios de comunicação e às transformações, mantendo sua função de influenciar percepções e moldar narrativas de poder. Desde a propaganda impressa do período imperial, passando pelo populismo varguista até as dinâmicas digitais contemporâneas, observa-se uma continuidade na prática de manipulação informacional, que se sofisticou e se ampliou com a disseminação das redes sociais e o advento da inteligência artificial.

Os *deepfakes* representam o ponto mais aprimorado e recente dessa evolução, ao combinar tecnologia avançada com potencial de impacto social imediato. Capazes de gerar conteúdos audiovisuais altamente realistas, essas ferramentas não apenas simulam eventos inexistentes, mas também desafiam a capacidade de detecção e fiscalização dos órgãos públicos, evidenciando lacunas jurídicas, tecnológicas e educacionais. A rapidez de produção e disseminação desses conteúdos, aliada à dificuldade de atribuição de autoria e responsabilidade, coloca em risco

a integridade do processo eleitoral, a confiança nas instituições e a qualidade do debate democrático.

Nesse contexto, a atuação da Justiça Eleitoral brasileira mostra-se estratégica e multifacetada. A criação de programas como o PPED e o CIEDDE, somada à atualização de resoluções específicas sobre o uso de inteligência artificial e conteúdos sintéticos, evidencia um modelo de enfrentamento preventivo, educativo e colaborativo, que combina fiscalização, regulação e conscientização do eleitor. No entanto, os desafios permanecem: a velocidade de evolução tecnológica supera, muitas vezes, os mecanismos de detecção existentes, e a legislação ainda carece de dispositivos específicos voltados à responsabilização e ao controle de conteúdos produzidos por IA generativa.

Portanto, o enfrentamento da desinformação automatizada exige estratégias integradas e operacionais, que combinem inovação tecnológica, regulação eficaz e educação digital. Nesse sentido, recomenda-se: a criação de um módulo específico sobre desinformação sintética a ser incorporado aos programas de educação política da Justiça Eleitoral, voltado à capacitação de eleitores, servidores e mesários, com orientações práticas sobre identificação de *deepfakes* e verificação de fontes; O estabelecimento de parcerias técnicas entre o TSE e universidades públicas, visando ao desenvolvimento de algoritmos nacionais de detecção de conteúdos sintéticos, reduzindo a dependência de soluções estrangeiras e fortalecendo a soberania tecnológica; A elaboração de diretrizes normativas específicas para o uso e a responsabilização de conteúdos produzidos com inteligência artificial durante o período eleitoral, com previsão de sanções e protocolos de resposta rápida; O incentivo a campanhas educativas permanentes em mídias sociais, com foco em literacia digital e análise crítica de informações audiovisuais.

Somente a integração entre esses elementos permitirá mitigar os efeitos das *deepfakes*, preservar a confiança pública e assegurar a integridade democrática, garantindo que o avanço tecnológico seja utilizado como instrumento de fortalecimento, e não de fragilização, das instituições e da participação cidadã. Em última análise, compreender a trajetória histórica e os desafios contemporâneos da manipulação informacional é fundamental para que a democracia brasileira se mantenha resiliente frente às novas formas de desinformação digital.

REFERÊNCIAS

AGGIO, Camilo de Oliveira. Comunicação eleitoral "desintermediada", mas o quão realmente interativa? Jair Bolsonaro e o Twitter nas eleições de 2018. **E-Compós (Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação), v. 23**, Jan–Dez. 2020. DOI: 10.30962/ec.1994.

BACHUR. João Paulo. Desinformação política, mídias digitais e democracia: Como e por que as fake news funcionam?. **RDP**, Brasília, Volume 18, n. 99, 436-469, jul./set. 2021, DOI: https://doi.org/10.11117/rdp.v18i99.5939.

BEIGUELMAN, Giselle. As verdades dos deepfakes. **Revista Zum**, v. 10, n. 18, p. 50-58, 2020.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Rio de Janeiro, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 1 nov. 2025.

BRASIL . **Áudio atribuído a Ciro Gomes com acusação de fraude eleitoral é falso.** Fato ou Boato?, 07 out. 2022. Disponível em: https://www.justicaeleitoral.jus.br/fato-ou-boato/checagens/audio-atribuido-a-ciro-gomes-com-acusacao-de-fraude-eleitoral-e-falso/#. Acesso em: 01 de nov. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, DF, 24 abr. 2014. Disponível em : https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htmAcesso em: 1 nov. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 15 ago. 2018. Disponível em:https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 1 nov. 2025.

BRASIL.Tribunal Regional Eleitoral do Rio de Janeiro.**Desinformação nas eleições é tema de palestra promovida pela EMERJ.** Rio de Janeiro, 21 out. 2025. Disponível em: https://www.tre-rj.jus.br/comunicacao/noticias/2025/Outubro/desinformacao-nas-eleicoes-e-tema-de-palestra-promovida-pela-emerj. Acesso em: 01 nov. 2025.

BRASIL.Tribunal Superior Eleitoral. **Eleições 2024 e enfrentamento da desinformação foram temas de destaque no 1º semestre no TSE.** Brasília, 03 jul. 2024. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Julho/eleicoes-2024-e-enfrentamento-da-desinformacao-foram-temas-de-destaque-no-1o-semestre-no-tse. Acesso em: 01 nov. 2025.

BRASIL. **Tribunal Superior Eleitoral.** Portaria n. 510, de 4 de agosto de 2021.

BRASIL. **Tribunal Superior Eleitoral.** Portaria n.282, de 22 de março de 2022a

BRASIL. **Tribunal Superior Eleitoral.** Relatório 2024a.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.714, de 20 de outubro de 2022b. **Diário da Justiça Eletrônico do TSE.** Brasília, DF, 20 out. 2022.

BRASIL. Tribunal Superior Eleitoral. Resolução n.º 23.732, de 27 de fevereiro de 2024b. Altera a Res.-TSE n.º 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. **Diário da Justiça Eletrônico do TSE**, Brasília, DF, 4 mar. 2024.

BRASIL. Tribunal Superior Eleitoral. **TSE garante compromisso de combate à desinformação com diversas ações.** Brasília 01 abr. 2024c. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Abril/tse-garante-compromisso-de-combate-a-desinformacao-com-diversas-acoes. Acesso em: 31 out. 2025

CAPELATO, Maria Helena R. Multidões em Cena. Propaganda Política no Varguismo e no Peronismo. São Paulo, **Fapesp/ Papirus**, 1998.

CARVALHO JÚNIOR, O. L. de.; CARVALHO, S. S.; SOUSA, B. A. de. Democracia em

xeque: inteligência artificial e Deep Fake. **Revista JRG de Estudos Acadêmicos.** Brasil, São Paulo, v. 7, n. 15, p. e151743, 2024. DOI: 10.55892/jrg.v7i15.1743. Disponível em: https://revistajrg.com/index.php/jrg/article/view/1743. Acesso em: 1 nov. 2025.

CNN BRASIL. **Áudio de William Bonner chamando Lula e Alckmin de "bandidos" é falso e foi feito com ferramenta de deepfake.** São Paulo, 02 agost. 2022. Disponível em: https://www.cnnbrasil.com.br/nacional/audio-de-william-bonner-chamando-lula-e-alckmin-de-bandidos-e-falso-e-foi-feito-com-ferramenta-de-deepfake/. Acesso em 01 de nov. 2025.

DO NORTE FILHO, Antônio Ferreira; VIEIRA, Maria Elvira Ferreira; DE SOUZA RODRIGUES, Isaac Saymon. DEEPFAKES E RESPONSABILIDADE PENAL: NOVOS DESAFIOS PARA O DIREITO PENAL DIGITAL. **Revista DCS**, v. 22, n. 83, p. e3563-e3563, 2025.

FOLHA DE S.PAULO. **É falso vídeo em que o Jornal Nacional apresenta Bolsonaro à frente na pesquisa Ipec.** São Paulo, 17 ago. 2022. Disponível em: https://www1.folha.uol.com.br/poder/2022/09/e-falso-video-em-que-jornal-nacional-apresenta-bolsonaro-a-frente-na-pesquisa-ipec.shtml. Acesso em: em 01 de nov de 2025

GOMES, José Jairo. **Direito eleitoral** - 20. ed., rev., atual. e reform. Barueri [SP] Atlas, 2024.

KAUFMAN, Dora. Deep learning: a Inteligência Artificial que domina a vida do século XXI. **Teccogs:** Revista Digital de Tecnologias Cognitivas, n. 17, 2018. Disponível em n. 17 (2018):Inteligência Artificial | TECCOGS: Revista Digital de Tecnologias Cognitivas . Acesso em: em 01 de nov de 2025.

PARISER, Eli. **O filtro invisível:** o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012.

SERVIAN, Artur Azevedo Santos et al. **Automação inteligente de processos para evitar fraudes analógicas, digitais e os deepfakes das LLMs generativas.** Universidade Federal de Uberlândia. Uberlândia, 2025. Disponível em Automação inteligente de processos para evitar fraudes analógicas, digitais e os deepfakes das LLMs generativas. Acesso em: em 01 de nov de 2025.

SUNSTEIN, Cass R. **#Republic:** Divided Democracy in the Age of Social Media. Princeton: Princeton University Press, 2018.

TAVARES, Cláudio De Mello. Inteligência Artificial e Deepfakes: Desafios Jurídicos e Tecnológicos para a Integridade do Processo Democrático e as Implicações para as Eleições Municipais de 2024. **Revista Justiça Eleitoral em Debate,** v. 14, n. 1, p. 49-58, 2024.