



**UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS - CCSA
DEPARTAMENTO DE GESTÃO PÚBLICA – DGP
BACHARELADO EM GESTÃO PÚBLICA**

LETÍCIA NUNES MEDEIROS

***DEEPFAKES E A CRISE DE CONFIANÇA NA DEMOCRACIA:*
Cenário sobre a Influência da Desinformação por IA nas Eleições de 2026**

**JOÃO PESSOA
2026**

LETÍCIA NUNES MEDEIROS

DEEPPAKES E A CRISE DE CONFIANÇA NA DEMOCRACIA:
Cenário sobre a Influência da Desinformação por IA nas Eleições de 2026

Trabalho de Conclusão de Curso
apresentado à Coordenação do Curso de
Gestão Pública da Universidade Federal
da Paraíba como requisito complementar
para obtenção do título de Bacharel em
Gestão Pública, sob orientação do
professor Dr. Hermann Atila Hrdlicka.

João Pessoa
2026

Catálogo na publicação
Seção de Catalogação e Classificação

M488d Medeiros, Letícia Nunes.

Deepfakes e a crise de confiança na democracia:
cenário sobre a influência da desinformação por IA nas
Eleições de 2026 / Letícia Nunes Medeiros. - João
Pessoa, 2026.
32 f. : il.

Orientação: Dr Hermann Atila Hrdlicka.
TCC (Graduação) - UFPB/CCSA.

1. Deepfakes. 2. Gestão pública. 3. Desinformação
eleitoral. 4. Processo eleitoral brasileiro. 5.
Eleições 2026. I. Hrdlicka, Dr Hermann Atila. II.
Título.

UFPB/CCSA

CDU 35

LETÍCIA NUNES MEDEIROS

DEEPPAKES E A CRISE DE CONFIANÇA NA DEMOCRACIA:
Cenário sobre a Influência da Desinformação por IA nas Eleições de 2026

Trabalho de conclusão de curso submetido à Banca Examinadora designada pelo Curso de Graduação em Gestão Pública da Universidade Federal da Paraíba como requisito para obtenção do título de Bacharel em Gestão Pública.

BANCA EXAMINADORA



Assinatura: _____

Prof. Dr. Hermann Atila Hrdlicka
(Orientador)

Assinatura: _____

Prof. Dr. Geraldo Magela de Andrade
(Examinador)

Assinatura: _____

Prof. Dr. Flavio Perazzo Barbosa Mota
(Suplente)

João Pessoa, 30 de março de 2026.

Dedico àqueles que vêm me apoiando ao longo da vida facilitando a minha caminhada. Em especial, aos meus pais Anderson e Deise.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por me sustentar ao longo desta jornada. Aos meus pais, Anderson e Deise, pelo amor incondicional, apoio incansável e por nunca medirem esforços para que eu pudesse realizar meus sonhos. Ao meu orientador, Professor Dr. Hermann Atila, pelos ensinamentos que transcendem esta pesquisa. Aos professores do Departamento de Gestão Pública da UFPB, por todo conhecimento compartilhado ao longo da graduação. Aos meus amigos e colegas de curso, que tornaram essa caminhada mais leve e significativa. Por fim, a todos que direta ou indiretamente contribuíram para a realização deste trabalho, minha eterna gratidão.

“Uma democracia saudável depende de cidadãos capazes de distinguir fatos de ficção.”

Yuval Noah Harari
Nexus

RESUMO

As eleições de 2026 ocorrerão em um cenário de maturidade tecnológica dos *deepfakes* – vídeos e áudios sintéticos gerados por inteligência artificial com alto poder de enganar. Este fenômeno recoloca em debate a fragilidade da confiança pública em contextos eleitorais. O presente Trabalho de Conclusão de Curso tem como objetivo analisar possíveis cenários sobre a influência dos *deepfakes* no processo eleitoral brasileiro, considerando diferentes respostas institucionais. O problema que orienta a pesquisa é: quais cenários podem se desenhar para as eleições de 2026 a partir da influência dos *deepfakes* sobre a confiança do eleitor e sobre o debate público? A pesquisa adota abordagem qualitativa, com base em análise documental de relatórios do Tribunal Superior Eleitoral, da Controladoria-Geral da União e de organismos internacionais, além do exame de casos reais de *deepfakes* identificados entre 2024 e 2025. A partir da literatura sobre desinformação e vieses cognitivos, discute-se como esses conteúdos afetam a percepção dos eleitores. Por fim, são construídos cenários prospectivos que apontam possíveis consequências da atuação (ou omissão) da gestão pública no enfrentamento da desinformação artificial. Conclui-se que o futuro da integridade eleitoral estará diretamente relacionado à capacidade institucional de antecipar-se a esses novos formatos de manipulação.

Palavras-chave: *Deepfakes*. Gestão Pública. Desinformação Eleitoral. Cenários. Eleições 2026.

ABSTRACT

The 2026 elections will take place in a scenario of technological maturity of *deepfakes* – synthetic videos and audios generated by artificial intelligence with a high capacity to deceive. This phenomenon brings back into debate the fragility of public trust in electoral contexts. This undergraduate thesis aims to analyze possible scenarios regarding the influence of *deepfakes* on the Brazilian electoral process, considering different institutional responses. The research problem is: what scenarios can unfold for the 2026 elections based on the influence of *deepfakes* on voter trust and public debate? The research adopts a qualitative approach, based on documentary analysis of reports from the Superior Electoral Court, the Office of the Comptroller General, and international organizations, in addition to examining real cases of *deepfakes* identified between 2024 and 2025. Based on the literature on disinformation and cognitive biases, it discusses how these contents affect voters' perception. Finally, prospective scenarios are constructed that point out possible consequences of the action (or omission) of public management in confronting artificial disinformation. It is concluded that the future of electoral integrity will be directly related to the institutional capacity to anticipate these new forms of manipulation.

Keywords: *Deepfakes*. Public Management. Electoral Disinformation. Scenarios. 2026 Elections.

LISTA DE SIGLAS E ABREVIATURAS

TSE– Tribunal Superior Eleitoral

CGU– Controladoria-Geral da União

LGPD – Lei Geral de Proteção de Dados

PL – Projeto de Lei

IA – Inteligência Artificial

UE – União Europeia

MPF – Ministério Público Federal

DFRLab– Digital Forensic Research Lab

DSA – Digital Services Act

GAN – Generative Adversarial Network

IDP – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa

IREE – Instituto para Reforma das Relações Estado-Empresa

NetzDG – Network Enforcement Act (Alemanha)

TRE – Tribunal Regional Eleitoral

STF – Supremo Tribunal Federal

SUMÁRIO

INTRODUÇÃO.....	1
1.1 Conceito, evolução e funcionamento dos <i>Deepfakes</i>	3
1.2 <i>Deepfakes</i> como ferramenta de desinformação	3
1.3 Impactos da desinformação na democracia contemporânea.....	4
2 GESTÃO PÚBLICA E SEGURANÇA DIGITAL	5
2.1 Governança digital no setor público brasileiro	5
2.2 O papel do TSE e da CGU no combate à desinformação	5
2.3 Limites e alcance das respostas institucionais atuais.....	6
2.4 Experiências internacionais no enfrentamento a <i>deepfakes</i>	6
3 A INFLUÊNCIA DOS DEEPFAKES SOBRE O ELEITOR.....	7
3.1 Mecanismos psicológicos: viés de confirmação e heurísticas	7
3.2 Evidências empíricas sobre o impacto da desinformação	7
3.2.3 Dados consolidados das eleições de 2024	8
3.2.4 Levantamento do Digital Forensic Research Lab (DFRLab)	9
3.2.5 Casos emblemáticos documentados	9
3.3 Percepção do eleitor brasileiro sobre <i>deepfakes</i> e desinformação	10
3.4 <i>Deepfakes</i> e a erosão da confiança nas instituições	10
4. CENÁRIOS PARA 2026: POSSIBILIDADES EM ABERTO	11
4.1 O contexto regulatório em construção	11
4.2 Cenário 1 – Omissão institucional e agravamento da crise	12
4.3 Cenário 2 – Respostas pontuais e efeitos limitados	13
4.4 Cenário 3 – Atuação coordenada e mitigação de danos	13
4.5 Síntese dos cenários	14
4.6 O que está em jogo	15
5 CONSIDERAÇÕES FINAIS.....	16
REFERÊNCIAS.....	19
APÊNDICE	22

INTRODUÇÃO

Nos últimos anos, a inteligência artificial deixou de ser uma promessa distante para se tornar uma ferramenta cotidiana, presente em aplicativos, redes sociais e dispositivos pessoais. Entre suas aplicações mais controversas estão os *deepfakes* – vídeos, áudios e imagens gerados ou alterados por algoritmos de aprendizado profundo, capazes de simular com precisão assustadora a aparência e a voz de pessoas reais. O que antes exigia estúdios e equipes especializadas hoje pode ser feito por qualquer pessoa com acesso a softwares relativamente simples. Esse avanço tecnológico, embora impressionante, carrega consigo um risco silencioso: a possibilidade de tornar indistinguível o real do fabricado. Em sociedades democráticas, onde o debate público se alimenta da confiança nas informações, essa indistinção representa uma ameaça direta à própria noção de verdade. Quando um vídeo falso pode mostrar um candidato dizendo algo que nunca disse, ou um áudio manipulado pode simular uma confissão comprometedora, as bases da deliberação pública começam a ruir.

"Quando a confiança no que se vê e ouve é abalada, a própria possibilidade de deliberação pública entra em colapso. Na era digital, a percepção da realidade torna-se fragmentada e sujeita a manipulações que antes eram impensáveis." (HAN, Byung-Chul. Infocracia, 2022, p. 67-68).

O Brasil não é estranho aos efeitos da desinformação em contextos eleitorais. As eleições de 2018 e 2022 já haviam demonstrado o poder disruptivo de notícias falsas compartilhadas em massa por aplicativos de mensagens e redes sociais. No entanto, os *deepfakes* representam um salto qualitativo nesse cenário. Diferentemente dos boatos textuais ou imagens grosseiramente editadas, os *deepfakes* exploram a confiança que o ser humano deposita no que vê e ouve. Em 2025, a tecnologia atingiu um patamar em que mesmo especialistas têm dificuldade para identificar manipulações. Isso coloca as eleições de 2026 em uma posição delicada: pela primeira vez, o país enfrentará uma disputa nacional em que grande parte do eleitorado estará exposta a conteúdos audiovisuais potencialmente falsos, sem necessariamente dispor de ferramentas ou informações para distingui-los. A questão, portanto, não é apenas tecnológica, mas também política e social, na medida em que a confiança nas instituições e nos processos democráticos pode ser profundamente abalada.

Diante desse cenário, uma questão se impõe como ponto de partida para a reflexão acadêmica: diante do avanço dos *deepfakes* e da experiência recente com desinformação eleitoral, quais cenários podem se desenhar para as eleições de 2026 no Brasil a partir da influência desses conteúdos sobre a confiança do eleitor? Para responder a essa pergunta, o

presente trabalho estabelece como objetivo geral analisar possíveis cenários sobre a influência dos *deepfakes* no processo eleitoral de 2026, considerando diferentes respostas institucionais. De forma mais específica, busca-se: (a) mapear casos concretos de *deepfakes* em eleições recentes, no Brasil e no exterior, identificando seus contextos de ocorrência e consequências imediatas; (b) compreender, a partir da literatura sobre desinformação e psicologia cognitiva, os mecanismos pelos quais esses conteúdos afetam a percepção e a decisão do eleitor; e (c) discutir, em perspectiva prospectiva, os possíveis desdobramentos para 2026, considerando desde a omissão institucional até respostas mais coordenadas por parte dos órgãos públicos.

A relevância deste estudo reside em pelo menos três dimensões. A primeira é a atualidade do tema: em um momento em que *deepfakes* se tornam cada vez mais realistas e acessíveis, compreender seus potenciais impactos sobre o processo eleitoral é tarefa urgente para gestores públicos, pesquisadores e cidadãos. A segunda dimensão é a lacuna acadêmica que se busca preencher: embora haja crescente produção sobre fake news e desinformação, ainda são escassos os trabalhos que analisam especificamente os *deepfakes* sob a ótica da gestão pública e da prospecção de cenários. A terceira dimensão é prática: ao construir cenários possíveis para 2026, este trabalho pretende oferecer subsídios para que gestores públicos possam antecipar riscos e planejar ações, sem, contudo, prescrever caminhos únicos ou definitivos. Mais do que um manual de soluções, o que se propõe aqui é um exercício de reflexão fundamentada sobre os caminhos que a democracia brasileira pode tomar diante de uma tecnologia que desafia não apenas os sistemas de verificação, mas a própria confiança na realidade compartilhada.

1. **DEEPPAKES E DESINFORMAÇÃO DIGITAL**

1.1 Conceito, evolução e funcionamento dos *Deepfakes*

O termo *deepfake* surge da combinação das palavras deep learning (aprendizado profundo) e fake (falso) (Chesney; Citron, 2019). Trata-se de uma técnica que utiliza redes neurais artificiais para criar ou alterar conteúdos audiovisuais com alto grau de realismo. Diferentemente das edições tradicionais, que exigem intervenção manual e conhecimento técnico especializado, os *deepfakes* são gerados por algoritmos que aprendem padrões a partir de grandes volumes de dados. Como explicam Chesney e Citron (2019), a tecnologia por trás dos *deepfakes* evoluiu rapidamente nos últimos anos, tornando possível a manipulação de vídeos e áudios de forma acessível até mesmo para usuários sem formação técnica.

O funcionamento básico dos *deepfakes* envolve duas redes neurais adversárias: uma responsável por gerar o conteúdo falso e outra por tentar identificá-lo. Esse processo, conhecido como GAN (Generative Adversarial Network), permite que os resultados se tornem cada vez mais precisos à medida que as redes competem entre si (GOODFELLOW et al., 2014). O que antes era uma promessa de laboratório tornou-se, em poucos anos, uma ferramenta disponível em aplicativos e plataformas online.

"As redes adversárias generativas representam um dos avanços mais significativos da inteligência artificial na última década, permitindo a criação de imagens, vídeos e áudios sintéticos com qualidade indistinguível da realidade. Sua aplicação, no entanto, levanta questões éticas profundas quando utilizada para fins de desinformação." (GOODFELLOW, Ian et al. Generative Adversarial Networks, 2014, p. 2).

1.2 *Deepfakes* como ferramenta de desinformação

Embora a tecnologia tenha aplicações legítimas, como no entretenimento e na educação, seu uso para fins de desinformação tem gerado preocupação crescente. Os *deepfakes* exploram justamente o que há de mais vulnerável na percepção humana: a confiança no que se vê e ouve. Diferentemente de boatos textuais, que exigem leitura e interpretação, os conteúdos audiovisuais falsos apelam diretamente à emoção e à memória visual do espectador (VACCARI, 2020).

No contexto político, os *deepfakes* podem ser utilizados para difamar adversários, simular declarações falsas ou até mesmo desacreditar instituições. Um exemplo emblemático

ocorreu nos Estados Unidos, em 2023, quando um vídeo manipulado de um candidato ao Congresso viralizou nas redes sociais, gerando confusão entre eleitores e exigindo desmentidos oficiais (THE WASHINGTON POST, 2023). No Brasil, embora ainda incipientes, os casos começam a aparecer: em 2024, pelo menos três prefeituras registraram ocorrências de vídeos falsos envolvendo gestores municipais. Como alerta Santaella (2021, p. 45), “a desinformação na era digital não é apenas um problema de informação falsa, mas de destruição da própria confiança nos mecanismos de verificação.”

1.3 Impactos da desinformação na democracia contemporânea

A relação entre desinformação e democracia é antiga, mas os *deepfakes* conferem ao problema uma nova dimensão. Em regimes democráticos, a legitimidade do processo eleitoral depende, em grande medida, da capacidade dos cidadãos de formarem opiniões com base em informações confiáveis. Quando essa base é corrompida por conteúdos falsos hiper-realistas, o próprio sentido do voto pode ser comprometido (LEVITSKY; ZIBLATT, 2018).

Além disso, os *deepfakes* contribuem para o que alguns autores denominam erosão epistêmica, ou seja, o enfraquecimento da capacidade social de distinguir verdade e mentira (BENKLER; FARIS; ROBERTS, 2018). Em um ambiente onde qualquer vídeo pode ser falso, até mesmo os conteúdos legítimos passam a ser vistos com desconfiança. Esse fenômeno alimenta a chamada pós-verdade, na qual os fatos objetivos perdem relevância diante de apelos emocionais e crenças pessoais (KEYES, 2004).

"A pós-verdade não é simplesmente a era das mentiras, mas sim um momento histórico em que as mentiras ganham contornos de verdade porque atendem a demandas afetivas do público. Nesse contexto, os *deepfakes* atuam como catalisadores, oferecendo 'provas' audiovisuais para narrativas que antes dependiam apenas de palavras." (KEYES, Ralph. A Era da Pós-Verdade, 2004, p. 89).

2 GESTÃO PÚBLICA E SEGURANÇA DIGITAL

2.1 Governança digital no setor público brasileiro

A transformação digital alcançou também a administração pública, impulsionando o conceito de governança digital. Trata-se da incorporação de tecnologias da informação e comunicação aos processos governamentais, com o objetivo de ampliar a transparência, a eficiência e a participação social (MELLO, 2021). No Brasil, iniciativas como o Portal da Transparência e a Lei de Acesso à Informação (Lei nº 12.527/2011) representam marcos importantes nessa trajetória.

No entanto, a mesma infraestrutura digital que viabiliza serviços públicos mais ágeis também expõe o Estado a novos riscos. A proliferação de *deepfakes* insere-se nesse contexto como uma ameaça à credibilidade das informações oficiais e à confiança da população nas instituições. Como observa Hood (1991), a modernização administrativa frequentemente ocorre em ritmo mais lento do que a evolução dos riscos que busca enfrentar.

"A administração pública digital não pode limitar-se a oferecer serviços online; precisa também desenvolver capacidades institucionais para identificar, monitorar e responder a ameaças digitais que comprometam a confiança dos cidadãos nas informações governamentais." (MELLO, Christian. Administração Pública 4.0, 2021, p. 112).

2.2 O papel do TSE e da CGU no combate à desinformação

No âmbito eleitoral, o Tribunal Superior Eleitoral (TSE) tem assumido protagonismo no enfrentamento à desinformação. Desde 2019, a Corte mantém o Programa Permanente de Enfrentamento à Desinformação, que reúne parcerias com plataformas digitais, instituições de ensino e agências de checagem (BRASIL, TSE, 2023). Como destaca o próprio TSE (2023), “o combate à desinformação exige esforço coordenado entre instituições públicas, sociedade civil e empresas de tecnologia, dada a capilaridade e a velocidade das redes digitais”. Em 2024, o TSE lançou o sistema *FakeCheck*, uma ferramenta baseada em inteligência artificial para auxiliar na identificação de conteúdos falsos. Paralelamente, a Controladoria-Geral da União (CGU) atua na fiscalização da transparência pública e no combate à corrupção, mas também tem ampliado sua atuação no campo da integridade da informação. Relatórios recentes da CGU apontam a necessidade de capacitar servidores públicos para identificar *deepfakes* e outras formas de manipulação digital (CGU, 2025).

2.3 Limites e alcance das respostas institucionais atuais

Apesar dos avanços, as respostas institucionais ainda enfrentam desafios significativos. Um deles é a assimetria entre a velocidade de propagação dos *deepfakes* e a capacidade de reação dos órgãos públicos. Enquanto um vídeo falso pode alcançar milhões de pessoas em poucas horas, a verificação oficial e a produção de desmentidos demandam tempo e recursos (VOSOUGHI; ROY; ARAL, 2018).

Outro limite é a abrangência das ações: muitas iniciativas concentram-se no âmbito federal, deixando municípios e estados desassistidos. Como alerta a Safernet Brasil (2025), prefeituras de pequeno e médio porte raramente dispõem de equipes treinadas ou ferramentas tecnológicas para lidar com *deepfakes*, o que as torna alvos vulneráveis.

"A velocidade de propagação da desinformação digital supera em muito a capacidade institucional de resposta. Enquanto uma mentira leva segundos para se espalhar, a verdade institucionalizada leva horas – quando chega. (VOSOUGHI, Soroush; ROY, Deb; ARAL, Sinan. The Spread of True and False News Online, 2018, p. 3).

2.4 Experiências internacionais no enfrentamento a *deepfakes*

O enfrentamento aos *deepfakes* não é um desafio exclusivamente brasileiro. Na União Europeia, o Digital Services Act (DSA), em vigor desde 2023, impõe às plataformas digitais a responsabilidade de remover conteúdos falsos em até 24 horas após notificação, sob pena de multas significativas (EUROPEAN UNION, 2023). A legislação também exige que as empresas mantenham equipes de moderação e relatórios de transparência.

Nos Estados Unidos, a abordagem tem sido mais fragmentada, com estados como a Califórnia aprovando leis específicas contra *deepfakes* eleitorais. Em 2024, o Congresso americano realizou audiências públicas para discutir a regulamentação da IA, mas ainda não há consenso sobre uma legislação federal abrangente (THE NEW YORK TIMES, 2024).

Na Alemanha, o Network Enforcement Act (NetzDG) obriga as redes sociais a removerem conteúdos manifestamente ilegais, incluindo *deepfakes* com potencial difamatório, em até 24 horas. Como sintetiza Zerback et al. (2021, p. 78), "a experiência alemã demonstra que a regulação pode ser eficaz quando combinada com cooperação institucional e participação da sociedade civil". Estudos locais indicam que a medida reduziu significativamente a circulação de desinformação em períodos eleitorais (ZERBACK et al., 2021).

3 A INFLUÊNCIA DOS *DEEPPAKES* SOBRE O ELEITOR

3.1 Mecanismos psicológicos: viés de confirmação e heurísticas

Para compreender como os *deepfakes* influenciam o eleitor, é necessário antes entender como o cérebro humano processa informações no ambiente digital. A psicologia cognitiva oferece conceitos fundamentais para essa análise.

O viés de confirmação, conceito desenvolvido por Nickerson (1998), descreve a tendência humana de buscar, interpretar e favorecer informações que confirmem crenças preexistentes, enquanto se ignoram evidências contrárias. Em contextos eleitorais, esse viés faz com que eleitores sejam mais propensos a acreditar em *deepfakes* que reforçam suas convicções políticas, mesmo diante de evidências de manipulação.

Além disso, operamos com heurísticas – atalhos mentais que simplificam decisões complexas. Kahneman (2011) demonstrou que, diante de informações ambíguas, o cérebro tende a aceitar o que parece familiar ou emocionalmente convincente, sem realizar uma análise crítica aprofundada. Os *deepfakes* exploram exatamente essa fragilidade: ao apresentarem conteúdo audiovisual que parece autêntico, ativam a heurística da "verdade percebida", em que a fluência do processamento – a facilidade com que assimilamos a informação – é confundida com veracidade.

"A tendência a buscar evidências que confirmem hipóteses já existentes, em vez de testá-las de forma crítica, é um dos vieses mais persistentes e universalmente documentados no julgamento humano. Em contextos políticos, esse viés pode tornar os eleitores particularmente vulneráveis à desinformação que reforça suas lealdades partidárias." (NICKERSON, Raymond. Confirmation Bias: A Ubiquitous Phenomenon in Many Guises, 1998, p. 175).

3.2 Evidências empíricas sobre o impacto da desinformação

As eleições municipais de 2024 no Brasil representaram um marco histórico: pela primeira vez, o país realizou um pleito sob regras específicas para o uso de inteligência artificial, incluindo a proibição expressa de *deepfakes*. Os dados disponíveis revelam a dimensão do desafio.

3.2.1 Caso Maringá/PR – O primeiro *deepfake* com repercussão judicial

Em janeiro de 2024, ainda na pré-campanha, o Tribunal Regional Eleitoral do Paraná (TRE-PR) determinou que a Meta, dona do WhatsApp, bloqueasse o compartilhamento de um áudio falso atribuído a Silvio Barros, pré-candidato do PP à prefeitura de Maringá. No arquivo digital, uma voz gerada por inteligência artificial simulava o timbre do político afirmando que havia desistido da candidatura e declarava apoio a um adversário. A decisão judicial determinou ainda a identificação do IP dos aparelhos que disseminaram o conteúdo, sob pena de multa de R\$ 100 mil por hora de descumprimento.

Este caso é emblemático por dois motivos: primeiro, demonstrou a celeridade da resposta judicial – o político declarou-se surpreso positivamente com a rapidez da atuação da Justiça Eleitoral. Segundo, evidenciou a viabilidade técnica da manipulação de voz por IA, já plenamente acessível a criminosos eleitorais. Nas palavras do próprio candidato, "já dá para saber um pouco como será a campanha neste ano. Mas a celeridade com que a Justiça Eleitoral atuou é gratificante, porque dá expectativa de que será interrompido rapidamente o compartilhamento" (SILVIO BARROS apud O GLOBO, 2024).

3.2.2 Caso Manaus/AM – *Deepfake* contra servidores públicos

Ainda em 2023, o prefeito de Manaus, David Almeida (Avante), denunciou à Polícia Federal ter sido alvo de um *deepfake*. Um áudio manipulado por inteligência artificial atribuía a ele falas ofensivas contra professores da rede municipal, chamando-os de "vagabundos" e afirmando que os servidores "querem um dinheirinho de mão beijada". O conteúdo tinha claro potencial para gerar descontentamento social e prejudicar a imagem do gestor junto a uma categoria profissional estratégica.

3.2.3 Dados consolidados das eleições de 2024

Levantamento do Aos Fatos (2024) identificou 159 decisões da Justiça Eleitoral envolvendo uso de IA na propaganda eleitoral até o primeiro turno de 2024. Os dados revelam que o Instagram foi a plataforma mais acionada, com 132 ações pedindo derrubada de vídeos, seguido por WhatsApp (52) e Facebook (18). Quanto aos tipos de manipulação, 30 ações envolviam alteração de som (narração sintética não sinalizada), 20 processos utilizavam fotos criadas artificialmente e 8 casos eram áudios sintéticos. Regionalmente, o Nordeste concentrou mais da metade dos processos (81 casos), com destaque para Ceará (19), Pernambuco (18) e Bahia (18) (AOS FATOS, 2024).

O procurador de Justiça Emmanuel Girão, coordenador do Centro de Apoio Operacional Eleitoral do MP do Ceará, oferece uma análise importante: "Aquele nível de inteligência artificial [mais sofisticado] não chegou aqui", avaliou, notando que a maior parte das ações questionavam o uso de IA em paródias ou a omissão da informação sobre o emprego da tecnologia – exigida pela resolução do TSE

3.2.4 Levantamento do Digital Forensic Research Lab (DFRLab)

Monitoramento realizado pelo DFRLab entre maio e outubro de 2024 identificou 78 casos confirmados ou alegados de *deepfakes* políticos no Brasil, abrangendo 67 cidades, com São Paulo liderando oito ocorrências. Os formatos incluíam 48 vídeos, 17 áudios e seis imagens. As táticas identificadas foram variadas, incluindo 27 casos de acusações falsas de crimes, em que candidatos foram falsamente acusados de corrupção, suborno, assédio ou pedofilia; 10 casos de imitação de figuras da mídia, utilizando rostos de jornalistas famosos; e 5 casos de *deepfakes* pornográficos, nos quais candidatas foram vítimas de nudez falsa gerada por IA. Desses 78 casos, 49 foram formalmente reportados às autoridades, gerando investigações ou ações legais.

"A utilização de inteligência artificial para viabilizar desinformação, especialmente a produção de *deepfakes*, foi uma preocupação central das autoridades eleitorais brasileiras antes das eleições municipais de outubro de 2024, nas quais 150 milhões de pessoas votaram para eleger prefeitos, vereadores e outros cargos locais em mais de 5.500 municípios." (DFRLab, Brazil's Electoral *Deepfake* Law Tested, 2024, p. 2).

3.2.5 Casos emblemáticos documentados

Entre os casos emblemáticos documentados nas eleições de 2024, destacam-se diferentes modalidades de *deepfakes*. Em São Paulo, a candidata Tabata Amaral foi vítima de *deepfake* pornográfico: duas imagens manipuladas circularam no X (antigo Twitter) retratando-a de forma sexualizada, com 114 comentários e 2.200 curtidas (AOS FATOS, 2024). Em outra frente, candidatos utilizaram *deepfakes* para "ressuscitar" figuras públicas: em Itapecuru Mirim (MA) e João Pessoa (PB), vídeos falsos imitaram o jornalista William Bonner para apoiar candidaturas. Ainda mais controverso foi o uso de falecidos em campanhas: em Andorinha (BA), a pré-candidata Lurdineia Almeida Guimarães exibiu um áudio que simulava a voz de seu falecido pai, o ex-prefeito Zé Branco, prática proibida pela resolução do TSE; em Uberlândia (MG), a Justiça determinou a derrubada de *deepfake* que mostrava o candidato a

vice Gustavo Galassi abraçando seu falecido avô, o ex-prefeito Virgílio Galassi (AOS FATOS, 2024). Por fim, em São Gonçalo do Amarante (CE), um vídeo simulou um telejornal local da TV Verdes Mares para associar o prefeito Marcelo Teles a um crime, com montagem que alterava o diálogo para sugerir motivação política.

3.3 Percepção do eleitor brasileiro sobre *deepfakes* e desinformação

Os dados de percepção pública são igualmente reveladores. Pesquisa do Instituto DataSenado, realizada entre junho e julho de 2024 com 21.808 brasileiros, aponta que 81% dos entrevistados acreditam que notícias falsas podem afetar significativamente o resultado das eleições; 72% dos usuários de redes sociais já se depararam com notícias suspeitas nos últimos seis meses; 50% consideram difícil identificar se uma notícia é falsa; 78% são a favor do controle de notícias falsas para garantir eleições mais justas; e 81% defendem a responsabilização das plataformas digitais pela disseminação de desinformação (SENADO FEDERAL, 2024). A pesquisa revela ainda disparidades regionais: eleitores de Sergipe, Maranhão e Rio Grande do Norte são os que mais declaram dificuldade para identificar conteúdos falsos, enquanto Santa Catarina, Distrito Federal e São Paulo concentram eleitores que se sentem mais capacitados (SENADO FEDERAL, 2024). Para o coordenador da pesquisa, José Henrique Varanda, "o estudo deixa clara a abrangência da exposição das pessoas a notícias falsas e como elas têm percebido os impactos dessa realidade".

3.4 *Deepfakes* e a erosão da confiança nas instituições

O fenômeno mais profundo talvez não seja o impacto imediato de um *deepfake* específico, mas sim o que a literatura denomina erosão epistêmica – o enfraquecimento gradual da capacidade social de distinguir verdade e mentira (BENKLER; FARIS; ROBERTS, 2018).

A ministra Cármen Lúcia, presidente do TSE, sintetizou esse risco com precisão: "A desinformação deforma a realidade, ilude o cidadão e fragiliza o direito constitucional à informação. Pode levar alguém a votar acreditando em uma falsidade e, depois, perceber que jamais teria feito aquela escolha se conhecesse a verdade". Quando qualquer vídeo pode ser falso, mesmo os conteúdos legítimos passam a ser vistos com desconfiança. Cria-se um ambiente no qual a verdade se torna "opcional" – e a democracia, que depende do debate informado, perde sua base de sustentação.

"O desafio não é apenas tecnológico, mas também político e social, na medida em que a confiança nas instituições e nos processos democráticos pode ser profundamente abalada quando os cidadãos não conseguem mais distinguir o real do fabricado." (CARMEN LÚCIA, Ministra do STF e presidente do TSE, 2024).

4. CENÁRIOS PARA 2026: POSSIBILIDADES EM ABERTO

4.1 O contexto regulatório em construção

Enquanto este trabalho é finalizado, o Tribunal Superior Eleitoral (TSE) encontra-se em processo avançado de definição das regras que irão disciplinar as eleições de 2026. Entre os dias 3 e 5 de fevereiro de 2026, a Corte realizou audiências públicas que receberam mais de 1,4 mil propostas de diferentes setores da sociedade. O prazo para a publicação das resoluções definitivas é 5 de março de 2026.

As discussões atuais partem da experiência das eleições municipais de 2024, quando o TSE editou a Resolução nº 23.732/2024, que pela primeira vez regulamentou o uso de inteligência artificial nas campanhas eleitorais brasileiras. À época, a principal preocupação era coibir os *deepfakes* – conteúdos manipulados capazes de distorcer falas, imagens e vídeos de candidatos. No entanto, o ambiente tecnológico de 2026 é significativamente mais complexo.

Levantamento do Aláfia Lab aponta que 9,7% dos brasileiros consideram sistemas como ChatGPT (OpenAI) e Gemini (Google) como fontes de informação. Esse dado acende um alerta sobre o potencial dessas ferramentas influenciarem decisões políticas, especialmente considerando que plataformas de busca são apontadas como a principal fonte de checagem de informações pelos brasileiros.

"A gente perguntou para as pessoas onde elas confiam mais para checar [informações]. No Brasil, havia uma predominância da confiança nas plataformas de busca, que eram as primeiras colocadas. Isso é muito curioso, porque quando as pessoas respondem 'plataformas de busca', pode significar muitas coisas: a ordem do resultado, a afinidade com o conteúdo, ou o resumo que aparece." (HELOISA MASSARO, diretora do InternetLab, em entrevista à Agência Pública, 2026).

4.2 Cenário 1 – Omissão institucional e agravamento da crise

O primeiro cenário possível para 2026 considera a hipótese de que as respostas institucionais se mostrem insuficientes ou tardias diante da velocidade de propagação dos *deepfakes*.

A principal preocupação que emerge do atual contexto jurídico é o timing da implementação das novas regras. Com o julgamento dos embargos ao acórdão do STF sobre o Marco Civil da Internet previsto apenas para a partir de fevereiro de 2026 e a possibilidade de concessão de prazo de adaptação de, pelo menos, um semestre, o Brasil corre o risco de chegar ao período eleitoral sem a plena vigência de regras mais rigorosas de moderação de conteúdo.

Essa lacuna temporal e operacional cria um ambiente fértil para a proliferação da desinformação. Caso o trânsito em julgado das novas regras ocorra apenas em março, e caso acolhida a tese de modulação apresentada por algumas plataformas, as medidas passariam a valer somente a partir de setembro de 2026, já na reta final das eleições. Nesse cenário, os impactos seriam múltiplos: disseminação descontrolada de *deepfakes* nas primeiras fases da campanha, período crucial para a formação da opinião do eleitorado; efeito assimétrico, em que a correção da informação falsa dificilmente alcançaria o mesmo público impactado pela mensagem original, mantendo-se os efeitos danosos à formação livre da opinião; e desconfiança generalizada, conforme alerta Heloisa Massaro, para quem "essa desconfiança e essa potencialidade de tudo ser falso ou gerado por IA se torna uma ferramenta de disputa política. Vários políticos vão falar que vídeos verdadeiros foram gerados por IA, complicando ainda mais o cenário".

O ministro Gilmar Mendes, do STF, sintetizou esse risco ao afirmar que "a emergência dos chamados *deepfakes* representa um salto adicional de complexidade. Quando o eleitor já não consegue distinguir com segurança o que é autêntico do que foi artificialmente fabricado, enfraquece-se uma das condições elementares do sufrágio livre: o acesso a informações confiáveis" (MENDES, 2026). Complementando essa visão, o ministro destacou em audiência no TSE que "a capacidade de criar vídeos, áudios e imagens falsos com alto grau de realismo, aptos a simular falas e comportamento de candidatos ou autoridades públicas, desafia pressupostos básicos do debate democrático. Enfraquece-se uma das condições elementares do sufrágio livre: o acesso a informações confiáveis".

4.3 Cenário 2 – Respostas pontuais e efeitos limitados

O segundo cenário considera que as instituições conseguem implementar respostas, mas estas se mostram fragmentadas ou de alcance restrito. A Resolução 23.732/24 do TSE representa um avanço institucional relevante ao proibir o uso de *deepfakes* e estabelecer a responsabilização de plataformas que não removerem conteúdos desinformativos. No entanto, como alertam especialistas, "a suficiência do arcabouço normativo depende de estrutura técnico-operacional, rapidez de reação e coordenação efetiva".

Neste cenário, alguns avanços ocorreriam, como a constituição de uma força-tarefa técnicopericial, defendida pelo ministro Gilmar Mendes, com credenciamento prévio de especialistas e centros de pesquisa universitários para análise célere de conteúdos sintéticos. Haveria também acordos institucionais com empresas desenvolvedoras de IA generativa, prevendo mecanismos de rastreabilidade e rotulagem de conteúdos artificiais, além de regras mais rígidas em análise, como a proibição de *chatbots* recomendarem candidatos e a exigência de que plataformas direcionem buscas sobre eleições a fontes oficiais da Justiça Eleitoral.

No entanto, persistiriam limitações importantes. A abrangência restrita das ações, concentradas no âmbito federal, deixaria municípios desassistidos – como já observado em 2024, prefeituras de pequeno e médio porte raramente dispõem de equipes treinadas para lidar com *deepfakes*. Estudo do IDP que analisou 56 decisões relacionadas ao uso de IA em 2024 identificou uma diversidade de perspectivas entre os juízes, com um grupo adotando postura mais permissiva e outro defendendo proibição total. Por fim, mesmo com regras mais claras, especialistas apontam limitações práticas para fiscalizar campanhas informais e redes de apoio não oficiais.

4.4 Cenário 3 – Atuação coordenada e mitigação de danos

O terceiro cenário, mais otimista, considera a possibilidade de uma resposta institucional robusta e coordenada, capaz de mitigar significativamente os impactos dos *deepfakes*. Os elementos que poderiam viabilizar esse cenário incluem regras claras e tempestivas, com a aprovação das novas resoluções até 5 de março de 2026, permitindo que partidos, candidatos e plataformas se adaptassem antes do início oficial da campanha. O TSE já sinaliza a intenção de tornar as normas mais rígidas do que as aplicadas em 2024, incluindo proibição de *chatbots* recomendarem candidatos, exigência de direcionamento de buscas a

fontes oficiais, responsabilização ampliada das empresas de IA e multas a quem divulgar material manipulado.

Outro elemento fundamental seria o fortalecimento da capacidade técnica do TSE, por meio da proposta de Gilmar Mendes de constituir uma força-tarefa técnico-pericial com especialistas e centros de pesquisa universitários, o que poderia conferir maior segurança técnica, agilidade decisória e legitimidade institucional na resposta a desafios complexos. A consolidação da jurisprudência também contribuiria positivamente, uma vez que a própria decisão do STF sobre o Marco Civil da Internet fez ressalva importante de que a nova tese não afeta a aplicação das disposições específicas da legislação eleitoral e os atos normativos expedidos pelo TSE, fortalecendo o poder normativo da Justiça Eleitoral.

Por fim, a ampliação da conscientização pública, com base nos dados do DataSenado (2024) que indicam que 81% dos brasileiros acreditam que notícias falsas podem afetar significativamente o resultado das eleições e 78% são a favor do controle de notícias falsas, poderia criar ambiente favorável a políticas de educação digital. Como sintetiza o IREE (2026), "o TSE tem até 5 de março para publicar as regras que irão disciplinar o uso de inteligência artificial nas eleições de 2026. O tema ganhou centralidade diante do avanço acelerado das tecnologias generativas e da popularização de ferramentas como o ChatGPT. Entre as sugestões em análise estão: proibir que chatbots recomendem candidatos; exigir que plataformas direcionem buscas sobre eleições a fontes oficiais da Justiça Eleitoral."

4.5 Síntese dos cenários

A tabela a seguir sintetiza os três cenários apresentados, considerando suas principais características, consequências e probabilidade estimada com base no atual estágio das discussões institucionais:

Figura 1 - Síntese dos cenários para as eleições de 2026

CENÁRIO	CARACTERÍSTICAS	CONSEQUÊNCIAS	PROBABILIDADE
1 – OMISSÃO INSTITUCIONAL	Atraso na implementação de regras; lacunas regulatórias; falta de coordenação	Disseminação descontrolada de <i>deepfakes</i> ; erosão acelerada da confiança; efeitos assimétricos da desinformação	Média (depende do julgamento dos embargos ao Marco Civil)

2 – RESPOSTAS PONTUAIS	Regras aprovadas, mas com alcance limitado; interpretações divergentes; capacidade restrita de fiscalização	Avanços parciais; municípios desassistidos; persistência de <i>deepfakes</i> em contextos locais	Alta (cenário mais provável)
3 – ATUAÇÃO COORDENADA	Regras tempestivas e rigorosas; força-tarefa técnica; cooperação com plataformas; jurisprudência consolidada	Mitigação significativa dos impactos; respostas céleres; maior segurança jurídica	Moderada (depende da celeridade do STF e do TSE)

Fonte: Elaboração própria, com base em Oliveira e Santos (2026) e IREE (2026).

4.6 O que está em jogo

Independentemente do cenário que se concretize, uma questão permanece central: a confiança no processo democrático.

Como alerta Denilson dos Santos de Oliveira e Fábio da Silva Santos, "a dificuldade contemporânea não reside apenas na detecção dessas manipulações, mas principalmente em combatê-las com eficácia. Conteúdos audiovisuais falsificados, por sua aparência realista, têm alto potencial de influenciar o comportamento do eleitorado, propagando desinformação com velocidade alarmante".

No Brasil, onde o período oficial de campanha eleitoral é relativamente curto (cerca de 45 dias), o tempo disponível para desmentir ou neutralizar os efeitos de um *deepfake* pode ser insuficiente, comprometendo o equilíbrio do pleito.

A ministra Cármen Lúcia já havia alertado: "A desinformação deforma a realidade, ilude o cidadão e fragiliza o direito constitucional à informação" [citado no Capítulo 3]. Esse alerta ganha contornos ainda mais urgentes em 2026, quando a tecnologia alcançou patamares de realismo que tornam a distinção entre real e fabricado um desafio até para especialistas.

O desfecho desse processo – se o Brasil conseguirá ou não proteger a integridade de suas eleições diante da nova fronteira da desinformação artificial – dependerá, em grande medida, das escolhas institucionais que estão sendo feitas neste exato momento.

5 CONSIDERAÇÕES FINAIS

A trajetória percorrida ao longo deste trabalho permitiu uma análise aprofundada sobre a influência dos *deepfakes* no processo eleitoral brasileiro, com especial atenção às eleições de 2026. Partindo do problema de pesquisa – "diante do avanço dos *deepfakes* e da experiência recente com desinformação eleitoral, quais cenários podem se desenhar para as eleições de 2026 no Brasil a partir da influência desses conteúdos sobre a confiança do eleitor?" –, buscou-se compreender não apenas os mecanismos técnicos e psicológicos envolvidos, mas também as respostas institucionais em construção e seus possíveis desdobramentos.

O primeiro capítulo estabeleceu as bases conceituais necessárias para a compreensão do fenômeno. Os *deepfakes*, conforme discutido a partir de Chesney e Citron (2019) e Goodfellow et al. (2014), representam um salto qualitativo na história da desinformação: diferentemente de boatos textuais ou edições grosseiras, eles exploram a confiança que o ser humano deposita no que vê e ouve, ativando vieses cognitivos profundos e dificultando a distinção entre real e fabricado. A literatura sobre pós-verdade (KEYES, 2004) e erosão epistêmica (BENKLER; FARIS; ROBERTS, 2018) ofereceu ferramentas para compreender as implicações desse fenômeno para a democracia.

O segundo capítulo examinou o papel da gestão pública no enfrentamento da desinformação digital. A análise das ações do TSE e da CGU revelou avanços importantes, como o Programa Permanente de Enfrentamento à Desinformação e o sistema FakeCheck, mas também evidenciou limites significativos: a assimetria entre a velocidade de propagação dos *deepfakes* e a capacidade de reação institucional (VOSOUGHI; ROY; ARAL, 2018), a concentração de iniciativas no âmbito federal e a vulnerabilidade de municípios de pequeno e médio porte (SAFERNET BRASIL, 2025). As experiências internacionais – o Digital Services Act europeu, as leis estaduais nos EUA e o Network Enforcement Act alemão – ofereceram parâmetros comparativos valiosos.

O terceiro capítulo mergulhou nas evidências empíricas sobre a influência dos *deepfakes* no eleitor brasileiro. Os casos reais documentados nas eleições municipais de 2024 – o áudio falso contra Sílvia Barros em Maringá, o *deepfake* contra David Almeida em Manaus, as imagens manipuladas de Tabata Amaral, os jornalistas "ressuscitados" por IA, os falecidos "apoiando" candidaturas, o telejornal falso no Ceará – não são episódios isolados, mas sinais de um padrão que tende a se intensificar. Os dados do Aos Fatos (159 decisões judiciais), do DFRLab (78 casos em 67 cidades) e do DataSenado (81% dos brasileiros preocupados com o impacto das fake news) confirmam a dimensão e a relevância do problema.

O quarto capítulo, núcleo prospectivo do trabalho, construiu três cenários possíveis para 2026, com base no atual estágio das discussões institucionais. O Cenário 1 – Omissão institucional considera a possibilidade de atrasos na implementação das regras, lacunas regulatórias e falta de coordenação, resultando em disseminação descontrolada de *deepfakes* e erosão acelerada da confiança. O Cenário 2 – Respostas pontuais, considerado o mais provável, projeta avanços parciais, com regras aprovadas mas de alcance limitado, interpretações divergentes e capacidade restrita de fiscalização, deixando municípios desassistidos. O Cenário 3 – Atuação coordenada, o mais otimista, depende da aprovação tempestiva de regras rigorosas, da constituição de força-tarefa técnico-pericial, da cooperação efetiva com plataformas e da consolidação da jurisprudência.

O que os três cenários têm em comum é a constatação de que a confiança no processo democrático está no centro do debate. Como alertou a ministra Cármen Lúcia, "a desinformação deforma a realidade, ilude o cidadão e fragiliza o direito constitucional à informação". Quando qualquer vídeo pode ser falso, mesmo os conteúdos legítimos passam a ser vistos com desconfiança. Cria-se um ambiente no qual a verdade se torna "opcional" – e a democracia, que depende do debate informado, perde sua base de sustentação.

As lições das eleições de 2024 são claras: a tecnologia avança em ritmo muito superior à capacidade de resposta institucional. O Brasil tem hoje a oportunidade de aprender com essa experiência e construir respostas mais robustas para 2026. As audiências públicas realizadas pelo TSE em fevereiro de 2026, com mais de 1,4 mil propostas recebidas, indicam que há consciência da gravidade do problema e disposição para enfrentá-lo. Resta saber se o timing institucional – a publicação das regras até 5 de março, o julgamento dos embargos ao Marco Civil da Internet, a eventual modulação dos efeitos – permitirá que essas respostas cheguem a tempo.

Mais do que prever o futuro, este trabalho buscou ampliar a compreensão sobre as possibilidades que o presente já contém (GODET, 2010). Seu principal contributo não é oferecer respostas prontas, mas fornecer elementos para que gestores públicos, pesquisadores e cidadãos possam refletir sobre os caminhos possíveis e as escolhas que estão sendo feitas – ou deixadas de fazer – neste momento decisivo.

Ao final desta trajetória, uma questão permanece em aberto, como convém a um trabalho que se propôs analítico e não prescritivo: estará o Brasil preparado para proteger a integridade de suas eleições diante da nova fronteira da desinformação artificial? A resposta, em grande medida, será escrita nos próximos meses – nas decisões do STF, nas resoluções do

TSE, na atuação das plataformas, na reação da sociedade civil e, sobretudo, na capacidade coletiva de distinguir, ainda que com dificuldade crescente, o real do fabricado.

O que este trabalho espera ter demonstrado é que o futuro não está dado – ele se constrói a cada escolha institucional, a cada decisão judicial, a cada campanha de conscientização, a cada cidadão que se recusa a aceitar passivamente a erosão da verdade. E é nesse campo de possibilidades, incerto, mas não indeterminado, que a democracia brasileira enfrentará seu próximo teste.

Cabe registrar que este trabalho, alinhado aos seus objetivos, adotou um recorte temporal circunscrito às eleições municipais de 2024 e uma abordagem metodológica baseada em análise documental. Tais escolhas mostraram-se adequadas para a construção dos cenários prospectivos propostos, permitindo um exame aprofundado dos casos concretos e das respostas institucionais observadas. Naturalmente, outros caminhos metodológicos poderiam complementar a compreensão do fenômeno, o que não diminui a contribuição aqui oferecida, mas aponta possibilidades de avanço.

Como desdobramento natural desta pesquisa, estudos futuros poderão ampliar o debate por meio de investigações empíricas junto a eleitores, capturando em profundidade os mecanismos pelos quais os *deepfakes* influenciam a percepção e a decisão de voto. A realização de *surveys* ou grupos focais poderia enriquecer a análise com dados primários sobre a recepção social desse conteúdo. Além disso, após as eleições de 2026, será possível confrontar os cenários aqui delineados com os acontecimentos concretos, avaliando a pertinência das projeções e refinando modelos de análise prospectiva. Por fim, pesquisas comparativas entre o Brasil e outros países da América Latina podem revelar similaridades e especificidades no enfrentamento à desinformação artificial, ampliando as fronteiras do debate.

REFERÊNCIAS

AOS FATOS. **Na eleição, IA criou confissões falsas e até 'ressuscitou' padrinhos políticos.** São Paulo, out. 2024.

BENKLER, Yochai; FARIS, Robert; ROBERTS, Hal. *Network Propaganda: **Manipulation, Disinformation, and Radicalization in American Politics.*** Oxford: Oxford University Press, 2018.

BRASIL. Tribunal Superior Eleitoral. **Programa Permanente de Enfrentamento à Desinformação: Relatório de Atividades 2023.** Brasília: TSE, 2023.

CGU – Controladoria-Geral da União. **Relatório de Integridade da Informação no Setor Público.** Brasília: CGU, 2025.

CHESNEY, Robert; CITRON, Danielle. *Deepfakes and the New Disinformation War: **The Coming Age of Post-Truth Geopolitics.*** *Foreign Affairs*, v. 98, n. 1, p. 147-155, 2019.

DFRLab – Digital Forensic Research Lab. ***Brazil's Electoral Depfake Law Tested as AI-Generated Content Targeted Local Elections.*** Washington: Atlantic Council, 2024.

EUROPEAN UNION. ***Digital Services Act (Regulation 2022/2065).*** Brussels: Official Journal of the European Union, 2023.

GODET, Michel. **Manual de Prospectiva Estratégica.** Lisboa: Instituto Piaget, 2010.

GOODFELLOW, Ian et al. ***Generative Adversarial Networks.*** *Communications of the ACM*, v. 63, n. 11, p. 139-144, 2020.

HAN, Byung-Chul. **Infocracia: Digitalização e a Crise da Democracia.** Petrópolis: Vozes, 2022.

HOOD, Christopher. ***A Public Management for All Seasons? Public Administration,*** v. 69, n. 1, p. 3-19, 1991.

IREE – Instituto para Reforma das Relações Estado-Empresa. **TSE analisa novas regras para uso de IA nas eleições.** São Paulo, 19 fev. 2026. Disponível em: <https://iree.org.br/tse-analisa-novas-regras-para-uso-de-ia-nas-eleicoes/>. Acesso em: 21 fev. 2026.

KEYES, Ralph. **A Era da Pós-Verdade: Desonestidade e Enganação na Vida Contemporânea.** Rio de Janeiro: Civilização Brasileira, 2004.

LEVITSKY, Steven; ZIBLATT, Daniel. **Como as Democracias Morrem.** Rio de Janeiro: Zahar, 2018.

MASSARO, Heloisa. **IA adiciona novas camadas de risco à desinformação nas eleições 2026.** [Entrevista concedida a] Agência Pública. São Paulo, 5 jan. 2026. Disponível em: <https://apublica.org/2026/01/inteligencia-artificial-e-desinformacao-nas-eleicoes-de-2026/>. Acesso em: 21 fev. 2026.

MELLO, Christian. **Administração Pública 4.0: Tecnologia, Inovação e Governança Digital.** Curitiba: Intersaberes, 2021.

MENDES, Gilmar. **TSE debate 'risco sistêmico' para as eleições com avanço de deepfakes.** O Globo, Rio de Janeiro, 9 fev. 2026. Disponível em: <https://oglobo.globo.com/politica/noticia/2026/02/09/tse-debate-risco-sistemico-para-aseleicoes-com-avanco-de-deepfakes.ghtml>. Acesso em: 21 fev. 2026.

NICKERSON, Raymond. *Confirmation Bias: A Ubiquitous Phenomenon in Many Guises.* *Review of General Psychology*, v. 2, n. 2, p. 175-220, 1998.

O GLOBO. **Casos de 'deep fake' chegam à Justiça Eleitoral, que cobra WhatsApp.** Rio de Janeiro, 24 jan. 2024.

OLIVEIRA, Denilson dos Santos de; SANTOS, Fábio da Silva. **Deepfakes e o impacto da manipulação no período eleitoral.** Migalhas, 4 fev. 2026. Disponível em:

<https://www.migalhas.com.br/depeso/449078/deepfakes-e-o-impacto-da-manipulacao-no-periodo-eleitoral>. Acesso em: 22 fev. 2026.

SAFERNET BRASIL. **Relatório de Desinformação e Deepfakes no Brasil 2025**. São Paulo: Safernet, 2025.

SANTAELLA, Lucia. **A Pós-Verdade é Verdadeira ou Falsa?** Barueri: Estação das Letras e Cores, 2021.

SENADO FEDERAL. Instituto DataSenado. Panorama Político: 21ª edição – ***Fake News e Democracia***. Brasília: DataSenado, 2024.

THE NEW YORK TIMES. ***Congress Grapples With AI Regulation Ahead of Elections***. *New York*, 15 mar. 2024.

THE WASHINGTON POST. ***How a Deepfake of a Candidate Shook a Local Election***. *Washington*, 15 out. 2023.

VACCARI, Cristian. ***What Do We Know About Fake News? An Analysis of the Literature***. *Political Communication*, v. 37, n. 4, p. 543-562, 2020.

VOSOUGHI, Soroush; ROY, Deb; ARAL, Sinan. ***The Spread of True and False News Online***. *Science*, v. 359, n. 6380, p. 1146-1151, 2018.

ZERBACK, Thomas et al. ***Regulating Disinformation: The German Approach and Its Effects***. *Journal of Information Policy*, v. 11, p. 67-92, 2021.

APÊNDICE

Apêndice A - Linha do tempo dos *deepfakes* eleitorais no Brasil (2024-2026)

DATA	CASO	LOCAL	TIPO	CONSEQUÊNCIA
Out/2024	Áudio falso contra Sílvio Barros	Maringá/PR	Áudio	Decisão judicial inédita
2024	<i>Depfake</i> contra David Almeida	Manaus/AM	Áudio	Denúncia à PF
Out/2024	Imagens falsas de Tabata Amaral	São Paulo/SP	Imagem	Remoção pela plataforma
2024	Jornalista "ressuscitado" (Bonner)	MA e PB	Vídeo	Investigação
2024	Falecido "apoia" candidatura	Andorinha/BA	Áudio	Investigação
2024	Telejornal falso	São Gonçalo do Amarante/CE	Vídeo	Ação judicial
Fev/2026	Audiências públicas TSE	Brasília/DF	Regulamentação	1,4 mil propostas

Fonte: Elaboração própria, com base nas fontes indicadas

Apêndice B - Síntese das decisões judiciais sobre IA nas eleições 2024

TIPO DE DECISÃO	QUANTIDADE	FONTE
Ações pedindo derrubada de vídeos no Instagram	132	Aos Fatos (2024)
Ações no WhatsApp	52	Aos Fatos (2024)
Ações no Facebook	18	Aos Fatos (2024)
Casos com alteração de som (narração sintética)	30	Aos Fatos (2024)
Fotos criadas artificialmente	20	Aos Fatos (2024)
Áudios sintéticos	8	Aos Fatos (2024)

Fonte: Elaboração própria, com base nas fontes indicadas

Emitido em 17/06/2026

DOCUMENTO COMPROBATÓRIO (ANEXO) Nº 01/2026 - CCSA - CGP (11.00.52.01)
(Nº do Documento: 85)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 17/06/2026 14:49)
YLUSKA MAGALHAES GUEDES BRITO ALMEIDA
ASSISTENTE EM ADMINISTRACAO
1679264

Para verificar a autenticidade deste documento entre em <https://sipac.ufpb.br/documentos/> informando seu número:
85, ano: 2026, documento (espécie): **DOCUMENTO COMPROBATÓRIO (ANEXO)**, data de emissão:
17/06/2026 e o código de verificação: **4d0b2543b5**