

Deepfakes e integridade eleitoral no compliance digital dos partidos

Alex Cavalcante dos Santos e Rafael Gomes

1. Introdução

A integridade eleitoral pressupõe que a formação da vontade política ocorra em ambiente no qual fatos, argumentos e propostas possam ser examinados sob condições mínimas de autenticidade. Essa premissa não exige consenso substantivo nem elimina a retórica própria da competição política, mas impede que a fraude informacional seja naturalizada como técnica legítima de campanha. A expansão da inteligência artificial generativa alterou a escala desse problema. Áudios, imagens e vídeos sintéticos podem reproduzir voz, aparência e gestos de pessoas reais, simular acontecimentos inexistentes e circular em velocidade incompatível com os tempos ordinários de verificação, resposta e tutela jurisdicional. O risco não decorre apenas da possibilidade de o eleitor acreditar em uma falsificação. A disseminação de conteúdos sintéticos também amplia a incerteza, estimula o cinismo e permite que registros autênticos sejam rejeitados como artificiais, fenômeno descrito como dividendo do mentiroso (Chesney & Citron, 2019; Vaccari & Chadwick, 2020).

A literatura jurídica e política concentrou parcela significativa de suas respostas em dois polos institucionais. O primeiro é o Estado, responsável por definir proibições, procedimentos e sanções. O segundo é formado pelas plataformas digitais, que organizam a circulação de conteúdos e detêm capacidade técnica para rotular, moderar, remover ou reduzir o alcance de publicações. Esses polos são indispensáveis, mas não esgotam a arquitetura do processo eleitoral. Os partidos selecionam candidaturas, administram recursos públicos, contratam fornecedores, organizam equipes de comunicação, definem estratégias e exercem poder disciplinar sobre agentes vinculados à sua estrutura. Sua posição constitucional impede que sejam tratados como espectadores neutros da desinformação produzida ou difundida por campanhas, dirigentes, filiados e prestadores de serviços. A responsabilidade partidária não se confunde com responsabilidade automática por toda manifestação individual de seus integrantes. Ela se refere ao dever de estruturar controles proporcionais aos riscos criados por uma atividade organizada, financiada e orientada à conquista do poder político.

O problema de pesquisa consiste em verificar em que medida os principais partidos políticos brasileiros incorporaram, em seus documentos normativos internos, mecanismos de compliance e integridade digital capazes de prevenir, detectar, apurar e sancionar o uso eleitoral de deepfakes e outras formas de desinformação. A investigação examina ainda como a ausência ou a presença

desses mecanismos se relaciona com o regime normativo estabelecido pelo Tribunal Superior Eleitoral para as eleições de 2026. A hipótese sustenta que os estatutos partidários selecionados, considerados no marco temporal definido pela pesquisa, não apresentam instrumentos específicos e sistemáticos de governança informacional, o que transfere à Justiça Eleitoral e às plataformas parcela excessiva do custo de contenção de danos que poderiam ser prevenidos no interior das próprias agremiações.

O objetivo geral é diagnosticar o grau de institucionalização da integridade informacional no corpus partidário e propor uma arquitetura mínima de prevenção. Os objetivos específicos compreendem delimitar os riscos democráticos dos deepfakes, identificar categorias documentais de governança digital, comparar os estatutos selecionados, examinar a complementaridade entre controles internos e regulação eleitoral e formular o Programa de Integridade Informacional Partidária, denominado PIIP. A contribuição do estudo reside no deslocamento analítico da responsabilidade exclusiva do Estado e das plataformas para a governança das organizações que estruturam a competição eleitoral. Não se pretende defender censura privada, vigilância ideológica ou controle prévio de opiniões. A proposta alcança a produção comunicacional vinculada ao partido e às campanhas, os recursos por eles administrados e os agentes que atuam sob sua direção, sempre com devido processo, proporcionalidade e proteção da liberdade de expressão.

A investigação foi deliberadamente concentrada no diagnóstico documental e na formulação do PIIP. O regime do TSE para 2026 é examinado como parâmetro normativo de contraste, sem reproduzir uma descrição exaustiva de todos os ilícitos, procedimentos e sanções eleitorais. Essa delimitação preserva o núcleo original da pesquisa e permite avaliar se a incorporação de deveres de transparência e conformidade às plataformas deve ser acompanhada por uma camada interna de integridade partidária. O texto está organizado em seis partes subsequentes. O referencial teórico relaciona esfera pública, deepfakes, compliance e prudência institucional. A metodologia explícita corpus, categorias e limitações. A análise documental apresenta a matriz comparativa dos dez partidos. Em seguida são discutidos os efeitos institucionais da omissão, a arquitetura do PIIP e sua articulação com as resoluções eleitorais de 2026. A conclusão responde ao problema, registra os limites do estudo e indica agenda de atualização empírica.

2. Deepfakes, esfera pública e integridade partidária

2.1. Fragmentação informacional e crise da evidência audiovisual

A democracia representativa depende de uma esfera pública na qual cidadãos e instituições possam submeter pretensões políticas a crítica, justificação e

contestação. A formulação habermasiana não pressupõe comunicação livre de poder, mas oferece um critério normativo para reconhecer quando a deliberação é substituída por manipulação que impede a formação autônoma do juízo (Habermas, 1989). No ecossistema digital, a visibilidade do discurso público deixou de ser organizada apenas por instituições jornalísticas, partidos, associações e órgãos estatais. Plataformas privadas passaram a selecionar conteúdos segundo sistemas de recomendação, segmentação e ranqueamento cuja lógica é pouco transparente. A economia da atenção favorece mensagens capazes de produzir reação rápida, retenção e compartilhamento, ainda que sua relevância pública ou veracidade sejam frágeis. A assimetria entre quem conhece os mecanismos de circulação e quem apenas recebe seus efeitos transforma a informação em instrumento de predição e modulação comportamental (Zuboff, 2019; Pasquale, 2015).

Bennett e Livingston (2018) descrevem uma ordem da desinformação formada pela interação entre polarização, enfraquecimento das instituições mediadoras, fragmentação midiática e estratégias organizadas de comunicação manipulativa. O dano democrático não se reduz à soma de afirmações falsas. A repetição de narrativas incompatíveis, a fabricação de controvérsias e a desqualificação prévia de fontes confiáveis podem produzir ambiente de suspeição permanente. Nesse cenário, decisões judiciais, jornalismo profissional, ciência e registros públicos passam a ser recebidos como meras versões concorrentes. A disputa deixa de ocorrer sobre a interpretação de fatos compartilhados e passa a envolver a própria possibilidade de reconhecê-los. O resultado é a erosão da base epistêmica da responsabilização política, pois o eleitor encontra dificuldade crescente para distinguir crítica legítima, erro, sátira, edição, propaganda e falsificação intencional.

Os deepfakes intensificam esse processo porque exploram a confiança social historicamente atribuída ao registro audiovisual. A expressão designa conteúdos sintéticos ou profundamente manipulados por técnicas de inteligência artificial capazes de representar pessoas dizendo ou fazendo aquilo que não disseram ou fizeram. Embora nem todo conteúdo sintético seja ilícito, sua utilização enganosa em campanhas pode difamar candidaturas, alterar propostas, simular apoios, fabricar confissões, desmobilizar eleitores ou atacar a própria credibilidade da Justiça Eleitoral. Batista e Santaella (2024) demonstram que a novidade do fenômeno está vinculada à combinação entre mecanismos perceptivos humanos e capturas algorítmicas, o que amplia a força persuasiva de representações artificiais. Mulholland e Oliveira (2021) situam os deepfakes no campo dos riscos à personalidade, à democracia e à qualidade da informação política, ressaltando que o audiovisual sintético pode produzir danos cuja correção tardia não recompõem integralmente o ambiente decisório.

A ameaça possui dupla direção. Conteúdos falsos podem ser aceitos como verdadeiros, mas registros autênticos também podem ser negados mediante alegação oportunista de manipulação. Chesney e Citron (2019) denominam essa segunda possibilidade dividendo do mentiroso. A simples disponibilidade social de tecnologias de falsificação reduz a força probatória intuitiva do áudio e do vídeo e oferece a agentes públicos uma estratégia de negação plausível. A pesquisa experimental de Vaccari e Chadwick (2020) acrescenta que deepfakes políticos não precisam enganar a maioria do público para causar dano. A exposição pode aumentar a incerteza e, por essa via, reduzir a confiança em notícias circuladas nas redes sociais. Pawelec (2022) conclui que o impacto depende do contexto e da intenção, mas identifica riscos às funções democráticas de inclusão, formação da agenda e decisão coletiva quando conteúdos sintéticos são empregados para desinformação ou discurso de ódio.

A resposta institucional precisa considerar o momento eleitoral. Um conteúdo divulgado próximo à votação pode atingir milhões de pessoas antes que a falsidade seja identificada, antes que o contraditório seja estabelecido e antes que uma ordem de remoção seja cumprida. Mesmo quando a tutela jurisdicional é célere, a reparação alcança um público distinto daquele exposto à mensagem original. A estratégia de desinformação aproveita, portanto, a assimetria entre velocidade tecnológica e tempo institucional. A prevenção não substitui o controle judicial, mas reduz a probabilidade de que estruturas partidárias financiem, aprovelem ou amplifiquem conteúdos cuja circulação produza dano irreversível. Essa constatação justifica examinar os partidos como organizações capazes de internalizar deveres de cautela, documentação e resposta.

2.2. Compliance, governança partidária e prudência institucional

Compliance designa um sistema organizado de prevenção, detecção, resposta e aperfeiçoamento destinado a alinhar condutas a normas jurídicas, políticas internas e padrões éticos. Sua efetividade não decorre da mera existência de um código. Sistemas de integridade dependem do compromisso da liderança, da avaliação de riscos, da definição de responsabilidades, de treinamento, controles, canais de denúncia, investigação, sanção e revisão periódica (Carvalho et al., 2020; OECD, 2020; ISO, 2021). A transposição desse referencial para partidos políticos exige adaptação. As agremiações são pessoas jurídicas de direito privado com autonomia constitucional, mas exercem funções indispensáveis à democracia representativa, selecionam candidaturas, recebem recursos públicos e influenciam diretamente a organização da disputa. O modelo pertinente não é uma cópia da governança empresarial, e sim um sistema de integridade orientado à função democrática dos partidos.

A Constituição de 1988 assegura autonomia partidária para definir estrutura interna, organização e funcionamento, ao mesmo tempo que submete as agremiações aos princípios do regime democrático, ao caráter nacional, à prestação de contas e às regras de acesso a recursos públicos. A autonomia protege o pluralismo e impede interferência estatal indevida, mas não converte o espaço partidário em zona imune a deveres de transparência e responsabilidade. Quanto maior a capacidade de uma organização estruturar campanhas, administrar verbas e orientar fluxos comunicacionais, maior é a necessidade de mecanismos que impeçam a utilização dessa estrutura para fraude informacional. Cavalcante (2025) sustenta que a relevância pública e o financiamento partidário justificam padrões de integridade compatíveis com a responsabilidade fiduciária das agremiações. O argumento deve ser manejado com transparência, porque a obra é de autoria de um dos pesquisadores e constitui fonte da seleção original do corpus. Neste artigo, seu uso é explicitado e submetido a reclassificação documental específica voltada à integridade digital.

A integridade informacional partidária pode ser definida como o conjunto de políticas, procedimentos e controles que orientam a produção, contratação, aprovação, impulsionamento, distribuição e correção de conteúdos eleitorais vinculados ao partido. Seu objeto não é a verdade oficial de opiniões, promessas ou interpretações políticas. O núcleo de proteção recai sobre autenticidade, rastreabilidade, transparência no uso de inteligência artificial, vedação de falsificações enganosas, resposta a incidentes e responsabilização de agentes que empreguem recursos partidários para manipulação ilícita. Essa distinção é essencial. Um programa que avaliasse previamente toda crítica política seria incompatível com a liberdade de expressão e com a dinâmica interna do pluralismo. Um programa que documenta fornecedores, exige rotulagem, impede deepfakes fraudulentos e investiga denúncias atua sobre riscos operacionais concretos, não sobre preferências ideológicas.

A prudência oferece fundamento ético complementar para esse desenho. Na Ética a Nicômaco, Aristóteles apresenta a *phronesis* como capacidade de deliberar corretamente sobre os meios adequados à realização do bem em situações contingentes. Tomás de Aquino desenvolve a prudência como reta razão aplicada à ação, articulando memória, compreensão da realidade, previsão e escolha responsável (Aristóteles, 1991; Aquino, 2004, II-II, q. 47). No ambiente digital, a prudência institucional exige verificar informações, resistir ao compartilhamento impulsivo, antecipar impactos e recusar o uso tecnicamente possível quando ele viola a integridade da disputa. O compliance converte essa exigência moral em rotinas verificáveis. Treinamentos, registros, segregação de funções, revisão de peças e canais de denúncia reduzem a dependência exclusiva da virtude individual e criam condições organizacionais para decisões responsáveis.

A governança partidária deve ser compreendida, ainda, como uma das modalidades de regulação social. Lessig (1999) demonstrou que comportamentos no ciberespaço são moldados por lei, mercado, normas sociais e arquitetura. Aplicada ao processo eleitoral, essa formulação indica que resoluções e sanções estatais não atuam isoladamente. A arquitetura das plataformas define possibilidades técnicas, os incentivos de mercado orientam alcance e engajamento, as normas internas dos partidos condicionam escolhas de campanha e a lei estabelece limites externos. Quando a dimensão partidária permanece ausente, o sistema perde a instância que está mais próxima de candidatos, fornecedores e equipes de comunicação. O PIIP é concebido como mecanismo de integração entre essas formas de regulação, preservando a competência da Justiça Eleitoral e adicionando uma camada preventiva de responsabilidade organizacional.

3. Metodologia

3.1. Desenho da pesquisa e delimitação do corpus

A pesquisa possui finalidade aplicada, objetivos exploratório-descritivos e abordagem predominantemente qualitativa, com apoio quantitativo meramente descritivo. Os procedimentos empregados foram revisão bibliográfica, análise documental e cotejo normativo. O componente quantitativo limitou-se à codificação binária da presença ou ausência de categorias nos documentos e à apresentação de frequências absolutas e relativas. Não houve aplicação de técnicas inferenciais nem constituição de base autônoma que justificasse classificar o estudo como método misto em sentido estrito. A análise qualitativa permaneceu central, porque a pesquisa examinou o conteúdo, o alcance e a adequação funcional das normas internas, inclusive quando dispositivos gerais de ética ou disciplina poderiam ser interpretados como indiretamente aplicáveis ao ambiente digital.

O corpus foi definido por amostragem intencional. Foram selecionadas dez agremiações de elevada representação parlamentar e participação no financiamento eleitoral de 2022, conforme a sistematização realizada por Cavalcante (2025). A amostra compreendeu União Brasil, Partido dos Trabalhadores, Movimento Democrático Brasileiro, Partido Social Democrático, Progressistas, Partido da Social Democracia Brasileira, Partido Liberal, Partido Socialista Brasileiro, Partido Democrático Trabalhista e Republicanos. A opção por partidos de maior expressão decorreu de sua capilaridade nacional, do volume de candidaturas e recursos administrados e de sua capacidade potencial de produzir, prevenir ou amplificar riscos informacionais. A lista foi mantida de modo uniforme na seleção, na matriz comparativa e na interpretação dos resultados.

A unidade primária de análise foi o estatuto partidário aprovado pelo TSE e disponível no repositório institucional até 31 de dezembro de 2023. Quando o próprio estatuto remetia a código de ética, regulamento disciplinar ou norma complementar publicamente acessível dentro do mesmo marco temporal, o documento foi considerado como fonte auxiliar. A data de corte foi preservada porque corresponde ao levantamento original que antecedeu a edição das regras eleitorais de 2026. A pesquisa não afirma, portanto, que todos os documentos vigentes em julho de 2026 permanecem idênticos. O contraste temporal é deliberado e permite avaliar o grau de preparação institucional anteriormente existente diante das exigências regulatórias posteriores. Atualizações estatutárias aprovadas após o corte constituem objeto de pesquisa subsequente.

Tabela 1 - Corpus documental padronizado

Partido	Documento considerado	Marco de aprovação ou disponibilidade
UNIÃO	Estatuto partidário de 2022	Aprovado pelo TSE em 8.2.2022
PT	Estatuto de 20.7.2022	Aprovado pelo TSE em 1.6.2023
MDB	Estatuto partidário de 2022	Aprovado pelo TSE em 17.2.2022
PSD	Estatuto partidário de 2022	Disponível e aprovado no marco de 2023
PP	Estatuto partidário de 2021	Versão disponível no repositório até 31.12.2023
PSDB	Estatuto de 9.12.2017	Aprovado em 21.8.2018 e substituído em 10.2.2020
PL	Estatuto partidário de 2019	Versão disponível no repositório até 31.12.2023

Partido	Documento considerado	Marco de aprovação ou disponibilidade
PSB	Estatuto partidário de 2011	Versão disponível no repositório até 31.12.2023
PDT	Estatuto partidário de 2022	Versão disponível no repositório até 31.12.2023
REPUBLICANOS	Estatuto partidário de 2021	Aprovado pelo TSE em 28.4.2022

Fonte. Elaboração dos autores com base no repositório de partidos políticos registrados no TSE e na delimitação de Cavalcante (2025).

3.2. Procedimentos de coleta, codificação e validação

A coleta documental utilizou os arquivos oficiais do TSE e, subsidiariamente, os sítios das agremiações. A leitura foi conduzida em duas etapas. Na primeira, realizaram-se buscas textuais pelos descritores desinformação, notícia falsa, fake news, internet, rede social, mídia digital, ética digital, integridade, compliance, inteligência artificial, conteúdo sintético, deepfake, robô e bot. Na segunda, procedeu-se à leitura contextual das disposições sobre deveres dos filiados, propaganda, comunicação, disciplina, competências de conselhos de ética, canais de denúncia, apuração, sanções, transparência e prestação de contas. A busca lexical não foi tratada como suficiente, pois uma norma pode disciplinar funcionalmente o risco sem empregar a terminologia mais recente. A classificação positiva exigiu dispositivo identificável, com objeto digital específico ou mecanismo institucional diretamente aplicável à prevenção, detecção, investigação ou resposta à desinformação eleitoral.

A matriz final foi reduzida a quatro categorias diretamente relacionadas ao problema de pesquisa. A primeira verificou menção expressa a desinformação, notícia falsa ou fake news. A segunda examinou inteligência artificial, conteúdo sintético ou deepfake. A terceira procurou regras específicas de conduta digital aplicáveis a candidatos, dirigentes, filiados, equipes ou fornecedores. A quarta identificou mecanismos estruturados de governança informacional, como responsável institucional, avaliação de risco, rastreabilidade, canal especializado, procedimento de apuração, indicadores ou relatório público. Disposições genéricas sobre ética, fidelidade, honra partidária ou infração

disciplinar não foram classificadas como governança digital específica, embora tenham sido consideradas na interpretação qualitativa.

A revisão bibliográfica foi realizada por busca orientada em repositórios acadêmicos e no Google Acadêmico, utilizado apenas como ferramenta de descoberta. Foram priorizados artigos com revisão por pares, livros de referência, normas técnicas, documentos da OECD e fontes primárias oficiais. A inteligência artificial generativa foi empregada de modo auxiliar na localização preliminar de referências, organização de tópicos e revisão linguística. Nenhuma obra foi incluída apenas porque indicada por ferramenta automatizada. Autoria, título, periódico, volume, páginas, DOI e correspondência entre o argumento e a fonte foram conferidos pelos autores. A validação bibliográfica incluiu o cotejo das citações com as obras originais e a uniformização dos dados de autoria, edição, ano, paginação e identificação editorial.

A análise possui limitações. Estatutos e códigos revelam a institucionalização formal, mas não demonstram, por si, as práticas reais de campanhas e diretórios. A ausência de regra específica não prova que o partido jamais tenha adotado treinamento, protocolo ou resposta pontual. Em sentido inverso, a presença futura de uma norma não assegurará sua efetividade. A amostra intencional não autoriza a generalização estatística para todas as agremiações brasileiras. O corte temporal anterior às resoluções de 2026 exige cautela na formulação das conclusões. O achado é um diagnóstico documental do período analisado e uma base para pesquisa longitudinal, não uma afirmação definitiva sobre toda a governança partidária atual.

4. Diagnóstico documental da integridade digital partidária

4.1 Resultados da matriz comparativa

A reclassificação dos dez partidos confirmou a hipótese no plano documental delimitado. Nenhum estatuto analisado apresentou menção expressa a deepfake, conteúdo sintético ou uso eleitoral de inteligência artificial. Também não foram identificadas regras específicas sobre desinformação ou notícias falsas que reunissem definição, dever de prevenção, competência de apuração e consequência institucional. O resultado foi igualmente negativo para códigos de conduta digital e sistemas estruturados de governança informacional. Em termos descritivos, a frequência de presença foi zero em dez documentos para as quatro categorias principais. O dado quantitativo auxilia a visualização do padrão, mas sua relevância é qualitativa. A lacuna não consiste apenas na ausência de palavras recentes. Ela envolve a inexistência de uma arquitetura normativa que distribua responsabilidades, documente fluxos de comunicação e ofereça resposta interna verificável.

Tabela 2 - Matriz comparativa de integridade informacional

Partido	Desinformação ou fake news	IA, conteúdo sintético ou deepfake	Conduta digital específica	Governança informacional estruturada
UNIÃO	Não	Não	Não	Não
PT	Não	Não	Não	Não
MDB	Não	Não	Não	Não
PSD	Não	Não	Não	Não
PP	Não	Não	Não	Não
PSDB	Não	Não	Não	Não
PL	Não	Não	Não	Não
PSB	Não	Não	Não	Não
PDT	Não	Não	Não	Não
Republicanos	Não	Não	Não	Não

Fonte. Elaboração dos autores. “Não” indica ausência de dispositivo explícito ou mecanismo institucional específico no corpus e no marco temporal da pesquisa.

Os documentos possuem normas gerais sobre fidelidade, disciplina, deveres partidários, respeito ao programa, prestação de contas e aplicação de sanções. Essas disposições podem oferecer fundamento residual para reagir a condutas gravemente desleais ou ilícitas. Entretanto, sua generalidade produz incerteza operacional. Elas não definem quem deve revisar conteúdo sintético, como registrar o uso de ferramentas de inteligência artificial, quais fornecedores precisam ser identificados, quando uma denúncia deve ser comunicada à Justiça Eleitoral, quais evidências devem ser preservadas ou quais indicadores permitem avaliar a resposta do partido. A aplicação analógica de cláusulas éticas pode ser útil depois do incidente, mas não substitui um sistema de prevenção desenhado para riscos digitais.

A ausência de previsão estatutária não exige que documentos partidários antecipem toda inovação tecnológica. Normas internas podem utilizar conceitos abertos e regulamentos flexíveis. O problema aparece quando riscos já reconhecidos pela literatura e pela regulação eleitoral não encontram tradução organizacional mínima. Deepfakes e campanhas coordenadas não são atos espontâneos em todos os casos. Sua produção pode envolver contratação de agência, aquisição de ferramentas, autorização de despesa, impulsionamento, distribuição de arquivos e mobilização de redes. Cada etapa deixa pontos de controle possíveis. Sem atribuição de responsabilidades, a organização depende da iniciativa individual e tende a reagir apenas quando o dano alcança relevância pública ou judicial.

4.2. Externalidades democráticas e responsabilidade institucional

A omissão partidária produz uma externalidade democrática. O candidato ou grupo que utiliza desinformação pode apropriar-se de vantagem eleitoral imediata, enquanto os custos da correção são distribuídos entre adversários, imprensa, sociedade civil, plataformas, Justiça Eleitoral e eleitorado. A vantagem é privada e o dano é socializado. Essa assimetria cria incentivo para estratégias de alto impacto e baixa rastreabilidade, sobretudo quando o risco de sanção interna é inexistente ou indefinido. Um programa de integridade modifica a estrutura de incentivos ao elevar o custo reputacional e disciplinar da manipulação, preservar registros e tornar previsível a resposta da agremiação. Sua função não é garantir ausência absoluta de ilícitos, mas reduzir tolerância, opacidade e impunidade organizacional.

O financiamento público reforça a dimensão institucional do problema. Recursos partidários e eleitorais sustentam estruturas de campanha, comunicação e mobilização que podem ser utilizadas tanto para informar quanto para manipular. A responsabilidade fiduciária não autoriza controle estatal do conteúdo ideológico das legendas, mas exige que verbas públicas não sejam administradas sem mecanismos mínimos de prevenção à fraude informacional. Cavalcante (2025) utiliza os dados de financiamento e representação para demonstrar a centralidade material dos partidos. A presente pesquisa não apresenta esse levantamento como novo. Sua contribuição específica está na aplicação de uma matriz de integridade digital ao corpus e na articulação do diagnóstico com as regras eleitorais editadas em 2026.

A lacuna tem ainda efeito probatório. Quando um conteúdo é questionado, a inexistência de registros sobre autoria, versão, aprovação, tecnologia utilizada e cadeia de distribuição dificulta separar conduta individual de decisão institucional. O partido pode não conseguir demonstrar diligência, interromper a circulação ou cooperar com a apuração. A rastreabilidade protege o processo eleitoral e a própria agremiação. Ela permite identificar incidentes, preservar

evidências, corrigir conteúdo e demonstrar que o sistema interno funcionou. Em vez de ampliar a responsabilidade objetiva, controles bem desenhados oferecem critérios para avaliar culpa organizacional, tolerância, falha de supervisão e resposta tempestiva.

A integridade informacional também está associada à confiança democrática. Deepfakes podem atingir candidaturas, autoridades, urnas, imprensa e procedimentos de votação. O dano sistêmico não depende de alteração comprovada do resultado. A propagação de suspeita generalizada sobre a possibilidade de conhecer fatos públicos já compromete a legitimidade do processo. O partido, por sua capilaridade, pode atuar antes da viralização, especialmente sobre equipes, fornecedores e canais oficiais. Sua intervenção não elimina a necessidade de educação midiática, perícia, regulação das plataformas e tutela judicial. Ela cobre, contudo, o elo institucional que permanece mais próximo da origem de parcela relevante da comunicação eleitoral organizada.

4.3. Alcance do achado e critérios de atualização

O resultado negativo em todas as categorias deve ser interpretado com precisão. Ele não significa ausência absoluta de valores éticos nos estatutos nem impossibilidade de responsabilizar condutas digitais com base em regras gerais. Significa que, no marco documental examinado, os riscos informacionais não haviam sido traduzidos em deveres operacionais próprios. Essa distinção impede tanto a minimização quanto a superestimação do achado. A ausência de terminologia específica seria pouco relevante se os documentos contivessem mecanismos funcionalmente equivalentes. A leitura contextual, porém, não encontrou responsável por integridade digital, fluxo de aprovação, obrigação de rastreabilidade, protocolo para conteúdo sintético, canal especializado ou relatório de incidentes. O déficit identificado é, portanto, organizacional e não meramente vocabular.

A confiabilidade da classificação depende de critérios replicáveis. Uma futura atualização deve conservar as mesmas categorias, registrar a versão exata de cada documento, indicar data de acesso e arquivar cópia do corpus. Alterações podem ser classificadas segundo grau de institucionalização. A simples inclusão da expressão desinformação representa avanço declaratório, mas não equivale a um programa. Um segundo nível exige deveres e vedações. Um terceiro acrescenta competências, procedimentos e sanções. O nível mais elevado reúne prevenção, detecção, resposta, indicadores, auditoria e prestação de contas. Essa escala permite acompanhar a evolução sem reduzir a análise a contagem de palavras e oferece base para comparação entre eleições e agremiações.

A pesquisa também distingue inovação analítica de novidade absoluta dos dados. A seleção partidária e parte da coleta original foram anteriormente trabalhadas por Cavalcante (2025) em estudo sobre compliance partidário. O presente artigo não reivindica primazia sobre esse levantamento. Sua originalidade está no recorte da integridade informacional, na matriz digital específica, na delimitação uniforme do corpus e na comparação com o marco eleitoral de 2026. Essa formulação evita autodeclarações amplas de ineditismo e permite identificar com exatidão o que foi reutilizado, reclassificado e desenvolvido. Em pesquisas de coautoria que utilizam obra prévia de um dos autores, essa transparência é condição de integridade científica e favorece a avaliação do efetivo acréscimo intelectual.

O diagnóstico pode orientar pesquisa empírica mais ampla. Entrevistas com dirigentes, responsáveis jurídicos e equipes de comunicação permitiriam verificar protocolos não publicados. Estudos de caso poderiam examinar como partidos reagiram a conteúdos manipulados, quanto tempo levaram para interromper a circulação e quais evidências preservaram. Uma etapa quantitativa poderia medir número de incidentes, alcance, reincidência, tempo de resposta e aplicação de sanções, desde que os indicadores fossem definidos antes da coleta e integrados à interpretação qualitativa. O desenho atual oferece a linha de base documental necessária para esse desenvolvimento, sem atribuir aos dados uma generalização que eles não suportam.

5. Programa de Integridade Informacional Partidária

5.1. Arquitetura mínima e sete pilares

O Programa de Integridade Informacional Partidária é uma arquitetura mínima de governança aplicável à comunicação eleitoral e partidária digital. O PIIP deve ser incorporado ao estatuto, ao código de ética ou a regulamento nacional vinculante, com possibilidade de adaptação por diretórios regionais e campanhas conforme porte, risco e capacidade. Sua efetividade depende de integração com as áreas jurídica, financeira, de comunicação, tecnologia, proteção de dados e disciplina. A proposta organiza-se em sete pilares complementares, concebidos para articular prevenção, detecção, resposta, responsabilização e aperfeiçoamento contínuo.

Tabela 3 - Pilares do Programa de Integridade Informacional Partidária

Pilar	Conteúdo mínimo	Resultado esperado
1 Liderança e governança	Aprovação formal, responsável independente, recursos, supervisão e indicadores.	Responsabilidade visível e capacidade de execução.
2 Riscos e código digital	Mapeamento periódico, regras sobre IA, deepfakes, fornecedores, impulsionamento e rotulagem.	Previsibilidade de condutas permitidas e vedadas.
3 Formação e cultura	Treinamento obrigatório para dirigentes, candidatos, equipes e prestadores.	Redução de erro, negligência e racionalização oportunista.
4 Controles e denúncia	Rastreabilidade de peças, revisão por risco, preservação de evidências e canal protegido.	Deteção precoce e resposta documentada.
5 Apuração e sanção	Procedimento célere, imparcial, com contraditório, gradação de sanções e cooperação externa.	Responsabilização proporcional e correção de incidentes.
6 Cooperação democrática	Protocolos com Justiça Eleitoral, plataformas, universidades, imprensa e sociedade civil.	Compartilhamento de alertas, evidências e boas práticas.
7 Auditoria e contas	Relatórios periódicos, métricas, revisão independente e plano de melhoria.	Transparência, aprendizagem e efetividade verificável.

Fonte. Elaboração dos autores a partir de referenciais de integridade da OECD (2017, 2020), do COSO (2013) e da ISO 37301:2021, adaptados à função constitucional dos partidos.

O primeiro pilar exige compromisso verificável da liderança. A executiva nacional deve aprovar o programa, designar responsável com acesso à direção, definir orçamento e receber relatórios periódicos. A função de

integridade precisa de autonomia para suspender a distribuição de peça de alto risco até análise técnica, sem subordinação exclusiva à equipe que concebeu a estratégia. O *tone at the top* não se resume a declaração pública. Ele se manifesta na alocação de recursos, na proteção de denunciantes, na disposição de investigar agentes influentes e na aplicação coerente de consequências. A liderança deve ainda estabelecer responsabilidade em todas as camadas partidárias, evitando que diretórios locais e campanhas funcionem como zonas sem supervisão.

O segundo pilar reúne avaliação de riscos e Código de Conduta Digital. A matriz deve considerar período eleitoral, alcance dos canais, uso de mensageria privada, contratação de influenciadores, impulsionamento, geração de conteúdo sintético, terceirização, histórico de incidentes e vulnerabilidade de grupos atingidos. O código precisa vedar deepfakes enganosos, falsificação de documentos, uso não rotulado de conteúdo sintético quando exigido, montagem sexualizada, manipulação de autoridades eleitorais e campanhas coordenadas de desinformação. Deve exigir identificação de responsáveis, declaração das ferramentas utilizadas, cláusulas contratuais de integridade e preservação de arquivos originais. Usos legítimos de inteligência artificial, como tradução, acessibilidade, edição não enganosa e simulação claramente identificada, podem ser admitidos mediante transparência e avaliação de risco.

O terceiro pilar transforma regras em cultura. Treinamentos gerais devem alcançar filiados e dirigentes, enquanto módulos específicos precisam ser obrigatórios para candidatos, coordenadores, equipes de comunicação, departamentos jurídicos, responsáveis financeiros e fornecedores. O conteúdo deve abranger identificação de manipulações, deveres de rotulagem, riscos da mensageria, proteção de dados, direitos da personalidade, violência política, preservação de evidências e fluxo de resposta. A capacitação deve ocorrer antes do início da campanha e ser atualizada diante de mudanças normativas ou tecnológicas. Registros de participação, avaliações e estudos de caso permitem medir a compreensão e aperfeiçoar o programa. A educação digital não é atividade periférica, pois os partidos exercem função de formação política e devem formar agentes capazes de atuar responsavelmente na esfera pública.

O quarto pilar abrange controles internos, rastreabilidade e canais seguros de denúncia. Materiais oficiais e impulsionados devem possuir identificação de autoria, versão, data, aprovadores, fornecedor, fonte de dados, tecnologia de geração e canais de distribuição. O nível de revisão deve ser proporcional ao risco. Conteúdos que reproduzam voz ou imagem de pessoas, tratem do sistema eleitoral ou circulem próximo à votação exigem escrutínio reforçado. O canal de denúncia deve ser acessível a filiados, colaboradores, fornecedores e público externo, permitir anonimato quando juridicamente possível e proteger contra retaliações. O programa precisa definir triagem, prioridade, prazo,

preservação de provas, suspensão cautelar e comunicação interna, sem converter o monitoramento em vigilância indiscriminada de opiniões privadas.

O quinto pilar disciplina a apuração, sanção e cooperação com autoridades. A investigação deve ser conduzida por equipe imparcial, com competência técnica e registro dos atos. O investigado precisa conhecer a imputação, apresentar manifestação e recorrer na forma do estatuto. Medidas cautelares, como retirada de conteúdo de canal oficial ou suspensão de impulsionamento, podem ser necessárias para interromper dano, desde que fundamentadas e revistas. A sanção deve considerar dolo, gravidade, alcance, posição do agente, uso de recursos públicos, reincidência, colaboração e reparação. Advertência, treinamento corretivo, perda de função, suspensão, descredenciamento de fornecedor e expulsão podem ser graduados segundo o caso. Índícios de ilícito eleitoral, civil ou penal devem ser comunicados à autoridade competente, preservada a cadeia de custódia das evidências.

O sexto pilar reconhece que integridade informacional é problema coletivo. Partidos podem estabelecer protocolos de alerta recíproco para conteúdos que atinjam o processo eleitoral, sem pactos sobre mérito político ou supressão de críticas. Cooperação com o TSE, tribunais regionais, plataformas, universidades, organizações de verificação e imprensa melhora a identificação técnica e a velocidade de resposta. Esses acordos devem preservar independência, dados pessoais, sigilo de apurações e pluralismo. O partido não pode terceirizar seu juízo disciplinar a verificadores privados, mas pode utilizar conhecimento especializado para confirmar manipulações e compreender padrões de disseminação.

O sétimo pilar estabelece auditoria, indicadores e prestação de contas. Relatórios anuais ou eleitorais devem informar treinamentos realizados, riscos mapeados, denúncias recebidas, tempo de resposta, incidentes confirmados, medidas corretivas e sanções em dados agregados. Indicadores não devem incentivar remoções automáticas ou quantidade artificial de punições. Sua finalidade é medir efetividade, recorrência, cobertura e aprendizagem. Auditoria independente ou revisão por órgão interno autônomo pode verificar desenho e funcionamento. A transparência deve proteger dados pessoais, sigilo processual e estratégia legítima de campanha. O resultado esperado é uma prestação de contas informacional que complemente a prestação financeira e permita avaliar se recursos, estruturas e tecnologias foram utilizados de maneira compatível com a integridade eleitoral.

5.2. Proporcionalidade, liberdade de expressão e devido processo

A principal objeção ao PIIP é o risco de censura interna. Essa preocupação é legítima e deve orientar o desenho do programa. A liberdade de expressão

protege crítica contundente, sátira, opinião, disputa de narrativas e divergência intrapartidária. O programa não pode impor verdade oficial sobre programas, diagnósticos econômicos ou escolhas ideológicas. Sua atuação deve concentrar-se em condutas verificáveis, como falsificação de identidade, manipulação audiovisual enganosa, descumprimento de rotulagem, fabricação de fatos, uso indevido de recursos, ocultação de autoria e desobediência a ordens eleitorais. Definições claras, decisão fundamentada, contraditório e recurso reduzem o risco de uso faccional do compliance.

A proporcionalidade exige adequação entre controle e risco. Não é razoável submeter toda postagem individual de filiado a aprovação central. O alcance prioritário deve recair sobre canais oficiais, propaganda, peças financiadas, equipes contratadas, dirigentes, candidatos e agentes que representem institucionalmente a agremiação. Conteúdos de elevado impacto merecem revisão reforçada, enquanto comunicações ordinárias podem ser submetidas a orientação e monitoramento posterior. O sistema deve observar a proteção de dados e segurança da informação. Registros precisam ter finalidade definida, acesso restrito e prazo de retenção compatível com obrigações eleitorais e disciplinares.

A autonomia partidária pode, inclusive, favorecer a institucionalização do PIIP. Em vez de aguardar regulamentação estatal minuciosa sobre toda rotina interna, as agremiações podem construir padrões próprios, adaptados a sua estrutura e identidade, desde que respeitem direitos fundamentais e a legislação. A exigibilidade jurídica defendida neste artigo opera em níveis. No plano atual, deveres de diligência podem ser extraídos da função constitucional dos partidos, da disciplina da propaganda, do dever de prestação de contas e da proibição de ilícitos eleitorais. No plano de política legislativa, seria possível exigir relatório de integridade informacional ou critérios mínimos para o uso de recursos públicos em comunicação digital. Qualquer condicionamento financeiro deve ser gradual, legalmente previsto, proporcional e acompanhado de suporte para partidos de menor porte.

5.3. Implementação escalonada e indicadores de efetividade

A implantação do PIIP pode ocorrer em ciclos. O primeiro ciclo compreende diagnóstico, designação de responsável, aprovação do código digital e mapeamento dos fluxos de comunicação. O segundo consolida treinamentos, cláusulas contratuais, canal de denúncia e procedimentos de resposta. O terceiro introduz auditoria, métricas, testes de efetividade e cooperação externa. Esse escalonamento permite adequar o programa ao porte da agremiação sem transformar limitações de estrutura em justificativa para inércia. Partidos nacionais com maior volume de candidaturas e recursos devem apresentar controles mais sofisticados, enquanto legendas menores

podem compartilhar soluções técnicas, modelos de treinamento e serviços independentes, desde que preservem responsabilidade e autonomia decisória.

Indicadores de desenho verificam se os elementos necessários existem. Entre eles estão aprovação formal, independência do responsável, cobertura do código, inclusão de fornecedores, existência de matriz de risco, canal protegido e protocolo de preservação de evidências. Indicadores de operação medem se o sistema funciona, considerando percentual de agentes treinados, tempo médio de triagem, proporção de peças de alto risco revisadas, cumprimento de prazos, qualidade dos registros e adoção de medidas corretivas. Indicadores de resultado devem ser usados com cautela. Redução de incidentes confirmados, menor reincidência e resposta mais rápida podem sugerir efetividade, mas números baixos também podem revelar subnotificação. Por isso, métricas precisam ser interpretadas em conjunto e acompanhadas de revisão qualitativa.

Testes periódicos são indispensáveis. Exercícios simulados podem reproduzir a divulgação de vídeo falso próximo à votação e avaliar quem decide, quais canais são acionados, quanto tempo se leva para preservar arquivos, suspender impulsionamento, publicar correção e comunicar autoridades. A simulação identifica falhas que documentos formais não revelam. Auditorias por amostragem podem verificar contratos, registros de aprovação e rotulagem. Pesquisas de percepção com candidatos, equipes e denunciante ajudam a medir conhecimento, confiança no canal e medo de retaliação. A melhoria contínua exige que incidentes sejam convertidos em aprendizado, não apenas em punição individual.

A prestação pública de contas deve apresentar informação suficiente para permitir escrutínio sem expor dados pessoais ou estratégias legítimas. O relatório pode informar escopo do programa, governança, treinamentos, categorias de risco, números agregados de denúncias, tempos de resposta, providências e recomendações de auditoria. A publicação deve explicar a metodologia dos indicadores e suas limitações, evitando métricas promocionais. O TSE poderia, em futura regulamentação ou orientação, disponibilizar modelo mínimo de relatório e repositório voluntário, favorecendo comparabilidade e difusão de boas práticas. O papel estatal, nesse estágio, seria estabelecer transparência e interoperabilidade, sem impor uniformidade ideológica ou gerir a disciplina interna dos partidos.

6. PIIP e regulação eleitoral para 2026

O TSE ampliou em 2026 o regime de propaganda e de ilícitos eleitorais relacionados à inteligência artificial. A Resolução nº 23.755/2026 alterou a Resolução nº 23.610/2019 e preservou o dever de informar, de modo explícito,

destacado e acessível, a fabricação ou manipulação de conteúdo sintético e a tecnologia utilizada. Acrescentou restrição à publicação, republicação e impulsionamento de novos conteúdos sintéticos que utilizem imagem, voz ou manifestação de candidato ou pessoa pública entre as setenta e duas horas anteriores e as vinte e quatro horas posteriores ao término do pleito, mesmo quando rotulados. A norma prevê remoção em caso de descumprimento, instrumentos de denúncia e medidas voltadas a conteúdos repetidos ou equivalentes aos já considerados ilícitos (TSE, 2026b).

A resolução enfrentou ainda assimetrias técnicas. O artigo 9º-I permite que o juiz inverta motivadamente o ônus da prova quando a comprovação da manipulação for excessivamente onerosa, transferindo ao responsável o dever de demonstrar a licitude, as etapas de uso da inteligência artificial e a veracidade da informação. O artigo 28, parágrafo 1º-C, veda a sistemas de inteligência artificial ranquear ou recomendar candidaturas, emitir preferência eleitoral, criar conteúdo sexualizado envolvendo candidato ou formular publicidade que represente violência política contra a mulher. O artigo 125-B exige dos provedores de aplicação um plano de conformidade com medidas, indicadores, prazos e resultados esperados. A Resolução nº 23.757/2026 acrescentou que a difusão de informações falsas ou descontextualizadas e o uso irregular de conteúdo sintético podem configurar uso indevido dos meios de comunicação e, conforme as circunstâncias, abuso dos poderes político e econômico (TSE, 2026c).

O marco não pode ser caracterizado como exclusivamente reativo. Rotulagem, restrição temporal, planos de conformidade e canais preventivos demonstram preocupação ex ante. Sua efetividade, contudo, enfrenta limites de escala, velocidade, prova e alcance em ambientes privados. A Justiça Eleitoral depende de informações, denúncias, cooperação técnica e cumprimento por intermediários. A regulação externa estabelece padrões gerais e consequências, mas não acompanha cada decisão interna de campanha. O PIIP ocupa esse espaço sem competir com o TSE. Ele busca impedir que conteúdo irregular seja produzido, financiado ou distribuído por estruturas partidárias e, quando o incidente ocorre, preserva elementos que facilitam remoção, correção e responsabilização.

Há uma assimetria normativa relevante. Provedores de aplicação passaram a estar sujeitos a planos de conformidade com critérios mensuráveis, enquanto não existe obrigação eleitoral equivalente e detalhada de programa interno para os partidos. A diferença pode ser explicada pelas capacidades técnicas e pelo papel específico das plataformas, mas não elimina a necessidade de governança partidária. Se a regulação reconhece que organizações privadas que estruturam a circulação devem mapear e mitigar riscos, é coerente exigir diligência compatível das organizações que estruturam candidaturas, campanhas e recursos. A resposta mais adequada é uma correção

democrática na qual o TSE define limites públicos, plataformas cumprem deveres de transparência e mitigação, partidos internalizam controles e sociedade civil contribui com pesquisa e verificação.

A relação entre PIIP e regime sancionatório deve evitar automatismos. A existência de programa não afasta responsabilidade por ilícito nem cria imunidade. Sua efetividade pode ser considerada na análise de diligência, resposta, colaboração e falha organizacional. Um programa meramente formal, sem recursos ou aplicação, não deve produzir benefício. Em sentido inverso, a ausência de PIIP não transforma todo conteúdo irregular de filiado em ato institucional do partido. A responsabilidade depende de vínculo, conhecimento, autorização, financiamento, benefício, capacidade de controle e reação. O valor do programa está em tornar esses elementos documentáveis e reduzir zonas de opacidade.

7. Conclusão

A pesquisa perguntou em que medida os principais partidos políticos brasileiros haviam incorporado mecanismos internos capazes de prevenir, detectar, apurar e sancionar deepfakes e desinformação eleitoral. O corpus padronizado de dez agremiações, delimitado aos documentos aprovados e disponíveis até 31 de dezembro de 2023, não apresentou regras específicas nas quatro categorias examinadas. A hipótese foi confirmada no plano documental e temporal definido. Disposições gerais de ética e disciplina oferecem fundamento residual, mas não constituem sistema de governança informacional com responsáveis, procedimentos, rastreabilidade, treinamento, canais, indicadores e prestação de contas.

O achado não autoriza afirmar que todos os partidos permaneceram inertes em toda campanha ou que documentos posteriores não tenham introduzido mudanças. A análise mede institucionalização formal e não desempenho real. Sua contribuição consiste em revelar a distância entre riscos digitais reconhecidos e a estrutura normativa interna então disponível, a partir de corpus uniforme de dez agremiações e de categorias replicáveis de integridade informacional. A obra de Cavalcante (2025), escrita por um dos autores, foi declarada como fonte da seleção e da contextualização, enquanto a contribuição específica do artigo foi delimitada como releitura orientada à integridade informacional e cotejo com as normas de 2026.

O Programa de Integridade Informacional Partidária oferece resposta concreta ao diagnóstico. Seus sete pilares articulam liderança, avaliação de riscos, código digital, formação, controles, denúncia, apuração, sanção, cooperação, auditoria e contas. O PIIP não deve controlar a opinião política nem substituir a Justiça Eleitoral. Seu campo legítimo é a comunicação institucional, as

campanhas, os fornecedores, os recursos administrados e os agentes sob direção partidária. Devido processo, proporcionalidade, proteção de dados e distinção entre crítica e fraude são condições de validade do modelo.

As resoluções do TSE para 2026 representam avanço ao disciplinar rotulagem, restrições temporais, prova, sistemas de inteligência artificial, ilícitos e planos de conformidade das plataformas. A regulação estatal contém instrumentos preventivos, mas não alcança integralmente a rotina interna de produção e circulação de conteúdo. O PIIP funciona como primeira camada organizacional e elemento de uma correção democrática. Ele reduz riscos antes da viralização, melhora a rastreabilidade e facilita a cooperação posterior, sem afastar sanções nem criar responsabilidade automática.

A agenda de pesquisa deve atualizar longitudinalmente os estatutos e regulamentos partidários após 2026, examinar práticas concretas, comparar respostas a incidentes e construir indicadores de efetividade. Estudos futuros podem incluir entrevistas, observação de campanhas e análise de decisões eleitorais, ampliando o desenho qualitativo com dados quantitativos sobre denúncias, tempo de resposta e reincidência. A integridade eleitoral não depende apenas de remoção e punição tardias. Ela exige que os partidos reconheçam a comunicação digital como dimensão central de sua responsabilidade democrática e adotem estruturas capazes de transformar prudência em prática institucional verificável.

8. Referências bibliográficas

Aquino, T. de. (2004). *Suma teológica* (Vol. 5, II-II, Questões 1-56). Loyola.

Aristóteles. (1991). *Ética a Nicômaco* (L. Vallandro & G. Bornheim, Trans.). Nova Cultural.

Batista, A. R. F., & Santaella, L. (2024). Prognósticos das deepfakes na política eleitoral. *Organicom*, 21(44), 187-196.
<https://doi.org/10.11606/issn.2238-2593.organicom.2024.221294>

Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*, 33(2), 122-139. <https://doi.org/10.1177/0267323118760317>

Brasil. (1988). *Constituição da República Federativa do Brasil de 1988*. Presidência da República.

Brasil. (1995). *Lei nº 9.096, de 19 de setembro de 1995*. Presidência da República.

Brasil. (1997). *Lei nº 9.504, de 30 de setembro de 1997*. Presidência da República.

- Carvalho, A. C., Bertocelli, R. P., Alvim, T. C., & Venturini, O. (Orgs.). (2020).** *Manual de compliance* (2ª ed.). Forense.
- Cavalcante, A. (2025).** *Partidos políticos e compliance: Um debate acerca da obrigatoriedade*. Ambra University Press.
- Chesney, R., & Citron, D. K. (2019).** Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753-1820. <https://doi.org/10.15779/Z38RV0D15J>
- Committee of Sponsoring Organizations of the Treadway Commission. (2013).** *Internal control-integrated framework*. COSO.
- Habermas, J. (1989).** *The structural transformation of the public sphere: An inquiry into a category of bourgeois society*. MIT Press.
- International Organization for Standardization. (2021).** *ISO 37301:2021 Compliance management systems-requirements with guidance for use*. ISO.
- Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020).** Deepfakes: Trick or treat? *Business Horizons*, 63(2), 135-146. <https://doi.org/10.1016/j.bushor.2019.11.006>
- Lessig, L. (1999).** *Code and other laws of cyberspace*. Basic Books.
- Mulholland, C., & Oliveira, S. R. de. (2021). Uma nova cara para a política? Considerações sobre deepfakes e democracia. *Direito Público*, 18(99), 368-396. <https://doi.org/10.11117/rdp.v18i99.5773>
- Organisation for Economic Co-operation and Development. (2017).** *Recommendation of the Council on Public Integrity*. OECD Publishing.
- Organisation for Economic Co-operation and Development. (2020).** *OECD public integrity handbook*. OECD Publishing. <https://doi.org/10.1787/ac8ed8e8-en>
- Paris, B., & Donovan, J. (2019).** *Deepfakes and cheap fakes: The manipulation of audio and visual evidence*. Data & Society.
- Pasquale, F. (2015).** *The black box society: The secret algorithms that control money and information*. Harvard University Press.
- Pawelec, M. (2022).** Deepfakes and democracy theory: How synthetic audio-visual media for disinformation and hate speech threaten core democratic functions. *Digital Society*, 1, Article 19. <https://doi.org/10.1007/s44206-022-00010-6>
- Tribunal Superior Eleitoral. (2026a).** *Partidos políticos registrados no TSE*. Recuperado em 21 de julho de 2026, de <https://www.tse.jus.br/partidos/partidos-registrados-no-tse>

Tribunal Superior Eleitoral. (2026b). *Resolução nº 23.755, de 2 de março de 2026.* <https://www.tse.jus.br/legislacao/compilada/res/2026/resolucao-no-23-755-de-2-de-marco-de-2026>

Tribunal Superior Eleitoral. (2026c). *Resolução nº 23.757, de 2 de março de 2026.* <https://www.tse.jus.br/legislacao/compilada/res/2026/resolucao-no-23-757-de-2-de-marco-de-2026>

Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media + Society*, 6(1), 1-13.
<https://doi.org/10.1177/2056305120903408>

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* PublicAffairs.

9. Declarações

Contribuição dos autores. Alex Cavalcante dos Santos e Rafael Gomes de Araújo contribuíram conjuntamente para a concepção do estudo, delimitação metodológica, levantamento e análise documental, desenvolvimento do PIIP, redação, revisão crítica e aprovação da versão final.

Transparência da fonte e conflito de interesses. Alex Cavalcante dos Santos é autor da obra Partidos Políticos e Compliance, utilizada para fundamentar o critério de seleção e contextualizar os dados de financiamento partidário. Essa relação foi declarada, a fonte não substituiu a reanálise documental realizada para o presente artigo e os autores não identificam conflito de interesses financeiro ou institucional.

Financiamento. A pesquisa não recebeu financiamento externo específico.

Disponibilidade dos dados. O corpus é composto por documentos públicos disponíveis no repositório institucional do Tribunal Superior Eleitoral. As categorias de codificação e os resultados consolidados constam da metodologia e das tabelas deste artigo.

Uso de inteligência artificial. Os autores utilizaram o ChatGPT, da OpenAI, exclusivamente como ferramenta auxiliar de revisão linguística, padronização formal e conferência editorial. O texto-base, a seleção bibliográfica, o desenho metodológico, a análise documental, as interpretações, a formulação do PIIP e as decisões substantivas de redação foram elaborados e validados pelos autores. Todas as fontes foram conferidas em documentos originais, periódicos, editoras ou repositórios institucionais, e os autores assumem integral responsabilidade pelo conteúdo.