idp | lia·idp Laboratório de governança e regulação de inteligência Artificial | CEDIS Centro de Direito, Internet e Sociedade

Integridade da informação nas eleições e plataformas digitais: caminhos para a corregulação

Relatório de pesquisa

Código de catalogação na publicação – CIP

M538i Mendes, Laura Schertel Ferreira
Integridade da informação nas eleições e plataformas digitais: caminhos para a corregulação / MENDES, L. S. F.; FERREIRA, L. M. T.; JUNQUILHO, T. A.; CRUZ, F. B.; SILVEIRA, M. de P.; GONÇALVES, C. G. B.; PONCE, P. P. (coord.). — Brasília: Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, 2026.

287 f. : il.
ISBN 978-65-87546-46-9

1. Eleição. 2. Internet. 3. Plataformas digitais. I. Título

CDDir 341.28

Elaborada por Biblioteca Ministro Moreira Alves

Como citar este documento:
MENDES, L. S. F.; FERREIRA, L. M. T.; JUNQUILHO, T. A.; CRUZ, F. B.; SILVEIRA, M. de P.; GONÇALVES, C. G. B.; PONCE, P. P. (coord.). Integridade da informação nas eleições e plataformas digitais: caminhos para a corregulação. Brasília: Laboratório de Governança e Regulação de Inteligência Artificial (LIA) do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), 2026. ISBN 978-65-87546-46-9
Disponível em:
XXXXXXXXX. Acesso em: (dia) (mês abreviado) (ano).

Integridade da informação nas eleições e plataformas digitais: caminhos para a corregulação

Coordenadores
Laura Schertel Ferreira Mendes
Tainá Aguiar Junquilho
Lucia Maria Teixeira Ferreira
Francisco Brito Cruz
Marilda de Paula Silveira
Paula Pedigoni Ponce
Cacyone Gomes Barbosa Gonçalves

Autores
Bárbara Benato Pontalti
Bruna Ammon Lisboa
Cacyone Gomes Barbosa Gonçalves Lavareda
Danielly Cristina Araújo Gontijo
Elaine Gomes dos Santos
Francisco Brito Cruz
Guilherme Antonio Balczarek Mucelin
Ian Ferrare Meier
Juliana de Fátima Moreira Costa
Laura Schertel Ferreira Mendes
Lucia Maria Teixeira Ferreira
Marina Giovanetti Lili Lucena
Marilda de Paula Silveira
Matheus de Oliveira Ferreira
Paula Pedigoni Ponce
Stefani Juliana Vogel
Tainá Aguiar Junquilho
Tayná Frota de Araújo
Thiago Gomes Marcilio

Revisores
Cacyone Gomes Barbosa Gonçalves Lavareda
Camila Cristina da Silva
Ian Ferrare Meier
Lyvia Rocha de Jesus Araujo
Matheus Garcia

Diagramador
João Pedro Coppola Romancini

2.7 MB | PDF
287 páginas

1ª edição, 2026

SUMÁRIO

PARTE I - INTRODUÇÃO

Laura Schertel Ferreira Mendes, Tainá Aguiar Junquilho, Lucia Maria Teixeira Ferreira Francisco Brito Cruz, Marilda de Paula Silveira, Paula Pedigoni Ponce e Cacyone Gomes Barbosa Gonçalves

1.1 INTEGRIDADE DA INFORMAÇÃO E CORREGULAÇÃO NO CONTEXTO ELEITORAL DIGITAL

A transformação do ambiente informacional, impulsionada pela intermediação algorítmica e pela lógica de funcionamento das grandes plataformas digitais, impõe novos desafios à preservação da integridade dos processos democráticos. As eleições contemporâneas deixaram de ser fenômenos estritamente territoriais e se converteram em processos informacionais transnacionais, marcados pela circulação contínua de dados, narrativas e fluxos comunicacionais potencialmente manipuladores. Nesse contexto, a regulação da comunicação política digital tornou-se elemento central do constitucionalismo democrático e da efetividade dos direitos fundamentais na esfera digital.

O Tribunal Superior Eleitoral (TSE), atento a essa realidade, reformulou o regime jurídico da propaganda político-eleitoral na internet por meio da Resolução TSE n.º 23.732/2024, que alterou substancialmente a Resolução n.º 23.610/2019. A nova redação introduziu, entre outros dispositivos, o artigo 9º-D, que impõe aos provedores de aplicação de internet deveres positivos voltados à proteção da integridade do processo eleitoral. O dispositivo inaugura, assim, um microssistema regulatório de integridade informacional, estruturado em torno da prevenção, mitigação e transparência na circulação de conteúdos digitais de natureza político-eleitoral (Brasil, 2024).

Trata-se de um marco normativo que desloca o eixo da responsabilidade das plataformas de uma lógica reativa, centrada apenas na remoção de conteúdos ilícitos, para uma lógica preventiva e de dever de cuidado ampliado, que exige a adoção de políticas internas coerentes, transparentes e verificáveis. A incorporação expressa dos princípios da função social e do dever de cuidado ao regime das plataformas (art. 9º-D, § 4º) reforça essa mudança de paradigma, reconhecendo que tais agentes desempenham papel estrutural na formação da opinião pública e, portanto, devem exercer suas atividades de modo compatível com os valores constitucionais da democracia e com a proteção dos direitos fundamentais dos cidadãos.

Como recomendação geral de aprimoramento da Resolução TSE n.º 23.610/2019, evidencia-se a necessidade de disciplinar a granularidade das obrigações trazidas pela Resolução TSE n.º 23.732/2024, mediante parâmetros objetivos, a exemplo do número de usuários ativos no Brasil. Plataformas e mecanismos de busca de grande dimensão devem sujeitar-se a deveres mais rigorosos, dentre os quais se incluem a realização de auditorias independentes anuais e a apresentação de relatórios periódicos mais frequentes. Ressalta-se, ademais, que a definição desses critérios objetivos para a aplicação diferenciada das obrigações demanda amplo debate técnico e institucional no âmbito da competência normativa do Tribunal Superior Eleitoral, de forma a assegurar proporcionalidade, coerência regulatória e aderência às especificidades do ecossistema digital.

O relatório “Integridade da Informação nas Eleições e Plataformas Digitais: Caminhos para a Corregulação” parte justamente dessa inflexão normativa. Seu objetivo é examinar a estrutura e o alcance jurídico dos deveres impostos pela Resolução TSE n.º 23.610/2019 (com as atualizações da Res. n.º 23.732/2024) e propor caminhos concretos para o fortalecimento de um modelo de corregulação eleitoral. Parte-se do reconhecimento de que o enfrentamento da desinformação e da manipulação informacional não pode ser conduzido apenas por instrumentos de enforcement estatal, exigindo arranjos cooperativos entre o poder público, as plataformas digitais e a sociedade civil. Essa perspectiva de governança distribuída traduz a compreensão de que a integridade informacional é um bem jurídico coletivo cuja proteção demanda coordenação institucional e compartilhamento de responsabilidades.

Inspirado por marcos internacionais, como o *Digital Services Act* (DSA) da União Europeia (2022), o *Online Safety Act* (OSA) do Reino Unido (2023), o modelo brasileiro delineado pela Resolução TSE n.º 23.610/2019 aproxima-se de um paradigma híbrido, em que a autorregulação das plataformas se submete a parâmetros públicos de integridade, proporcionalidade e transparência. A noção de corregulação aqui desenvolvida não se confunde com a transferência de funções regulatórias ao setor privado, mas com a construção de um espaço institucional de colaboração supervisionada, em que a Justiça Eleitoral define os objetivos e limites normativos, e as plataformas operacionalizam os meios técnicos de cumprimento, sob controle e fiscalização pública.

A análise comparada empreendida ao longo do relatório evidencia que a efetividade desse modelo depende da consolidação de uma cultura de *accountability* informacional nas plataformas, pautada por quatro eixos estruturantes: (i) coerência normativa entre termos de uso, políticas internas e obrigações legais; (ii) transparência ativa e publicização dos resultados das ações de moderação e mitigação de riscos; (iii) existência de mecanismos de auditoria e revisão independentes; e (iv) compromisso institucional com a preservação da integridade eleitoral como valor público transversal. Em síntese, a integridade da informação passa a ser tratada como um direito de cidadania digital, cuja proteção requer a integração entre regulação pública, dever de cuidado privado e participação social qualificada.

Somente por meio dessa estrutura de governança cooperativa e responsiva, fundada em técnica, transparência e legitimidade democrática, será possível assegurar que o espaço digital continue a servir como arena plural de expressão política, e não como vetor de erosão da confiança pública nas instituições eleitorais.

1.2 A FUNÇÃO SOCIAL E O DEVER DE CUIDADO: PRINCÍPIOS ORIENTADORES DA ATUAÇÃO DAS PLATAFORMAS DIGITAIS NO CONTEXTO ELEITORAL

O art. 9º-D, § 4º, da Resolução TSE n.º 23.610/2019 incorporou expressamente a função social e o dever de cuidado como princípios norteadores dos termos de uso das plataformas, vinculando-os ao dever de prevenção voltado a evitar ou mitigar a utilização de seus serviços para a prática de ilícitos eleitorais (Brasil, 2019a).

No que tange à função social, trata-se do princípio clássico da função social da empresa, consagrado nos arts. 116, parágrafo único, e 154 da Lei n.º 6.404/1976 (Lei das Sociedades Anônimas – LSA), com a particularidade de sua aplicação aos provedores de aplicação de internet (Brasil, 1976). Tal aplicação parte do reconhecimento de que a atuação dessas entidades transcende a dimensão meramente econômica, uma vez que operam sobre interesses da mais alta relevância social, como a preservação da integridade do processo eleitoral e a efetivação da autodeterminação do eleitorado e dos demais cidadãos que dela dependem (Ferreira, 2025; Frazão, 2011).

Nessa esteira, a função social mencionada pelo art. 9º-D, § 4º, da Resolução TSE n.º 23.610/2019 deve ser compreendida como princípio que, informado pelos valores constitucionais da dignidade da pessoa humana, do valor social da livre iniciativa, da igualdade substancial e da solidariedade social, impõe aos provedores de aplicação de internet o dever de conciliar seus interesses individuais e

econômicos com a tutela de interesses socialmente relevantes (Tepedino, 2009), cuja proteção jurídica se revela necessária diante da centralidade e notoriedade de seus serviços na sociedade digital contemporânea.

Dessa forma, a função social não se limita a conter condutas antissociais, mas orienta e direciona a prestação de serviços pelas plataformas de modo a compatibilizar o interesse público com o interesse econômico (Frazão, 2011). Em outras palavras, o princípio da função social, além de estabelecer limites negativos ao exercício da livre iniciativa, impõe também uma atuação positiva dos provedores de aplicação de internet em prol do interesse público, notadamente no que se refere à preservação do regime democrático.

Como consectário lógico do princípio da função social, o dever de cuidado configura-se como um dever jurídico que impõe às plataformas a implementação de medidas preventivas voltadas a impedir ou atenuar a utilização de seus serviços na prática de ilícitos eleitorais. Nessa acepção, o dever jurídico de cuidado vincula o provedor de aplicação aos valores democráticos e à ordem jurídica, exigindo a observância de um modelo de conduta diligente, em consonância com as expectativas da lei e da sociedade (Ferreira, 2025).

Antes mesmo da edição da Resolução TSE n. 23.610/2019, o direito brasileiro já contava, ainda que de forma implícita, com dever geral de cuidado em relações contratuais, sobretudo em decorrência do princípio da boa-fé objetiva (Frazão, 2021), que impõe às partes a adoção de um padrão de conduta pautado pela lealdade e confiança recíprocas, com destaque para sua função criadora de deveres anexos (Código Civil, art. 422), dentre os quais está o dever de proteção (Martins-Costa, 2019).

Demais disso, o dever de cuidado ganhou reforço, ao longo do tempo, diante da conclusão, já pacífica no âmbito dos tribunais, de que a relação entre plataformas e usuários é uma relação contratual de consumo[1]. Nesse sentido, o Código de Defesa do Consumidor (CDC) não deixa dúvidas quanto à necessidade de conferir ampla proteção ao consumidor, com destaque para o teor do inciso III do art. 4º que exige a compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (art. 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores (Brasil, 1990).

De forma complementar, o art. 6º, inciso VI, consagra como direito básico do consumidor a "efetiva prevenção e reparação dos danos patrimoniais e morais, individuais, coletivos e difusos", incorporando expressamente o dever de proteção.

Mais recentemente, o dever de cuidado adquiriu nova dimensão ao ser reconhecido pelo Supremo Tribunal Federal no julgamento do RE 1.075.412/PE (Tema 995 da Repercussão Geral), que trata da responsabilidade civil de empresa jornalística por declarações de terceiros em entrevista (Brasil, 2025). Na ocasião, a Corte estabeleceu a seguinte tese:

1 Confira-se, a título exemplificativo: "[...] 1. A exploração comercial da internet sujeita as relações de consumo daí advindas à Lei nº 8.078/90. 2. O fato de o serviço prestado pelo provedor de serviço de internet ser gratuito não desvirtua a relação de consumo, pois o termo 'mediante remuneração` contido no art. 3º, § 2º, do CDC deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor" (Brasil, 2010).

> **1. A plena proteção constitucional à liberdade de imprensa é consagrada pelo binômio liberdade com responsabilidade, vedada qualquer espécie de censura prévia. Admite-se a possibilidade posterior de análise e responsabilização, inclusive com remoção de conteúdo, por informações comprovadamente injuriosas, difamantes, caluniosas, mentirosas, e em relação a eventuais danos materiais e morais. Isso porque os direitos à honra, intimidade, vida privada e à própria imagem formam a proteção constitucional à dignidade da pessoa humana, salvaguardando um espaço íntimo intransponível por intromissões ilícitas externas.**
>
> **2. Na hipótese de publicação de entrevista em que o entrevistado imputa falsamente prática de crime a terceiro, a empresa jornalística somente poderá ser responsabilizada civilmente se:**
> **i) à época da divulgação, havia indícios concretos da falsidade da imputação; e**
> **ii) o veículo deixou de observar o dever de cuidado na verificação da veracidade dos fatos e na divulgação da existência de tais indícios. (Brasil, 2023).**

Sob clara influência do novo marco normativo estabelecido pela Resolução TSE n.º 23.732/2024, merece registro a decisão paradigmática do Supremo Tribunal Federal - na ocasião do julgamento dos Temas 987 (RE n.º 1.037.396/SP) e 533 (RE n.º 1.057.258/MG), ambos submetidos ao regime da Repercussão Geral que, apesar da ressalva expressa de não se aplicar diretamente ao contexto eleitoral, reconheceu a existência do dever de cuidado das plataformas digitais em situações de circulação massiva de conteúdos ilícitos graves, incluindo a prática de atos antidemocráticos, atos de terrorismo e incitação à discriminação (Brasil, 2025).

No que se refere à adoção do dever de cuidado pelas plataformas digitais, autores como Lorna Woods e William Perrin defendem que redes sociais e serviços de mensageria devem assumir uma responsabilidade proativa na mitigação de riscos relevantes capazes de afetar usuários e a sociedade em geral. Essa concepção se ancora no princípio da precaução, que busca conciliar a inovação tecnológica com a prevenção de danos potenciais, impondo às plataformas a obrigação de agir sempre que existam indícios razoáveis de prejuízos possíveis (Woods; Perrin, 2019).

Como anota Ana Frazão, "o conteúdo do dever de cuidado não pode ser feita em abstrato, devendo ser densificada a partir de critérios como a previsibilidade do risco, a gravidade do dano, a profissionalidade e o porte do agente econômico" (Frazão, 2021, p. 10). Quando se trata da integridade do processo eleitoral e da preservação do regime democrático, considerando a tutela ampla e específica assegurada pelo ordenamento jurídico, o dever de cuidado assume caráter especialmente rigoroso e exigente. Tal exigência se manifesta, sobretudo, sob o viés preventivo, impondo ao agente econômico a obrigação de agir para evitar a ocorrência ou a propagação de danos, ainda que estes derivem de conteúdos publicados por terceiros.

1.3 O ART. 9º-D DA RESOLUÇÃO TSE 23.610/2023: UMA LÓGICA REGULATÓRIA PAUTADA NA PREVENÇÃO

O art. 9º-D da Resolução TSE n.º 23.610/2019 impõe aos provedores de aplicação de internet a adoção e a publicização de medidas destinadas a impedir ou mitigar a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam comprometer a integridade do processo eleitoral. Esse dever envolve a implementação de medidas técnicas e administrativas voltadas a prevenir o impulsionamento de propaganda político-eleitoral irregular, com especial atenção aos casos relacionados à disseminação de desinformação.

Com efeito, "só se pode prevenir aquilo que é previsto" (Menke; Goulart, 2021, p. 348). Nesse sentido, o princípio da prevenção não se aplica indiscriminadamente a qualquer situação de risco, mas se ancora na existência de indícios científicos razoáveis sobre o impacto de determinada atividade no contexto eleitoral.

Nos termos do dispositivo, os incisos I e II consagram, respectivamente, os deveres de elaboração de termos de uso e políticas internas de conteúdo, bem como a implementação de instrumentos eficazes de notificação e de canais de denúncia, acessíveis tanto aos usuários quanto a instituições e entidades públicas e privadas.

Os termos de uso e políticas de conteúdo devem informar de forma inequívoca os usuários sobre regras aplicáveis ao conteúdo político-eleitoral, assegurando que haja mecanismos internos de monitoramento capazes de aferir o cumprimento dessas normas pelas próprias plataformas, fortalecendo a governança interna e a responsabilização corporativa.

Os canais de denúncia devem ser intuitivos, de fácil acesso e utilização, e incluir meios de comunicação dedicados à Justiça Eleitoral e demais instituições relevantes. Deve existir um fluxo de trabalho estruturado após a recepção de denúncias, com prazos claros de análise, retorno ao denunciante e registro das ações corretivas adotadas. A eficácia desses canais precisa ser auditável, considerando volume de denúncias, tempo de resposta e medidas implementadas, fortalecendo o engajamento do usuário e da comunidade científica como pressupostos para uma participação informada.

Já o inciso III estabelece o dever de planejamento e execução de ações corretivas e preventivas, incluindo o aprimoramento dos sistemas de recomendação de conteúdo, essenciais para conter a viralização de desinformação. Assim, as plataformas não se limitam a reagir a denúncias, devendo assumir postura proativa na prevenção da disseminação de conteúdos manipulados ou enganosos (Junquilho et al., 2024). As plataformas devem implementar métricas e indicadores que permitam medir o cumprimento dos deveres de prevenção, identificar ações preventivas efetivamente aplicadas e adotar medidas corretivas quando conteúdos desinformativos viralizam. É imprescindível a demonstração de um plano de ação proativo, que não se limite à reação a incidentes, mas que articule estratégias antecipatórias frente aos riscos sistêmicos da desinformação eleitoral.

O inciso IV dispõe sobre a transparência e a prestação de contas, exigindo que os provedores divulguem publicamente os resultados de suas ações de moderação. Trata-se de medida crucial para responsabilizar as plataformas quanto à eficácia de suas políticas e ferramentas de controle, sendo a transparência um vetor central para que os usuários possam avaliar a efetividade das iniciativas

adotadas contra a desinformação e para permitir um controle social robusto sobre a atuação desses agentes. As plataformas devem publicar relatórios detalhados de transparência, com periodicidade definida, evidenciando as ações realizadas e seus resultados. Esses relatórios devem incluir métricas verificáveis, como volume de conteúdo removido, alcance reduzido, número de contas sancionadas, e permitir auditoria independente, garantindo *accountability* e confiança pública.

O inciso V impõe aos provedores, em ano eleitoral, a elaboração de avaliação de impacto de seus serviços sobre a integridade do processo eleitoral, com vistas à implementação de medidas eficazes e proporcionais para mitigar os riscos identificados, incluindo aqueles relacionados à violência política de gênero. Os relatórios de impacto devem conter informações mínimas sobre os riscos identificados e as medidas de mitigação adotadas, seguindo metodologias robustas e reconhecidas, capazes de abarcar os riscos sistêmicos relevantes ao contexto brasileiro. A adequação e proporcionalidade das medidas devem ser avaliadas à luz da gravidade, escala e complexidade dos riscos identificados, assegurando que as intervenções sejam eficazes e socialmente legítimas.

Em função do avanço contínuo das técnicas de manipulação de conteúdo e do risco de sua disseminação em larga escala, o inciso VI prevê a obrigação de aprimoramento das capacidades tecnológicas e operacionais das plataformas, priorizando ferramentas e funcionalidades que contribuam para o enfrentamento dessas ameaças. A plataforma deve investir continuamente em tecnologia, incluindo inteligência artificial para detecção de deepfakes e comportamentos coordenados inautênticos, e em equipes capacitadas, com treinamento específico sobre o contexto eleitoral brasileiro. Ferramentas adicionais devem ser disponibilizadas aos usuários para aumentar seu controle sobre o conteúdo consumido, demonstrando um compromisso contínuo com o aprimoramento das capacidades operacionais frente a novas ameaças.

O § 1º do art. 9º-D veda ao provedor de aplicação a comercialização ou disponibilização de serviços de impulsionamento de conteúdo, em qualquer modalidade, inclusive mediante priorização nos resultados de busca, quando destinados à veiculação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam comprometer a integridade do processo eleitoral.

De forma análoga, o § 2º do mesmo dispositivo impõe aos provedores a adoção de medidas imediatas e eficazes para interromper o impulsionamento, a monetização e o acesso a conteúdos que contenham fatos notoriamente inverídicos ou gravemente descontextualizados, capazes de comprometer a integridade do pleito. O dispositivo estabelece, ainda, a necessidade de instauração de apuração interna dos fatos, bem como de análise dos perfis e contas envolvidos, de modo a prevenir a nova circulação do conteúdo e a inibir condutas ilícitas, inclusive mediante a indisponibilização dos serviços de impulsionamento ou monetização. Destaca-se, nesse sentido, que tais medidas devem ser implementadas independentemente de decisão judicial, refletindo o papel ativo que se exige das plataformas na prevenção e no enfrentamento da desinformação (Junquilho et al., 2024).

Para cumprir esse objetivo, o provedor deve impedir que o serviço de impulsionamento seja utilizado para disseminação de desinformação, adotando medidas imediatas para cessar monetização, circulação e acesso de conteúdos ilícitos, bem como identificar responsáveis para prevenir reincidência. A plataforma deve estar tecnicamente apta a veicular conteúdo corretivo com alcance equivalente ao da desinformação anterior, adotando providências proativas, sem depender de ordem judicial, e garantindo revisão eficaz de anúncios, com mecanismos de monitoramento capazes de avaliar seu desempenho preventivo.

Quanto às medidas previstas no art. 9º-D, o Tribunal não se limitou a exigir a sua adoção, mas determinou também a efetiva publicização das ações, alinhando-se ao conceito contemporâneo de *accountability*. Ademais, nos termos do § 4º do art. 28, as plataformas que ofereçam o serviço de impulsionamento de conteúdo eleitoral devem manter canal de comunicação com seus usuários, valorizando a participação do eleitorado na fiscalização do cumprimento da legislação eleitoral.

Por fim, com o objetivo de prevenir o impulsionamento de propaganda eleitoral em desconformidade com as diretrizes do TSE, o § 6º do art. 29 impõe aos provedores a adoção de medidas técnicas para assegurar que as pessoas contratantes insiram os dados de identificação do responsável pelo impulsionamento, por meio de mecanismos de transparência específicos ou de livre inserção, desde que respeitados os requisitos contratuais de cada provedor. Dessa forma, busca-se não apenas viabilizar o cumprimento do dever de identificação, mas também fortalecer a transparência e a fiscalização da veiculação da propaganda eleitoral nas plataformas.

O provedor deve impedir que o serviço de impulsionamento seja utilizado para disseminação de desinformação, adotando medidas imediatas para cessar monetização, circulação e acesso de conteúdos ilícitos, bem como identificar responsáveis para prevenir reincidência. A plataforma deve estar tecnicamente apta a veicular conteúdo corretivo com alcance equivalente ao da desinformação anterior, adotando providências proativas, sem depender de ordem judicial, e garantindo revisão eficaz de anúncios, com mecanismos de monitoramento capazes de avaliar seu desempenho preventivo.

1.4 A ESCOLHA DO *BENCHMARKING* REGULATÓRIO

O presente relatório adotou três jurisdições estrangeiras centrais como referência para o *benchmarking* regulatório aplicado aos distintos aspectos da Resolução TSE nº 23.610/2019: União Europeia (UE), Reino Unido (RU) e Índia. A seleção desses ordenamentos decorre da robustez e da reconhecida influência de seus marcos normativos, bem como da utilidade que oferecem para a construção de parâmetros comparativos adequados à realidade brasileira, especialmente no contexto do Sul Global.

A opção metodológica privilegiou modelos regulatórios sólidos e dotados de capacidade efetiva de irradiação internacional.

União Europeia (UE) - *Digital Services Act* (DSA): O DSA estabelece um quadro regulatório horizontal e escalonado, com obrigações reforçadas para plataformas de muito grande porte, hoje referência global. Trata-se do benchmark mais direto para a análise do art. 9º-D, I, da Resolução TSE nº 23.732/2024, ao exigir que termos, políticas e procedimentos internos sejam compatíveis com a integridade informacional do processo eleitoral - compreensíveis, previsíveis e verificáveis. O modelo europeu, de modo geral, evita restringir conteúdos políticos, concentrando-se na mitigação da opacidade e dos riscos sistêmicos associados às plataformas digitais (Brasil, 2024; União Europeia, 2022).

Reino Unido – *Online Safety Act* (OSA): O OSA aprofunda o enfoque na safety by design e na governança regulatória exercida pela Ofcom (a agência reguladora das tele comunicações no Reino Unido), conferindo centralidade aos fluxos de reclamação e aos mecanismos de transparência. O diploma consolida deveres de cuidado, avaliações de risco e obrigações estruturadas de prestação de contas, compondo um sistema de enfor cement graduado que admite sanções de até 10% do faturamento global das plataformas (Reino Unido, 2023).

Índia – *IT Rules* 2021: A incorporação do modelo indiano - relevante representante do Sul Global - permite aproximar o *benchmarking* de realidades socioeconômicas mais próximas da brasileira. Cumpre registrar que, em 2024, assim como o Brasil, a Índia foi classificada como flawed democracy (democracia falha) no "Democracy Index", publicado pela The Economist, indicador que avalia a qualidade democrática em 167 países, o que reforça a pertinência comparativa da experiência regulatória analisada. A regulamentação combina exigências de clareza textual, celeridade decisória, mecanismos periódicos de transparência e responsabilização pública, aproximando-se estruturalmente do modelo normativo brasileiro (Economist Intelligence Unit, 2024; Índia, 2021).

Em síntese, a seleção das jurisdições buscou construir um diálogo regulatório capaz de conciliar o rigor e a abrangência dos modelos ocidentais avançados com a pertinência e afinidade operacional de uma experiência relevante do Sul Global, produzindo parâmetros mais equilibrados e ajustados às especificidades do ecossistema digital brasileiro.

1.5 APRIMORAMENTO DA RESOLUÇÃO DO TSE Nº 23.610/2019 E FORTALECIMENTO DA CAPACIDADE INSTITUCIONAL DO TRIBUNAL

Um dos principais desafios contemporâneos para a integridade da informação no contexto eleitoral não reside apenas na formulação de novas normas, mas sobretudo na capacidade institucional de implementá-las e assegurar seu efetivo cumprimento. Nesse cenário, o Tribunal Superior Eleitoral (TSE), embora não constitua um regulador digital em sentido estrito, tem assumido progres-

sivamente um papel central na supervisão das dinâmicas informacionais mediadas por plataformas digitais, em razão de sua responsabilidade constitucional de garantir a normalidade e a legitimidade do processo eleitoral.

A crescente centralidade das plataformas digitais e de sistemas de inteligência artificial na organização do debate público impõe desafios regulatórios que transcendem a lógica tradicional de fiscalização baseada exclusivamente em intervenções pontuais, como a remoção de conteúdos específicos. A experiência recente evidencia que um modelo reativo é insuficiente para enfrentar riscos sistêmicos associados à circulação massiva de desinformação, à opacidade de mecanismos de recomendação e à exploração econômica de conteúdos ilícitos ou irregulares em contextos eleitorais. Nesse ambiente, torna-se necessário fortalecer não apenas o conteúdo normativo existente, mas, sobretudo, os instrumentos institucionais que permitam sua implementação contínua, auditável e eficaz.

Este relatório apresenta, nesse contexto, um conjunto de propostas voltadas ao aprimoramento da Resolução TSE nº 23.610/2019 e ao fortalecimento da capacidade institucional do Tribunal de acompanhar e promover o cumprimento das obrigações já estabelecidas no ordenamento eleitoral por plataformas digitais e empresas de inteligência artificial. As recomendações aqui formuladas partem de uma premissa central: não se trata apenas de criar novas obrigações materiais, mas de dotar a Justiça Eleitoral de instrumentos adequados para acompanhar, de forma sistemática e preventiva, o cumprimento das regras já vigentes, com base em estruturas institucionais existentes.

Com esse objetivo, recomenda-se, ao final do relatório, a criação de obrigações para as empresas de IA, a melhoria das normas sobre *deepfakes*, bem como a inserção de dispositivo específico nas Disposições Finais da Resolução, voltado à instituição de um instrumento de conformidade eleitoral estruturado sob lógica de corregulação. Como demonstrado ao longo do relatório, esse mecanismo consolida, em caráter transversal e sistemático, deveres de diligência já previstos na Resolução, traduzindo-os em compromissos procedimentais verificáveis e auditáveis. O plano de conformidade eleitoral previsto no dispositivo permitirá que provedores explicitem, de modo transparente, as medidas adotadas para assegurar o cumprimento das obrigações constantes na Resolução, preservando sua autonomia técnica na definição de soluções operacionais, ao mesmo tempo em que viabiliza acompanhamento contínuo, avaliação de resultados e supervisão institucional.

A atribuição conferida à Corregedoria-Geral Eleitoral nesse contexto harmoniza-se diretamente com suas competências já estabelecidas, em especial aquelas previstas na Resolução TSE nº 23.742/2024, que lhe confere a condução de procedimentos administrativos voltados à elucidação de fatos que possam representar risco à normalidade, à legitimidade e à isonomia do pleito. Ao centralizar nessa instância a avaliação e o acompanhamento dos planos de conformidade, o modelo proposto aproveita uma estrutura institucional vocacionada à fiscalização técnica e preventiva, capaz de monitorar riscos sistêmicos e assegurar a aplicação uniforme das normas eleitorais.

O desenho proposto adota abordagem estruturada, proporcional e baseada em risco, combinando previsibilidade regulatória, flexibilidade operacional e transparência pública. Ao articular mecanismos de supervisão responsiva, critérios objetivos de conformidade e incentivos institucionais associados a regimes já existentes de credenciamento e cadastro, o arranjo aproxima a Justiça Eleitoral de práticas consolidadas de supervisão adotadas por outros órgãos reguladores, fortalecendo uma governança preventiva, auditável e compatível com a complexidade do ambiente digital contemporâneo.

Ao apresentar estas recomendações, os coordenadores deste relatório esperam contribuir de forma construtiva para o debate público sobre os desafios contemporâneos de preservação da integridade da informação no ambiente digital. O fortalecimento da capacidade institucional das autoridades eleitorais para implementar e acompanhar o cumprimento das normas vigentes constitui elemento essencial para a proteção da legitimidade do processo eleitoral. Ao mesmo tempo, a construção de mecanismos transparentes, proporcionais e auditáveis de supervisão contribui para ampliar a confiança pública e fomentar a participação responsável de todos os atores envolvidos (instituições, plataformas e sociedade civil) na promoção de um ambiente informacional saudável. Trata-se, em última instância, de reforçar as condições que sustentam a integridade das eleições, fundamento e alicerce do Estado Democrático de Direito no Brasil.

1.6. A EVOLUÇÃO LEGISLATIVA DA REGULAÇÃO DA PROPAGANDA ELEITORAL NA INTERNET NA LEI 9.504/1997 (2017–2025)

Marilda de Paula Silveira

A disciplina da propaganda eleitoral na internet, concentrada principalmente nos arts. 57-A a 57-J da Lei nº 9.504/1997, foi introduzida originalmente pela Lei nº 12.034/2009. A partir de 2017, contudo, observa-se uma nova fase de evolução legislativa, marcada menos pela criação de novos dispositivos e mais pelo ajuste do modelo normativo existente, em resposta à centralidade das plataformas digitais no debate público e no processo eleitoral.

A Lei nº 13.488, de 6 de outubro de 2017, constitui o marco legislativo fundamental da regulação da propaganda eleitoral na internet no Brasil. Diferentemente de alterações posteriores, que operaram ajustes pontuais ou densificações infralegais, essa lei promoveu uma reformulação estrutural dos arts. 57-A a 57-J da Lei nº 9.504/1997, ao reconhecer explicitamente o ambiente digital como espaço legítimo de propaganda eleitoral e ao introduzir, pela primeira vez, o impulsionamento de conteúdos como categoria jurídica própria no direito eleitoral.

Ao dar nova redação ao art. 57-B, o legislador passou a admitir expressamente a propaganda eleitoral *"por meio de blogs, redes sociais, sítios de mensagens instantâneas e aplicações de internet assemelhadas"*, afastando qualquer dúvida quanto à licitude da atuação eleitoral em plataformas digitais. Esse reconhecimento, contudo, não foi irrestrito. Desde a origem, a lei estabeleceu uma distinção central entre a circulação orgânica de conteúdos e a amplificação artificial de alcance.

Enquanto a manifestação espontânea de pessoas naturais foi admitida, o uso de mecanismos de impulsionamento passou a ser reservado exclusivamente a candidatos, partidos e coligações, vedada a contratação por terceiros estranhos à disputa.

Essa lógica é aprofundada no art. 57-C, que consagra uma regra geral de vedação à propaganda eleitoral paga na internet, admitindo como única exceção o impulsionamento de conteúdos. O impulsionamento é, assim, positivamente definido como forma excepcional de propaganda eleitoral remunerada, condicionada a requisitos cumulativos de transparência, autoria e territorialidade: identificação inequívoca do conteúdo como propaganda, contratação exclusiva por atores eleitorais legitimados e vínculo com provedor de aplicação com sede ou representação no País. Com essa arquitetura normativa, o legislador buscou conciliar o reconhecimento da centralidade das plataformas digitais na disputa política com a necessidade de conter assimetrias econômicas e manipulações artificiais do debate público.

A Lei nº 13.488/2017 não se limitou a autorizar o impulsionamento. Ela também instituiu vedações explícitas a práticas de manipulação digital, inclusive aquelas que prescindem de pagamento. O § 3º do art. 57-B proibiu o uso de *"ferramentas digitais não disponibilizadas pelo provedor da aplicação de internet, ainda que gratuitas, para alterar o teor ou a repercussão de propaganda eleitoral",* antecipando preocupações posteriores com o uso de automações, bots e outros mecanismos artificiais de amplificação. Do mesmo modo, vedou-se o falseamento de identidade no cadastro de usuários, reforçando a exigência de autenticidade e responsabilização no ambiente digital.

No plano institucional, a lei conferiu à Justiça Eleitoral poderes expressos de intervenção sobre conteúdos digitais. O art. 57-I autorizou a suspensão do acesso a conteúdos que descumpram a legislação eleitoral, *"no âmbito e nos limites técnicos de cada aplicação de internet",* mediante decisão judicial proporcional à gravidade da infração. Esse dispositivo evidencia que, desde 2017, a propaganda eleitoral na internet passou a ser compreendida como atividade sujeita a controle jurisdicional específico, compatível com a natureza técnica das plataformas e com a necessidade de proteção da normalidade do pleito.

O modelo legal é completado pelo art. 57-J, que atribuiu ao Tribunal Superior Eleitoral o dever de regulamentar os arts. 57-A a 57-I *"de acordo com o cenário e as ferramentas tecnológicas existentes em cada momento eleitoral"*, bem como de promover regras de boas práticas para campanhas na internet. Esse dispositivo é decisivo para compreender a evolução normativa subsequente: o legislador optou por combinar regras substantivas claras na lei com uma delegação normativa expressa e condicionada ao TSE, reconhecendo a impossibilidade de o texto legal acompanhar, por si só, a velocidade das inovações tecnológicas.

Ainda no âmbito da Lei nº 13.488/2017, a alteração do art. 58, § 3º, IV, introduziu um princípio de simetria comunicacional no exercício do direito de resposta em ambiente digital. Determinou-se que, quando a ofensa tiver sido impulsionada, a resposta deverá ser divulgada com o mesmo impulsionamento, veículo e destaque, neutralizando o alcance artificial previamente contratado. Com isso, o legislador reconheceu que, no ambiente digital, a intensidade do dano comunicacional está diretamente relacionada aos mecanismos de amplificação utilizados.

Esse conjunto normativo demonstra que o impulsionamento de conteúdos não surge como simples técnica de marketing eleitoral, mas como elemento central de um regime jurídico voltado à preservação da igualdade de oportunidades entre candidatos, à transparência da comunicação política e à integridade do processo eleitoral. As leis posteriores não criaram esse regime, mas passaram a operar sobre a base estruturada em 2017, seja por ajustes legislativos pontuais, seja — sobretudo — pela densificação infralegal promovida pelas resoluções do Tribunal Superior Eleitoral, em cumprimento ao mandato expresso do art. 57-J da Lei nº 9.504/1997.

1.6.1 AS REFORMAS DE 2021 E A CONSOLIDAÇÃO DE UMA LEITURA MATERIAL DA PROPAGANDA DIGITAL

O ano de 2021 foi marcado por um conjunto amplo de reformas eleitorais, entre as quais se destacam as Leis nº 14.192, nº 14.208 e nº 14.211. Do ponto de vista estritamente legislativo, essas normas não promoveram uma reescrita dos arts. 57-A a 57-J, mas produziram efeitos relevantes sobre sua interpretação e alcance.

A Lei nº 14.192/2021, ao instituir normas para prevenir, reprimir e combater a violência política contra a mulher, não alterou diretamente a estrutura normativa da propaganda na internet, mas introduziu novos parâmetros materiais que passaram a incidir sobre a atividade de comunicação política, inclusive no ambiente digital. A propaganda eleitoral deixa de ser analisada apenas sob a ótica formal (meios, autoria e temporalidade) e passa a ser também avaliada quanto ao seu conteúdo discriminatório, intimidatório ou excludente.

Já as Leis nº 14.208/2021 e nº 14.211/2021, voltadas à criação da federação partidária e à disciplina do financiamento de campanhas, tampouco modificaram diretamente os dispositivos sobre propaganda digital. Contudo, ao reorganizarem a estrutura dos atores eleitorais e o regime de financiamento, reforçaram o papel da propaganda na internet como principal canal de visibilidade eleitoral, intensificando a centralidade prática dos arts. 57 e seguintes da Lei nº 9.504/1997.

Desde 2021 até o presente momento, não houve alterações legislativas estruturais no texto

da Lei nº 9.504/1997 especificamente voltadas à propaganda eleitoral na internet. Os arts. 57-A a 57-J permanecem, em sua essência, com a mesma arquitetura normativa.

Essa estabilidade textual, contudo, não significa estagnação normativa. Ao contrário, o legislador optou por **preservar um modelo aberto e principiológico**, capaz de acomodar transformações tecnológicas sem sucessivas reformas legais. A regulação direta de fenômenos como redes sociais, plataformas digitais, automação de conteúdos e inteligência artificial foi deliberadamente deslocada para o plano infralegal, especialmente para a atuação da Justiça Eleitoral.

O resultado é um modelo legal estável no texto, mas dinâmico na aplicação, no qual a lei fixa as balizas estruturais e delega à Justiça Eleitoral a tarefa de concretizar, detalhar e atualizar a regulação da propaganda na internet — tema que será aprofundado, como você indicou, na análise das resoluções do TSE.

Assim, no período mais recente, a Lei nº 9.504/1997 mantém-se como marco geral da propaganda eleitoral digital que é regulada pelas resoluções do TSE, nos termos do art. 57-J.

1.6.2 EVOLUÇÃO DAS RESOLUÇÕES DO TSE SOBRE PROPAGANDA NA INTERNET A PARTIR DA RES.-TSE Nº 23.610/2019

Este relatório adota como recorte analítico a Resolução TSE nº 23.610/2019 por se tratar do primeiro ato normativo infralegal do Tribunal Superior Eleitoral que sistematiza, de forma unitária e detalhada, a disciplina da propaganda eleitoral, incluindo um capítulo próprio dedicado à propaganda na internet, em consonância com o mandato normativo conferido pelo art. 57-J da Lei nº 9.504/1997.

Embora resoluções anteriores tenham tratado pontualmente de aspectos da propaganda eleitoral em pleitos específicos, a Res.-TSE nº 23.610/2019 inaugura um modelo regulatório estável, de aplicação geral e vocação permanente, que passa a servir de matriz para as alterações posteriores e para a consolidação de conceitos, deveres e procedimentos relativos ao ambiente digital. Assim, o exame concentrado a partir dessa resolução permite uma análise mais coerente, comparável e cumulativa da evolução normativa do TSE, sem prejuízo do reconhecimento de que seu conteúdo se ancora nas inovações legislativas introduzidas pela Lei nº 13.488/2017.

A Resolução TSE nº 23.610, de 18 de dezembro de 2019, foi editada para *"dispor sobre propaganda eleitoral"* e, no seu texto, estruturou um capítulo próprio para a matéria digital *("DA PROPAGANDA ELEITORAL NA INTERNET")*, estabelecendo o ponto de partida regulatório do Tribunal para a comunicação eleitoral em ambiente online.

Na disciplina original, a resolução organiza a regulação digital em três eixos normativos, que se tornariam estruturantes nas versões posteriores:

(i) delimitação do espaço e do sujeito legitimado para a propaganda digital: a arquitetura normativa concentra a propaganda online em ambientes identificáveis e vinculados às campanhas, com deveres de comunicação de endereços eletrônicos à Justiça Eleitoral (em linhas que, posteriormente, seriam densificadas).

(ii) impulsionamento de conteúdo, com requisitos de transparência e restrições: a resolução trata do impulsionamento como modalidade específica, exigindo contratação direta com provedor com representação no país e restringindo a finalidade a promover/beneficiar candidaturas e agremiações, "vedada a realização de propaganda negativa". Determina ainda que "todo impulsionamento" contenha identificação (CNPJ/CPF) e a expressão "Propaganda Eleitoral".

(iii) mensagens eletrônicas e instantâneas, com lógica de consentimento/descadastramento e tutela de dados: disciplina mensagens eletrônicas e instantâneas enviadas por campanhas, impondo identificação da pessoa remetente e "mecanismo que permita ... descadastramento e eliminação dos ... dados pessoais", com prazo de 48 horas para atendimento.

Esse tripé (período e escopo; impulsionamento; mensagens/dados) é o núcleo da primeira vigência no tema internet e orienta a evolução posterior: as mudanças, em vez de romperem com o modelo, incrementam densidade regulatória sobretudo em impulsionamento, mensageria, transparência e integridade informacional.

Já em 2020, por conta da Emenda Constitucional nº 107/2020, o TSE editou a Res.-TSE nº 23.624/2020, que não redesenhou a disciplina material da propaganda digital, mas promoveu ajustes temporais para aplicação exclusiva às Eleições 2020 adiadas em razão da pandemia de COVID. No tocante à internet, a resolução explicitamente ajusta o início: *"é permitida a propaganda eleitoral na internet a partir de 27 de setembro de 2020",* como adaptação do caput do art. 27 da Res.-TSE nº 23.610/2019.

O significado regulatório desse ato, no tema específico, é metodologicamente importante: ele evidencia que, no primeiro ciclo de aplicação, a preocupação central do TSE foi compatibilizar o calendário do capítulo digital com o novo cronograma eleitoral, sem modificar o desenho normativo de fundo.

Para o ciclo de 2022, contudo, o cenário digital já havia se alterado e exigiu mudanças relacionadas à densificação de pré-campanha, definições operacionais e integração com proteção de dados. A Resolução TSE nº 23.671, de 14 de dezembro de 2021, altera a Res.-TSE nº 23.610/2019 e representa um passo de densificação relevante, especialmente por três movimentos normativos verificáveis no texto:

Em **primeiro lugar,** temos a tipificação mais direta do ilícito de propaganda antecipada e extensão do impulsionamento à pré-campanha. A resolução passa a explicitar, por exemplo, que "considera-se propaganda antecipada passível de multa aquela com *"pedido explícito de voto"* ou que utilize meio proscrito. E, de modo diretamente conectado ao ambiente digital, prevê que *"o impulsionamento de conteúdo político-eleitoral … também será permitido durante a pré-campanha",* desde que sem pedido explícito e com moderação de gastos.

Em **segundo lugar**, a criação de linguagem regulatória própria para mensageria e circulação em larga escala. No conjunto de definições, a Res.-TSE nº 23.671/2021 incorpora no texto o conceito de "disparo em massa" como *"envio, compartilhamento ou encaminhamento de um mesmo conteúdo … para um grande volume de usuárias e usuários por meio de aplicativos de mensagem instantânea".* Esse ponto é decisivo porque fornece uma categoria operacional para o controle de práticas digitais, que passa a orientar articulação entre propaganda, mensageria e ilícitos de campanha.

Em **terceiro lugar,** o reforço de transparência/tecnicidade do impulsionamento e obrigações informativas ligadas a dados pessoais. A alteração inclui mecanismos de transparência do impulsionamento (por exemplo, solução para identificação do CNPJ e regras para manutenção da identificação em compartilhamentos/encaminhamentos). Além disso, insere regra segundo a qual provedores devem informar usuárias/os usuários sobre a possibilidade de tratamento de dados para veiculação de propaganda eleitoral, "no âmbito e nos limites técnicos" de cada provedor.

Em síntese, o conjunto de 2021 consolida uma transição: o texto passa a operar não apenas com proibições/autorizações abstratas, mas com conceitos e deveres que dialogam com práticas concretas de distribuição digital (impulsionamento e mensageria) e com o vocabulário de proteção de dados.

1.6.3 ALTERAÇÕES DE 2024 (RES.-TSE Nº 23.732/2024): PASSAGEM PARA UM MODELO DE GOVERNANÇA INFORMACIONAL, TRANSPARÊNCIA ESTRUTURAL E DISCIPLINA EXPLÍCITA DE IA E *DEEPFAKES*

As alterações introduzidas pela Res.-TSE nº 23.732/2024 na Res.-TSE nº 23.610/2019 representam uma mudança de densidade e de técnica regulatória no tratamento da propaganda na internet. Se, na matriz de 2019 (e mesmo nas alterações de 2021), o eixo predominante era a combinação entre período, regras de impulsionamento e limites para mensageria, a reforma de 2024 amplia significativamente o escopo ao inserir um conjunto articulado de deveres dirigidos a candidaturas/agremiações, provedores de aplicação e, sobretudo, ao ecossistema de circulação (recomendação algorítmica, publicidade segmentada, repositórios de anúncios, repositórios de decisões e medidas de mitigação de risco).

A Res.-TSE nº 23.732/2024 renomeia o capítulo pertinente como *"Dos Conteúdos Político-Eleitorais e da Propaganda Eleitoral na Internet"*, sinalizando, desde o plano estrutural, que a regu-

lação passa a abranger não apenas propaganda eleitoral stricto sensu, mas também a circulação de conteúdos político-eleitorais em sentido mais amplo.

Essa mudança é acompanhada por dispositivos que explicitam que a veiculação de conteúdo político-eleitoral fora do período estrito de campanha submete-se a regras de transparência e ao regime de tecnologias digitais (IA/conteúdo sintético), *"no que couber"*, alcançando provedores e responsáveis pela criação/divulgação.

Do ponto de vista teórico, a literatura recente tem observado que a propaganda digital contemporânea se caracteriza por estratégias baseadas em dados, segmentação e amplificação, com potencial de assimetria e manipulação da vontade do eleitorado; a alteração de 2024 se aproxima desse diagnóstico ao deslocar parte da regulação para instrumentos de rastreabilidade e mitigação de riscos do ambiente informacional.

A inovação mais marcante em transparência está no art. 27-A, dirigido diretamente ao provedor de aplicação que preste serviço de impulsionamento, inclusive por priorização de resultado de busca. O dispositivo impõe (i) manutenção de repositório de anúncios, com acompanhamento em tempo real do conteúdo, valores, responsáveis pelo pagamento e características dos grupos populacionais que compõem a audiência (perfilamento); e (ii) disponibilização de ferramenta de consulta com busca avançada e (iii) possibilidade de coletas sistemáticas via API de dados de anúncios (conteúdo, gasto, alcance, público atingido e pagadores).

Há dois aspectos metodologicamente relevantes aqui: a) Definição normativa ampla de *"conteúdo político-eleitoral", "independente da classificação feita pela plataforma"*, incluindo matérias relacionadas ao processo eleitoral, propostas, projetos de lei e exercício de direitos políticos; b) caráter permanente das obrigações, inclusive em anos não eleitorais e períodos pré e pós-eleições, além de vincular o cumprimento do art. 27-A ao credenciamento do provedor para prestar serviço de impulsionamento.

Essa engenharia aproxima a resolução de um modelo de *accountability* e auditoria pública da publicidade política, ao criar condições para monitoramento por Justiça Eleitoral, pesquisadores e sociedade. A literatura institucional (incluindo materiais de acompanhamento produzidos por centros acadêmicos[1]) tem destacado que a atuação do TSE em desinformação e propaganda digital evoluiu para mecanismos de transparência e uniformização de aplicação normativa.

Além disso, a Res.-TSE nº 23.732/2024 introduz, de forma explícita, um regime de conteúdo sintético multimídia gerado por IA (art. 9º-B) e um regime proibitivo de conteúdos fabricados/manipulados com potencial lesivo ao processo eleitoral (art. 9º-C).

No art. 9º-B, a regra central é o dever de informar, de modo explícito, destacado e acessível, que o conteúdo *"foi fabricado ou manipulado e a tecnologia utilizada"*, com requisitos de apresentação conforme o formato (áudio; marca d'água e audiodescrição em imagem; requisitos cumulativos em vídeo; e indicação em material impresso).

O mesmo artigo prevê exceções para ajustes de qualidade e elementos usuais de identidade visual/marketing, mas disciplina de modo relevante o uso de chatbots/avatares como mediação da comunicação de campanha: admite-se o uso sob o regime do caput, porém é *"vedada qualquer simulação de interlocução com a pessoa candidata ou outra pessoa real"*. E o descumprimento pode implicar remoção imediata do conteúdo ou indisponibilidade do serviço.

No art. 9º-C, a resolução veda o uso de conteúdo fabricado/manipulado para difundir fatos notoriamente inverídicos ou descontextualizados com potencial de dano ao equilíbrio do pleito ou à integridade do processo eleitoral; e, em seu §1º, estabelece proibição expressa de *deepfake* (áudio/vídeo) para favorecer ou prejudicar candidatura, ainda que haja autorização, quando houver criação/substituição/alteração de imagem ou voz de pessoa viva, falecida ou fictícia.

O §2º densifica as consequências: o descumprimento configura abuso do poder político e uso indevido dos meios de comunicação social, com cassação do registro ou do mandato, e remete à apuração de responsabilidades.

A relevância desse bloco é dupla: (i) introduz um regime de transparência obrigatória para IA (rotulagem) e (ii) cria um regime de ilicitude qualificada (*deepfake* + desinformação notória com potencial lesivo), com consequência eleitoral severa (cassação), o que coloca a disciplina de IA no centro do debate sobre integridade eleitoral.

Outro núcleo inovador está nos deveres impostos aos provedores de aplicação que permitam conteúdo político-eleitoral. O art. 9º-D, como visto, estabelece como dever do provedor adotar e publicizar medidas para impedir ou diminuir a circulação de *"fatos notoriamente inverídicos ou gravemente descontextualizados"* que possam atingir a integridade do processo eleitoral, listando medidas como: termos de uso/políticas de conteúdo, canais de denúncia, ações corretivas/preventivas (incluindo aprimoramento de sistemas de recomendação), transparência de resultados, e avaliação de impacto em ano eleitoral com medidas proporcionais de mitigação de riscos, inclusive quanto à violência política de gênero.

O mesmo dispositivo veda a disponibilização de impulsionamento para veicular conteúdo notoriamente inverídico ou gravemente descontextualizado que possa atingir a integridade do processo eleitoral, impõe providências imediatas para cessar impulsionamento/monetização/acesso e prevê, inclusive, a possibilidade de a Justiça Eleitoral determinar veiculação de conteúdo informativo corretivo *"por impulsionamento e sem custos"*, no mesmo alcance do conteúdo irregular.

ESSE PONTO É O QUE MAIS MOBILIZA O DEBATE ACADÊMICO E INSTITUCIONAL.

E o §4º é particularmente relevante: afirma que essas providências decorrem da função social e do dever de cuidado e *"não dependem de notificação da autoridade judicial".*

A resolução também cria um mecanismo de governança judicial e uniformização: o art. 9º-G prevê um repositório público das decisões do TSE que determinem remoção de conteúdos que atinjam a integridade do processo eleitoral, com número do processo, íntegra da decisão e campos destacados. Além disso, determina que provedores informem o cumprimento e, quando exigido, alimentem o repositório com arquivo do conteúdo, capturas de tela de comentários, metadados (IP, data/hora) e metadados relativos ao engajamento no momento da remoção, com parte publicizada e parte sob sigilo (com rastreabilidade de acesso).

Essa engenharia se relaciona a dois objetivos: (i) padronização decisória (reduzindo respostas divergentes a conteúdos substancialmente idênticos) e (ii) produção de evidência e auditabilidade

para apuração de ilícitos e compreensão de alcance/impacto, o que dialoga com preocupações destacadas em materiais técnicos sobre desinformação e atuação normativa do TSE.

A Res.-TSE nº 23.732/2024 reforça, ainda, o papel de checagens por agências que tenham termo de cooperação, afirmando que as classificações são independentes, mas que checagens disponibilizadas no sítio da Justiça Eleitoral e outras fontes fidedignas podem servir como parâmetro para aferição de violação a dever de diligência e presteza atribuído a candidatos/partidos/federações/coligações.

Esse ponto integra o desenho normativo de 2024 ao articular *"dever de diligência"* com fontes públicas de checagem, reforçando a ideia de que a integridade eleitoral depende de deveres distribuídos entre atores (campanhas e plataformas), não apenas de sanções posteriores.

1.6.3.1 - A RESOLUÇÃO TSE Nº 23.714/2022 E O EXERCÍCIO DO PODER DE POLÍCIA

No ciclo normativo da Justiça Eleitoral brasileira, a Resolução TSE nº 23.714, de 20 de outubro de 2022, representa uma alteração específica e complementar à regulação da propaganda eleitoral na internet, pois não trata de propaganda em sentido clássico, mas disciplina medidas voltadas ao enfrentamento da desinformação que atinge a integridade do processo eleitoral.

A norma foi editada em um contexto de elevado volume de denúncias de informações falsas vinculadas às eleições gerais de 2022, o que levou o Tribunal Superior Eleitoral a adotar uma resposta normativa própria, baseada em sua competência de regulação e fiscalização do processo eleitoral.

O caput do art. 2º da Res.-TSE nº 23.714/2022 estabelece que:

> *"É vedada, nos termos do Código Eleitoral, a divulgação ou compartilhamento de fatos sabidamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos."*

Nessa redação, a norma diferencia-se das disposições sobre propaganda eleitoral tradicional (que constam da Res.-TSE nº 23.610/2019 e suas alterações) por concentrar sua disciplina sobre conteúdos que prejudicam a integridade do processo eleitoral — especialmente aqueles que não se limitam à promoção de candidatos ou partidos, mas que disseminam informações falsas ou profundamente descontextualizadas, capazes de distorcer a percepção pública sobre aspectos essenciais das eleições.

Em termos operacionais, a resolução estabelece mecanismos de remoção célere de conteúdos decisivamente prejudiciais. O art. 2º, § 1º prevê que, diante da identificação de fatos sabidamente inverídicos ou gravemente descontextualizados, o TSE poderá determinar: *"às plataformas a imediata remoção da URL, URI ou URN, sob pena de multa de R$ 100.000,00 (cem mil reais) a R$ 150.000,00 (cenquenta mil reais) por hora de descumprimento"*, contados a partir do término do segundo hora após o recebimento da notificação.

O art. 3º, por sua vez, autoriza a Presidência do TSE a estender decisão colegiada para outras URLs com conteúdo idêntico, inclusive nos casos de replicações sucessivas pelo provedor ou aplicações, sem a necessidade de novas decisões judiciais para cada reprodução do mesmo conteúdo irregular.

Essas disposições revelam que a Res.-TSE nº 23.714/2022 não se limita a coibir práticas de propaganda eleitoral tradicional, mas cria um regime de elevação do comando regulatório para situações de ameaça sistêmica à legitimidade do pleito em ambiente digital — em especial quando a informação falsa atinge a confiança no processo e nos seus instrumentos (como a votação, apuração e totalização).

A relevância dessa resolução, no entanto, também tem sido objeto de debate jurídico — inclusive no âmbito do Supremo Tribunal Federal. No julgamento da ADI nº 7.261/DF, o STF referendou a decisão que indeferiu medida cautelar contra dispositivos da Res.-TSE nº 23.714/2022, assentando que a norma não extrapola a competência normativa do TSE nem configura censura prévia generalizada, uma vez que sua aplicação é vinculada à proteção da integridade do processo eleitoral e se ancora em precedentes e atos normativos anteriores da Justiça Eleitoral voltados ao enfrentamento da desinformação no contexto das campanhas digitais.

A decisão do STF, ao validar a Res.-TSE nº 23.714/2022 em sede de controle concentrado, reconheceu que a disciplina do enfrentamento à desinformação integra a regulação constitucional e legal da justiça eleitoral sobre propaganda, comunicação e integridade do debate público. Ainda que a resolução não faça parte do núcleo tradicional de normas sobre propaganda eleitoral, ela complementa esse regime ao responder a um fenômeno que se manifesta de forma expressiva no ambiente digital e que, se não enfrentado, pode comprometer a formação da vontade do eleitorado e a igualdade de oportunidades entre os concorrentes.

Nota-se que, em 2024, a regulação do TSE deixa de se limitar ao controle de forma e ao perímetro clássico do *"conteúdo publicado"* e passa a incorporar instrumentos orientados à governança do ecossistema informacional eleitoral: transparência estruturada do impulsionamento (repositório + perfilamento + API + credenciamento), disciplina explícita de IA (rotulagem) e *deepfakes* (proibição com consequência de cassação), deveres positivos de mitigação de risco pelas plataformas (incluindo avaliação de impacto e medidas não dependentes de ordem judicial), e mecanismos de uniformização/rastreabilidade por repositório público.

1.6.4. O ART. 19 DO MARCO CIVIL DA INTERNET APÓS O RE 1.037.396: DELIMITAÇÃO DO TEMA 987 E PRESERVAÇÃO DO REGIME JURÍDICO ELEITORAL

O julgamento do Recurso Extraordinário nº 1.037.396 (Tema 987 da repercussão geral) não teve por objeto a regulação do processo eleitoral nem da propaganda eleitoral na internet. Desde a formulação da tese, o Supremo Tribunal Federal delimitou expressamente o alcance normativo da decisão, excluindo do âmbito da repercussão geral aquilo que é disciplinado pela legislação eleitoral e pelos atos normativos expedidos pela Justiça Eleitoral, em especial pelo Tribunal Superior Eleitoral.

Essa delimitação consta de forma literal e inequívoca na tese fixada pelo STF, segundo a qual:

> *"Enquanto não sobrevier nova legislação, o art. 19 do MCI deve ser interpretado de forma que os provedores de aplicação de internet estão sujeitos à responsabilização civil,* ***ressalvada a aplicação das disposições específicas da legislação eleitoral e os atos normativos expedidos pelo TSE."***

Esse trecho cumpre função dogmática central. Ao ressalvar explicitamente a legislação eleitoral e os atos normativos do TSE, o STF retira o processo eleitoral do núcleo normativo da repercussão geral, preservando-o como microssistema jurídico autônomo, dotado de princípios, finalidades e instrumentos próprios. Assim, a tese firmada no Tema 987 não se aplica automaticamente à propaganda eleitoral na internet, nem redefine os critérios de remoção de conteúdo, responsabilização de plataformas ou limites à comunicação política durante o período eleitoral.

A exclusão do regime eleitoral do âmbito da repercussão geral não significa, contudo, que o STF tenha ignorado o impacto da comunicação digital sobre as eleições. Ao contrário, o acórdão reconhece expressamente que a regulação insuficiente do ambiente digital produz efeitos que alcançam o processo político-eleitoral. Nesse sentido, o Tribunal afirma que a ausência de respostas normativas adequadas favoreceu o surgimento de: *"discursos de ódio, teorias da conspiração, atos antidemocráticos, desinformação e campanhas de notícias fraudulentas", fenômenos que, segundo o próprio acórdão, "interferem no processo político eleitoral e minam o regime democrático e suas instituições".*

Essa referência ao processo eleitoral, entretanto, possui natureza argumentativa e constitucional, e não regulatória. O STF utiliza o impacto das distorções informacionais sobre as eleições como fundamento para reconhecer a insuficiência do art. 19 do Marco Civil da Internet no regime geral, mas se abstém de disciplinar diretamente a propaganda eleitoral ou de interferir na competência normativa da Justiça Eleitoral.

Essa distinção é reforçada quando o acórdão reconhece que a circulação massiva de conteúdos ilícitos pode comprometer a formação da opinião pública, ao produzir: *"a criação de realidades paralelas, cada vez mais dissonantes da verdade factual, o que distorce a opinião pública; [e] leva à polarização e ao extremismo, ao eclipsar as posições intermediárias do espectro político"*

Ainda assim, o Tribunal opta por não subsumir o processo eleitoral ao regime geral do Marco Civil, afirmando a necessidade de respeito às normas específicas que regem a disputa eleitoral. Com isso, o STF reconhece implicitamente que a propaganda eleitoral na internet se insere em um campo jurídico no qual a liberdade de expressão é tradicionalmente compatibilizada com outros valores constitucionais, como a igualdade de oportunidades entre candidatos, a liberdade de escolha do eleitor e a normalidade e legitimidade do pleito.

Do ponto de vista normativo, portanto, o que o acórdão estabelece é uma relação de convivência entre regimes jurídicos, e não de subordinação. O Marco Civil da Internet, mesmo após o reconhecimento da inconstitucionalidade parcial e progressiva do art. 19, não se sobrepõe à legislação eleitoral. Ao contrário, a decisão do STF afirma que, em matéria eleitoral, prevalecem as disposições específicas da Lei nº 9.504/1997 e os atos normativos do TSE, que permanecem como parâmetros centrais para a regulação da propaganda eleitoral na internet.

Em síntese, o RE 1.037.396 reconhece que a comunicação digital afeta o processo eleitoral, mas exclui expressamente o regime eleitoral do âmbito vinculante da repercussão geral, preservando a autonomia normativa da Justiça Eleitoral. Essa delimitação é essencial para a correta compreensão dos impactos do julgamento sobre a propaganda eleitoral na internet e constitui premissa metodológica indispensável para a análise das resoluções do TSE, a ser desenvolvida em etapa posterior do relatório.

1.7 ESTADO DA ARTE DA CORREGULAÇÃO: ESTUDO DOS TERMOS DE COOPERAÇÃO COM PLATAFORMAS

Paula Pedigoni Ponce

Desde o ciclo eleitoral de 2020, o Tribunal Superior Eleitoral vem adotando parcerias com plataformas provedoras de aplicação. Trata-se de estratégia de corregulação implementada. O objetivo desta seção é sumarizar a estrutura e as principais obrigações estabelecidas no âmbito destas parcerias ao longo dos ciclos eleitorais de 2020, 2022 e 2024, destacando pontos de evolução. Para tanto, foi realizada a análise dos memorandos de entendimento de plataformas provedoras de aplicação. As parcerias inserem-se em programa estabelecido em 2019.

O Programa de Enfrentamento à Desinformação com Foco nas Eleições 2020 foi lançado pelo TSE em 30.08.2019, por meio da Portaria nº 663/2019, durante a presidência da Ministra Rosa Weber, e tinha como objetivo enfrentar os efeitos negativos provocados pela desinformação à imagem e à credibilidade da Justiça Eleitoral, à realização das eleições e aos atores nelas envolvidos (Brasil, 2020). Desde a instituição do Programa, foi estabelecida a formalização de parcerias entre o TSE e instituições públicas ou privadas interessadas em contribuir com o alcance dos objetivos do programa (art. 4º da Portaria nº 633/2019). Até maio de 2020, o Programa já contava com 49 parceiros - que incluíam entidades sem fins lucrativos (INCT.DD, Internetlab, Redes Cordiais, Abranet, ABI, Abert, ANJ, entre outras), partidos políticos (DEM, PTB, PCdoB, entre outros), agências de checagem (Boatos.org, Agência aos Fatos e Agência Lupa) e plataformas provedoras de aplicação (Google, Facebook, Twitter e WhatsApp) (Brasil, 2019a).

1.1 ELEIÇÕES DE 2020

No Plano Estratégico do Programa de Enfrentamento com Foco nas Eleições de 2020, o TSE estabeleceu que deveria envidar esforços para celebrar *"memorandos de entendimento ou outros instrumentos de parceria que definam as medidas concretas que serão desenvolvidas pelos parceiros para o enfrentamento à desinformação no âmbito do Programa, em suas respectivas áreas de atuação"* (Brasil, 2020, p. 1). Na oportunidade, já mencionava que se pretendia desenvolver, em colaboração com o WhatsApp, *chatbot* a partir da API do WhatsApp *Business* para facilitar o acesso do cidadão às informações úteis sobre as Eleições 2020 (Brasil, 2020, p. 30).

Com efeito, na eleição de 2020, foram firmados memorandos de entendimentos com Facebook/Instagram, TikTok, Twitter e WhatsApp. Podem ser indicados quatro eixos principais desses acordos firmados para as eleições de 2020: (i) ações para a disseminação de informações confiáveis - a partir da utilização das plataformas para a divulgação de informações e resposta à dúvidas sobre os pleitos eleitorais, incluindo a preparação de materiais para a divulgação de informações sobre as plataformas e informações sobre as medidas de combate à desinformação adotadas pelas plataformas; (ii) o estabelecimento de canal de comunicação extrajudicial entre as plataformas; e (iii) ações para a capacitação - incluindo a realização de eventos e formações com os servidores da justiça eleitoral sobre o funcionamento das plataformas.

A partir das informações disponibilizadas nos memorandos de entendimentos entre o TSE e as plataformas, celebrados em 2020, foi preparado o quadro a seguir:

	Eixo I: ações para a disseminação de informações confiáveis	Eixo II: ações para capacitação	Eixo III: canal de denúncias entre TSE e plataforma
WhatsApp (Brasil, 2020b)	Acesso à API do WhatsApp Business para disponibilizar chatbot no WhatsApp para facilitar a comunicação entre o TSE e os eleitores brasileiros Cartilha educativa com explicações sobre o aplicativo WhatsApp e informações úteis sobre o combate à desinformação	Eventos para treinamento de servidores Tribunais Regionais Eleitorais sobre o funcionamento do aplicativo e as medidas adotadas em preparação às eleições	Canal de comunicação extrajudicial para que o TSE reportasse contas suspeitas de realização de disparos em massa
Facebook/Instagram (Brasil, 2020c)	Megafone no início da timeline com informações sobre as eleições Stickers sobre eleições (Instagram) Guia de Mulheres na Política sobre participação feminina nas eleições, com apoio na divulgação e distribuição (Instagram)	Eventos online com os servidores dos TREs e Zonas Eleitorais e conteúdos gravados sobre as ferramentas do Facebook e sobre sua atuação nas eleições TSE distribuirá cartilhas para TREs e Zonas Eleitorais com aspectos práticos sobre as plataformas do Facebook e do Instagram e informações sobre o funcionamento das plataformas, combate a abusos e sobre o contencioso eleitoral digital	N/A
Google/Youtube (Brasil, 2020d)	Disponibilização na busca do Google de informações úteis sobre o processo de votação, como regularização do título de eleitor e orientações sobre como votar Produção de uma série de webinars disponibilizados nos canais da Google Brasil e da Justiça Eleitoral no YouTube, ampliando o acesso a informações confiáveis	Promoção de treinamentos voltados à capacitação de servidores do TSE e TREs, inclusive da perspectiva jurídica	N/A[2]

2 Em seu Memorando de Entendimentos, o Google reforçou os canais já existentes, incluindo links para denúncias de anúncios, e-mails para ordens judiciais e denúncias em outros produtos Google.

TikTok (Brasil, 2020e)	Página no Tiktok com Centro de Informações - centralizando informações educativas e confiáveis sobre o processo eleitoral	Realização de treinamentos para as equipes de comunicação do TSE sobre como utilizar a plataforma (inclusive com relação a como produzir vídeos de qualidade)	Canal de recebimento de denúncias do TSE sobre conteúdo com riscos de danos à integridade das eleições[3]
Twitter (Brasil, 2020f)	Prompt no campo de busca do Twitter direcionando para site do TSE Divulgação de conteúdos do TSE na conta do Twitter Brasil e em totens urbanos Apoio à transmissão de eventos, prompts, hashtags e emojis ao vivo do TSE Criação de emojis especiais sobre as eleições	Sessões de capacitação para equipes do TSE e TREs sobre melhores práticas do Twitter, funcionamento da plataforma e temas relacionados ao contencioso eleitoral	Atuação prioritária na análise de conteúdos denunciados pelo TSE por possíveis violações às regras da plataforma

Os resultados das parcerias foram amplamente divulgados. Primeiro, foi criada uma página no site da Justiça Eleitoral sobre as "Parcerias Digitais para as Eleições 2020" - com disponibilização dos memorandos de entendimentos e resultados da parceria (Brasil, s.d.). Ademais, as informações foram detalhadas no Relatório de Ações e Resultados do Programa de Enfrentamento com Foco nas Eleições de 2020 (Brasil, 2021a). Neste, ainda, foi indicado que, após a celebração dos acordos, foram realizadas reuniões periódicas entre o TSE e os pontos focais dos provedores, para acompanhamento da implementação das medidas e avaliação contínua dos resultados.

1.7.2. ELEIÇÕES DE 2022

Em 2021, foi instituído o Programa Permanente de Enfrentamento à Desinformação da Justiça Eleitoral (PPED), por meio da Portaria TSE nº 510/2021. A criação de um programa permanente ocorreu pois o TSE concluiu que a adoção de esforços de combate à desinformação centrados em períodos eleitorais não seria suficiente, considerando a crescente complexidade do fenômeno da desinformação e do fato de que as campanhas de desinformação não se reduzem aos períodos eleitorais, sendo produzidas e disseminadas em outros períodos, exigindo uma atuação contínua por parte das instituições (Brasil, 2021b).

3 Havia, ainda, obrigação de TikTok e TSE de manter troca de informações constante durante o processo eleitoral de 2020 para minimizar os riscos de danos à integridade de eleições

O foco do programa é a "desinformação relacionada à Justiça Eleitoral e aos seus integrantes, ao sistema eletrônico de votação, ao processo eleitoral em suas diferentes fases e aos atores nele envolvidos" (art. 1º da Portaria TSE nº 510/2021), de modo que se alinharia à missão constitucional do TSE de garantir a legitimidade e regularidade democrática do processo eleitoral (Brasil, 2021b). O programa foi estruturado a partir de três eixos: (i) informar, para disseminar informação de qualidade; (ii) capacitar, que tinha como objetivo a alfabetização midiática e capacitação para públicos internos e externos à Justiça Eleitoral; e (iii) responder, visando à adoção de medidas para identificar, conter e desestimular práticas de desinformação.

Antes das eleições de 2022, o TSE estabeleceu parcerias com 13 plataformas digitais: Amazon, Facebook, Google, Instagram, Kwai, Linkedin, Spotify, Telegram, TikTok, Twitch, Twitter, WhatsApp e YouTube. As obrigações dos memorandos de entendimentos foram classificadas de acordo com os três eixos do Programa Permanente. Observa-se que os eixos são similares e espelham aqueles identificados nas parcerias firmadas em 2020 - isto é, tratando de disseminação de informações confiáveis a partir das redes, ações de capacitação e atuação conjunta para a identificação e contenção de desinformação. Com relação ao último ponto, o TSE destacou no *"Programa Permanente de Enfrentamento à Desinformação no âmbito da Justiça Eleitoral: plano estratégico: eleições 2022"* que promove uma *"autorregulação estruturada"* sobre desinformação contra o processo eleitoral, para garantir a transparência na política das plataformas, bem como consistência e celeridade no monitoramento e enforcement dessas políticas (Brasil, 2022, p. 33). Além disso, recomendava que as plataformas produzissem relatórios sobre as medidas tomadas para a proteção do processo eleitoral para fins de *accountability.*

	Eixo I: Informar - disseminação de informação de qualidade	**Eixo II: Capacitar - alfabetização midiática e capacitação**	**Eixo III: Responder - identificação e contenção de desinformação**
WhatsApp (Brasil, 2020b)	Acesso à API do WhatsApp Business para disponibilizar chatbot no WhatsApp para facilitar a comunicação entre o TSE e os eleitores brasileiros Cartilha educativa com explicações sobre o aplicativo WhatsApp e informações úteis sobre o combate à desinformação **Nova:** atuação conjunto para o desenvolvimento de Stickers	Eventos para treinamento de servidores do TSE e TRE sobre o funcionamento do aplicativo e as medidas adotadas em preparação às eleições Nova: Evento contempla servidores do TSE e os seguintes temas: *"boas práticas no uso de recursos e funcionalidades do aplicativo; (ii) regras e políticas aplicáveis e (iii) aspectos práticos do contencioso eleitoral"*	Canal de comunicação extrajudicial para que o TSE reportasse contas suspeitas de realização de disparos em massa **Nova:** Dever do TSE de disponibilizar formulário eletrônico para TRE e eleitores para denúncias, bem como de instruir as denúncias e encaminhar os casos de fundadas suspeitas para a plataforma **Nova:** Previsão de que as denúncias são apenas informativas, não gerando obrigação legal de remoção ou constituírem prova de ilícito eleitoral, as medidas de banimento adotadas pelo WhatsApp são apenas realizadas com base em violações aos termos e políticas da empresa.

Facebook/Instagram (Brasil, 2020c)	Megafone no início da timeline com informações sobre as eleições Stickers sobre eleições (Instagram) Nova versão do Guia de Mulheres na Política sobre participação feminina nas eleições, com apoio na divulgação e distribuição (Instagram) Nova: Rótulo eleitoral em conteúdos relacionados às eleições no Facebook e Instagram com direcionamento para o site da Justiça Eleitoral **Nova:** Criação de chatbot no Instagram para facilitar acesso a informações eleitorais.	Eventos online com os servidores dos TREs e TSE e conteúdos gravados sobre as ferramentas do Facebook e sobre sua atuação nas eleições Nova: Evento contempla servidores do TSE e os seguintes temas: "boas práticas no uso de recursos e funcionalidades do aplicativo; (ii) regras e políticas aplicáveis ao processo eleitoral, desinformação e temas correlatos e (iii) aspectos práticos do contencioso eleitoral" Distribuição para TREs de cartilhas com aspectos práticos sobre as plataformas do Facebook e do Instagram e informações sobre o funcionamento das plataformas, combate a abusos e sobre o contencioso eleitoral digital. **Nova:** Workshops para os servidores do TSE sobre a definição de discurso de ódio e conteúdos proibidos nas plataformas da Meta	**Nova:** Disponibilização de acesso à API da Biblioteca de Anúncios da Meta para o TSE acessar dados sobre anúncios políticos, mediante criação de conta de desenvolvedor e suporte do Facebook Brasil. **Nova:** Criação de canal extrajudicial para que TSE denuncie conteúdos potencialmente desinformativos sobre o processo eleitoral - as denúncias são não-vinculativas
Google/Youtube (Brasil, 2020d)	Nova: Destaque editorial de uma coleção de aplicativos com conteúdo cívico na Google Play Store durante o período eleitoral, podendo incluir apps oficiais do TSE. Nova: Publicar um Doodle relacionado às Eleições 2022. Nova: Adotar "medidas para garantir que os usuários tenham acesso a informações confiáveis sobre o processo eleitoral", incluindo ações do TSE contra a desinformação. Nova: Programa Cresça com o Google (versão online), voltado a eleitores, com conteúdos sobre desinformação eleitoral e o funcionamento das plataformas.	Promoção de treinamentos voltados à capacitação de servidores do TSE e TREs, inclusive da perspectiva jurídica Nova: Especificação dos temas de 8 treinamentos, que incluirão treinamento sobre o funcionamento do Youtube e Google Ads, bem como sobre o sistema de comunicação de ordens judiciais. Nova: Capacitação para outros atores relevantes, como partidos políticos, checadores de fatos, instituições de pesquisa e parceiros do Programa de Enfrentamento à Desinformação, com foco em Google Ads, YouTube e ferramentas de checagem de fatos. Nova: Produção de conteúdo informativo, com a criação de uma página especial para as Eleições 2022, explicando o funcionamento das plataformas e políticas do Google.	Nova: Criação pelo Google de página Trends Hub com dados sobre tendências de buscas relacionadas ao processo eleitoral, atualizada ao longo de 2022. Nova: Treinamentos para TSE, credenciado no programa Trusted Flagger. O TSE começou a integrá-lo em 2020 e o programa fornece ferramentas avançadas de denúncia de conteúdo e feedback de decisões[4] Nova: Publicação de relatório de Transparência de Anúncios Políticos no Brasil. Nova: Atualização das políticas do Google Ads e Display & Video 360, exigindo verificação obrigatória dos anunciantes de conteúdos políticos.

4 Além disso, é indicado canal de e-mail para envio de ordens judiciais por TSE e TREs e formulário para o Youtube.

TikTok (Brasil, 2020e)	Página no Tiktok com Centro de Informações - centralizando informações educativas e confiáveis sobre o processo eleitoral Nova: Apoiar transmissões ao vivo do TSE, com divulgação na plataforma. Nova: Auxiliar a divulgação de conteúdos produzidos pela conta oficial do TSE no TikTok (por meio de banners ou na página central). Nova: Adoção de etiqueta de eleição para conteúdos selecionados relativos às eleições de 2022, com link para o site da Justiça Eleitoral.	Nova: Treinar equipes do TSE e TREs, incluindo: (i) workshop sobre medidas de combate à desinformação; (ii) capacitação sobre políticas e termos de uso da plataforma. Nova: Oferecer treinamentos a atores relevantes: partidos, agências de checagem, instituições de pesquisa e parceiros do Programa de Enfrentamento à Desinformação. Nova: Produção de cartilhas educativas sobre a plataforma.	Canal de recebimento de denúncias do TSE sobre conteúdo que potencialmente viole as regras e políticas do TikTok.[5] Nova: Disponibilizar um canal especial para o envio de ordens judiciais pelo TSE e TREs. Nova: Dar feedback sobre as denúncias enviadas e fornecer relatório de transparência com dados estatísticos sobre a aplicação das políticas. Nova: Remover conteúdos maliciosos, como contas falsas e comportamento inautêntico coordenado, conforme políticas do TikTok. Nova: Apoiar instituições de checagem parceiras do TSE com capacitações e ações específicas.
Twitter (Brasil, 2020f)	Prompt no campo de busca com informações relacionadas ao processo eleitoral e link para site do TSE Nova: Desenvolver uma curadoria especial ("Moment") no Twitter de conteúdos publicados pelo TSE, TRE, mídias e instituições de checagem de fatos. Apoio à divulgação de conteúdos do TSE na conta do Twitter Brasil Apoio à transmissão de eventos ao vivo do TSE Criação de emojis especiais sobre as eleições	Sessões de capacitação para equipes do TSE e TREs sobre melhores práticas do Twitter, funcionamento da plataforma e temas relacionados ao contencioso eleitoral. Nova: Promover capacitação para atores relevantes, como partidos, agências de checagem e parceiros do Programa de Enfrentamento à Desinformação. Nova: Cooperar na produção de materiais educativos sobre uso seguro da plataforma e boas práticas para mitigar desinformação.	Atuação diligente na análise de conteúdos denunciados pelo TSE por possíveis violações às regras da plataforma. Nova: Criar canal dedicado de comunicação com o TSE para denúncias de conteúdos potencialmente violadores das regras da plataforma. Nova: Disponibilizar um canal especial para o envio de ordens judiciais pelo TSE.

5 O Canal de denúncia estabelecido no Memorando de Entendimentos de 2020 estabelecia um canal para denúncias de conteúdos que potencialmente ofereçam riscos de danos à integridade das eleições, de modo que o objeto das denúncias foi alterado para se referir às regras e políticas do TikTok.

Em termos de capacitação, observa-se que as ações de capacitação foram focadas no TSE e TREs, diferentemente das eleições de 2020, nas quais houve capacitações de zonas eleitorais. Ademais, nota-se que os memorandos de entendimentos passaram a especificar um conjunto mínimo de temas para os treinamentos.

Com relação ao terceiro eixo, de resposta à desinformação, a partir da análise comparativa dos memorandos de entendimentos, destaca-se a evolução de dispositivos acerca dos canais de denúncias disponíveis para o TSE - considerando que, em 2022, todos os memorandos analisados contavam com previsão de compartilhamento de denúncias por parte do TSE. Entretanto, observa-se que nenhuma das plataformas se comprometeu à remoção de conteúdos indicados pela Justiça Eleitoral, havendo a especificação de que a análise de denúncias seria feita a partir das políticas e termos de uso de cada uma das plataformas.

Ainda na dimensão de resposta à desinformação, o TSE passou a ter acesso facilitado à biblioteca de anúncios da Meta e ao Relatório de Transparência de Anúncios do Google. Além disso, outro aspecto relacionado a conteúdos, foram os compromissos de rotulagem de conteúdos eleitorais assumidos pela Meta e TikTok. As obrigações relacionam-se aos deveres de transparência, descritos no item 2.13.

Com relação à implementação dos memorandos de entendimentos, nota-se que o TSE divulgou o relatório de ações e resultados do Programa Permanente de Enfrentamento à Desinformação no âmbito da Justiça Eleitoral (Brasil, 2023). O Relatório conta com informações sobre as iniciativas previstas nos Memorandos de Entendimentos, bem como dados das plataformas sobre sua atuação com relação à remoção de conteúdo relacionados às eleições, sintetizadas abaixo (Brasil, 2023):

	WhatsApp	Facebook e Instagram	TikTok	Twitter	Google/ Youtube
Postagens rotuladas	N/A	74 mi no Facebook	1,5 milhão de vídeos, sendo que as etiquetas foram acessadas quase 17 milhões de vezes.	N/A	N/A
Denúncias no canal de denúncias	N/A	530, em 85% dos conteúdos indicados foram adotadas ações pela Meta	128 URLs indicadas, em 106 houve remoção após análise pelo TikTok	N/A	N/A
Anúncios de conteúdo político rejeitados	N/A	135 mil conteúdos	N/A (proibição de anúncios com conteúdo político pelo TikTok)	N/A	N/A

Conteúdos removidos no período de campanha eleitoral	N/A	310 mil conteúdos por violência e incitação e mais de 290 mil por discurso de ódio.	66 mil vídeos foram removidos	N/A	10 mil vídeos removidos e 2.500 canais excluídos do Youtube
Conteúdos removidos relacionados a 8 de janeiro de 2023	N/A	Conteúdos removidos entre o início da campanha eleitoral, em 16 de agosto e 8 de janeiro: 570 mil conteúdos no Facebook e mais de 520 mil conteúdos no Instagram que violaram as políticas de discurso de ódio, além de 380 mil e 630 mil que violaram as políticas de bullying e assédio, em cada uma das plataformas, respectivamente.	Entre os dias 8 e 15 de janeiro, foram removidos, espontaneamente, mais de 1,3 mil conteúdos violadores da política contra o extremismo, 5,5 mil conteúdos violadores da política de desinformação com riscos de danos no mundo real e 3,6 mil conteúdos por violação da política de desinformação sobre as eleições.	N/A	N/A

Nesse ponto, chama atenção que não há uma padronização das informações fornecidas pelas plataformas, de modo que várias não chegaram a informar dados de moderação de conteúdo no período eleitoral. Esse ponto foi endereçado na Resolução n° 23.732/2024, que estabelece o dever de plataformas de adotar transparência com relação aos resultados de desinformação (art. 9°-D, inc. IV), discutida na seção. Todavia, um potencial ponto de aprimoramento para a regulação seria o de especificar um modelo de divulgação pública, pelas próprias plataformas, da atuação em moderação de conteúdo nos períodos eleitorais - incluindo um conjunto mínimo de informações, incluindo: números de atuação proativa de remoção de conteúdo, de atuação reativa, entre outras informações relativas à conteúdo eleitoral.

Especialmente quanto ao Sistema de Alerta de Desinformação Contra as Eleições (SIADE), criado em 2022 a partir do canal de denúncias de disparo em massa estabelecido em 2020, o Relatório informa que, entre 21 de junho de 2022 e 23 de março de 2023, foram recebidos 43.559 apontamentos de conteúdos ou práticas (como disparos em massa e comportamento inautêntico), dos quais 26.285 (68%) foram, efetivamente, encaminhados às plataformas. Outros 32% das denúncias recebidas foram arquivadas (Brasil, 2023, p. 69). Não há, entretanto, detalhamento sobre a atuação das plataformas a partir das denúncias recebidas a partir do SIADE.

1.7.3 ELEIÇÕES DE 2024.

Para o ciclo eleitoral de 2024, o TSE manteve e expandiu a estratégia de cooperação com plataformas digitais no âmbito do Programa Permanente de Enfrentamento à Desinformação, estruturado nos eixos de sensibilizar sobre os perigos da desinformação, identificar e cooperar com diferentes atores (Brasil, 2024a).

No plano institucional, destaca-se a criação do Centro Integrado de Enfrentamento à Desinformação e Defesa da Democracia (CIEDDE), por meio da Portaria TSE nº 180/2024, concebido como instância de coordenação em tempo real entre o TSE, os TREs, órgãos públicos parceiros e plataformas digitais, incluindo Meta, Google, TikTok, Kwai, Telegram, LinkedIn e X Brasil (Brasil, 2024b, p. 12). O CIEDDE foi estruturado enquanto rede de comunicação em tempo real desses agentes. Além disso, o relatório do "Programa Permanente de Enfrentamento à Desinformação no âmbito da Justiça Eleitoral: relatório de ações e resultados: eleições 2024" destacou aperfeiçoamentos do SIADE, inclusive com maior integração com os TREs, fluxos de trabalho e reformulação da interface (Brasil, 2024b, pp. 42 e 43).

Quanto às parcerias com plataformas, foram formalizados memorandos de entendimento com Meta (Facebook, Instagram, WhatsApp e Threads), Google, TikTok, Kwai, LinkedIn, Telegram e X Brasil, com o objetivo de fortalecer o combate à desinformação durante o período eleitoral de 2024. (Brasil, 2024b, p. 14). Esses memorandos mantiveram a lógica de três eixos observada em 2020 e 2022, com ênfase na atuação coordenada via CIEDDE e na utilização do SIADE como principal canal de denúncias. Os memorandos de entendimento foram analisados e suas obrigações sumarizadas na tabela a seguir, conforme já realizado para os demais ciclos eleitorais:

	Eixo I: Informar - disseminação de informação de qualidade	**Eixo II: Capacitar - alfabetização midiática e capacitação**	**Eixo III: Responder - identificação e contenção de desinformação**
Meta (WhatsApp, Facebook, Instagram e Threads) (Brasil, 2024c)	Acesso à API do WhatsApp Business para disponibilizar chatbot no WhatsApp para facilitar a comunicação entre o TSE e os eleitores brasileiros Megafone no início da timeline do Facebook e Instagram com informações sobre as eleições.	Seminários de capacitação com TSE, TREs e magistrados sobre o uso das plataformas (Facebook, Instagram, Threads, WhatsApp), incluindo políticas de desinformação, boas práticas de uso, regras das plataformas e aspectos práticos do contencioso eleitoral.	Disponibilização de acesso à API da Biblioteca de Anúncios da Meta para o TSE acessar dados sobre anúncios políticos, mediante criação de conta de desenvolvedor e suporte do Facebook Brasil. Nova: Dever de colaboração com as ações do CIEDDE, conforme plano de trabalho. Nova: SIADE utilizado como canal de recebimento de denúncias e conteúdos publicados no Facebook, Instagram, Threads ou WhatsApp (canais e suspeitas disparos em massa). Nova: No âmbito do SIADE, o TSE é responsável por receber, triar e analisar inicialmente as denúncias, com base nos parâmetros do Repositório Público de Decisões. Quando o TSE identificar potencial ilicitude, a denúncia será encaminhada à Meta para análise e providências conforme as políticas da plataforma e legislação aplicável. A Meta deve analisar e tomar providências cabíveis em até 24 horas após o recebimento da denúncia, caso não seja possível, deverá sinalizar para o TSE. Deve ser indicada URL específica do conteúdo. Nova: Suspensão de anúncios de candidatos, partidos e coligações no Facebook e no Instagram durante os períodos em que a resolução veda o impulsionamento de conteúdos, nos termos dos artigos 29, parágrafo 11º da Resolução n.º 23.610/2019, com previsão que a suspensão será aplicada sobre as contas de candidatos.

Facebook/ Instagram (Brasil, 2020c)	Seleção editorial de uma coleção de aplicativos com conteúdo cívico na Google Play Store durante o período eleitoral, podendo incluir apps oficiais do TSE. Adotar "medidas para garantir que os usuários tenham acesso a informações confiáveis sobre o processo eleitoral", incluindo ações do TSE contra a desinformação. Project Shield para proteção dos agentes no processo eleitoral.	Promoção de treinamentos voltados à capacitação de servidores do TSE, TRE e magistrados envolvidos no processo eleitoral sobre as medidas de combate à desinformação da Plataforma e políticas e termos de uso aplicáveis. Produção de conteúdo informativo, com a criação de uma página especial para as Eleições 2022, explicando o funcionamento das plataformas e políticas do Google. Treinamento sobre a Plataforma no contexto das eleições para outros atores relevantes, como partidos políticos, checadores de fatos, instituições de pesquisa e parceiros do Programa de Enfrentamento à Desinformação.	Criação pelo Google da página Trends Hub com dados sobre tendências de buscas relacionadas ao processo eleitoral, atualizada ao longo de 2024 e a ser mantida durante as eleições. Nova: Dever de colaboração com as ações do CIEDDE, conforme acordado entre as partes. Nova: Utilização do Google do canal do CIEDDE como canal de denúncias de conteúdos a serem enviados à plataforma.

Google/ Youtube (Brasil, 2020d)	Nova: Destaque editorial de uma coleção de aplicativos com conteúdo cívico na Google Play Store durante o período eleitoral, podendo incluir apps oficiais do TSE. Nova: Publicar um Doodle relacionado às Eleições 2022. Nova: Adotar "medidas para garantir que os usuários tenham acesso a informações confiáveis sobre o processo eleitoral", incluindo ações do TSE contra a desinformação. Nova: Programa Cresça com o Google (versão online), voltado a eleitores, com conteúdos sobre desinformação eleitoral e o funcionamento das plataformas.	Promoção de treinamentos voltados à capacitação de servidores do TSE e TREs, inclusive da perspectiva jurídica Nova: Especificação dos temas de 8 treinamentos, que incluirão treinamento sobre o funcionamento do Youtube e Google Ads, bem como sobre o sistema de comunicação de ordens judiciais. Nova: Capacitação para outros atores relevantes, como partidos políticos, checadores de fatos, instituições de pesquisa e parceiros do Programa de Enfrentamento à Desinformação, com foco em Google Ads, YouTube e ferramentas de checagem de fatos. Nova: Produção de conteúdo informativo, com a criação de uma página especial para as Eleições 2022, explicando o funcionamento das plataformas e políticas do Google.	Nova: Criação pelo Google de página Trends Hub com dados sobre tendências de buscas relacionadas ao processo eleitoral, atualizada ao longo de 2022. Nova: Treinamentos para TSE, credenciado no programa Trusted Flagger. O TSE começou a integrá-lo em 2020 e o programa fornece ferramentas avançadas de denúncia de conteúdo e feedback de decisões Nova: Publicação de relatório de Transparência de Anúncios Políticos no Brasil. Nova: Atualização das políticas do Google Ads e Display & Video 360, exigindo verificação obrigatória dos anunciantes de conteúdos políticos.

TikTok (Brasil, 2020e)	Página no Tiktok com Centro de Informações - centralizando informações educativas e confiáveis sobre o processo eleitoral Apoiar transmissões ao vivo do TSE, com divulgação na plataforma. Auxiliar a divulgação de conteúdos produzidos pela conta oficial do TSE no TikTok (inclusive no Centro de Informações). Adoção de etiqueta de eleição para conteúdos selecionados relativos às eleições de 2024, com link para o site da Justiça Eleitoral.	Treinar equipes do TSE, TREs e magistrados envolvidos no processo eleitoral, incluindo: (i) workshop sobre medidas de combate à desinformação; (ii) capacitação sobre políticas e termos de uso da plataforma; (iii) informações necessárias para viabilizar o cumprimento de ordens judiciais. Oferecer treinamentos a atores relevantes: partidos, agências de checagem, instituições de pesquisa e parceiros do Programa de Enfrentamento à Desinformação.	Nova: Dever de colaboração com as ações do CIEDDE, com o objetivo de promover a atuação coordenada e célere no enfrentamento à disseminação de conteúdos desinformativos, discursos de ódio, discriminatórios e antidemocráticos, nos termos da Portaria TSE nº 180/2024. Nova: SIADE utilizado como canal de recebimento de denúncias e conteúdos publicados. Nova: No âmbito do SIADE, o TSE é responsável por receber, triar e analisar inicialmente as denúncias, com base nos parâmetros do Repositório Público de Decisões. Quando o TSE identificar potencial ilicitude, a denúncia será encaminhada ao TikTok para análise e providências conforme as políticas da plataforma. O TikTok deve envidar seus melhores esforços para concluir a análise em até 24 horas após o recebimento da denúncia, caso não seja possível, deverá sinalizar para o TSE. Deve ser indicada URL específica do conteúdo.
X (ex-Twitter) (Brasil, 2024f)	Nova: O X Brasil disponibiliza o recurso Nota da Comunidade, pelo qual colaboradores podem adicionar contexto a postagens, ajudando a ampliar a compreensão dos usuários sobre conteúdos relevantes no período eleitoral.	Sessões de capacitação para equipes do TSE, TREs e magistrados sobre as regras e políticas da plataforma X, a aplicação de regras, além de canais e processos de denúncias disponíveis.	Atuação diligente na análise de conteúdos denunciados pelo TSE por possíveis violações às regras da plataforma. Nova: Dever de colaboração com as ações do CIEDDE, com o objetivo de promover a atuação coordenada e célere no enfrentamento à disseminação de conteúdos desinformativos, discursos de ódio, discriminatórios e antidemocráticos, nos termos da Portaria TSE nº 180/2024 e plano de trabalho. Nova: SIADE utilizado como canal de recebimento de denúncias e conteúdos publicados. Nova: No âmbito do SIADE, o TSE é responsável por receber, triar e analisar inicialmente as denúncias, com base nos parâmetros do Repositório Público de Decisões. Quando o TSE identificar potencial ilicitude, a denúncia será encaminhada ao Twiter para análise e providências conforme as políticas da plataforma. O Twiter deve envidar seus melhores esforços para concluir a análise em até 24 horas após o recebimento da denúncia, caso não seja possível, deverá sinalizar para o TSE. Deve ser indicada URL específica do conteúdo.

No ciclo eleitoral de 2024, as principais inovações institucionais nas parcerias entre o TSE e as plataformas digitais foram a criação do Centro Integrado de Enfrentamento à Desinformação e Defesa da Democracia (CIEDDE) e o aprimoramento do Sistema de Alertas de Desinformação Eleitoral (SIADE), que passaram a concentrar e estruturar a atuação coordenada entre Justiça Eleitoral, órgãos públicos e plataformas (Brasil, 2024b, p. 12-13).

Não obstante, observa-se que as informações públicas atualmente disponibilizadas sobre os processos internos, os fluxos decisórios e os resultados da atuação do CIEDDE e do SIADE são ainda limitadas, o que tende a dificultar uma avaliação externa mais precisa da efetividade desses instrumentos e o fortalecimento do controle público sobre sua operação. Em especial, nota-se a ausência de divulgação de métricas sobre a atuação das plataformas no combate à desinformação, como volume de denúncias por plataforma, taxas de resposta, medidas adotadas e resultados agregados de moderação de conteúdo, o que restringe a comparabilidade e a mensuração sistemática dos impactos das iniciativas implementadas (Brasil, 2024b).

1.7.4 CONCLUSÕES PRELIMINARES SOBRE OS MEMORANDOS DE ENTENDIMENTOS COM PLATAFORMAS

As parcerias firmadas com as plataformas digitais representam uma relevante forma de interação entre essas plataformas e a Justiça Eleitoral. A iniciativa se delineia como um exemplo de "autorregulação estruturada", conforme proposto pelo TSE, e se aproxima de modelos de corregulação discutidos ao longo deste relatório. De fato, a experiência de formulação e cumprimento de memorandos de entendimentos pode servir como base para a compreensão das obrigações estabelecidas nas Resoluções do TSE sobre o tema.

Primeiro, especialmente a partir do Eixo I, as parcerias possibilitam a divulgação de informações sobre as eleições. Os relatórios do TSE detalham como os avisos em aplicativos e outras campanhas de disseminação a partir de plataformas impactaram milhões de brasileiros (Brasil, 2023). Com relação ao Eixo III, nota-se como ele é exemplo central de atuação coordenada do TSE e das plataformas - e a consolidação de canais de denúncias para o TSE em períodos eleitorais.

A partir da análise da evolução dos memorandos ao longo dos ciclos eleitorais, observa-se não apenas a maior especificação de deveres para as plataformas, mas também relevantes ganhos institucionais em termos de conhecimento sobre sua atuação. Os memorandos possibilitaram uma experiência continuada de diálogo e troca entre plataformas e TSE, contribuindo para uma compreensão mais precisa sobre o funcionamento e os limites operacionais desses atores — resultado particularmente associado ao Eixo II, voltado à capacitação.

Apesar de se mostrar uma iniciativa relevante, considerando esses aspectos, destaca-se o caráter ainda incipiente dos memorandos de entendimento no sentido de representar um mecanismo efetivo de corregulação. Ao longo do presente relatório, são apresentadas recomendações para melhor substanciar os deveres dos provedores de aplicação estabelecidos a partir da regulamentação do TSE.

Em especial, observa-se a dificuldade de avaliar os efeitos concretos das parcerias firmadas, o que evidencia limitações em termos de transparência. Embora os relatórios disponibilizados pelo TSE tragam informações sobre a implementação dos memorandos, os dados publicamente acessíveis sobre a atuação das plataformas — especialmente no que se refere ao eixo de resposta à desinformação e à operação do CIEDDE e do SIADE — permanecem insuficientes. A divulgação mais detalhada dessas informações pelas próprias plataformas constituiria relevante insumo para a própria Justiça Eleitoral, pesquisadores e instituições da sociedade civil, contribuindo para o fortalecimento do controle público e para a avaliação sistemática da efetividade das iniciativas adotadas.

REFERÊNCIAS

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei nº 6.404, de 15 de dezembro de 1976. Dispõe sobre as Sociedades por Ações. Diário Oficial da União: seção 1, Brasília, DF, 1976. Disponível em: https://www2.camara.leg.br/legin/fed/lei/1970-1979/lei-6404-15-dezembro-1976-368447-publicacaooriginal-1-pl.html. Acesso em: 10 dez. 2025.

BRASIL. Superior Tribunal de Justiça (Terceira Turma). Recurso Especial n. 1.193.764/SP. Relatora: Ministra Nancy Andrighi, Brasília, 14 dez. 2010. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?num_registro=201000845120. Acesso em: 10 dez. 2025.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário 1.075.412/PE (Tema 995 da Repercussão Geral). Relator: Ministro Marco Aurélio. Relator para acórdão: Ministro Edson Fachin. Brasília: STF, 2023. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=775013462. Acesso em: 10 dez. 2025.

BRASIL. Supremo Tribunal Federal. Informação à sociedade: RE 1.037.396 (Tema 987) e 1.057.258 (Tema 533) responsabilidade de plataformas digitais por conteúdo de terceiros. Brasília: STF, 2025. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/Informac807a771oa768SociedadeArt19MCI_vRev.pdf. Acesso em: 10 dez. 2025.

BRASIL. Tribunal Superior Eleitoral. Parcerias digitais para as Eleições 2020. [s.d]. Disponível em: <https://www.justicaeleitoral.jus.br/parcerias-digitais-eleicoes/>. Acesso em: 3 set. 2025.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 2019. Dispõe sobre propaganda eleitoral. Brasília, DF, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 10 dez. 2025

BRASIL. Tribunal Superior Eleitoral. TSE lança Programa de Enfrentamento à Desinformação com Foco nas Eleições 2020. 2019. Disponível em: <https://www.tse.jus.br/comunicacao/noticias/2019/Agosto/tse-lanca-programa-de-enfrentamento-a-desinformacao-com-foco-nas-eleicoes-2020>. Acesso em: 3 set. 2025.

BRASIL. Tribunal Superior Eleitoral. Programa de Enfrentamento à Desinformação com Foco nas Eleições 2020. Brasília, 2020. Disponível em: <https://www.tse.jus.br/comunicacao/noticias/arquivos/tse-programa-de-enfrentamento-a-desinformacao/@@display-file/file/Programa_de_enfrentamento_web.pdf>. Acesso em: 3 set. 2025.

BRASIL. Tribunal Superior Eleitoral. Memorando de Entendimento-TSE nº 43/2020. 2020b. Disponível em: https://www.justicaeleitoral.jus.br/desinformacao/arquivos/termos-de-cooperacao-plataformas-digitais/mou-whatsapp.pdf.

BRASIL. Tribunal Superior Eleitoral. Memorando de Entendimento-TSE nº 41/2020. 2020c. Disponível em: https://www.tse.jus.br/comunicacao/noticias/arquivos/tse-memorando-de-entendimento-facebook/@@display-file/file/memorando_facebook.pdf.

BRASIL. Tribunal Superior Eleitoral. Memorando de Entendimento-TSE nº 40/2020. 2020d. Disponível em: https://www.justicaeleitoral.jus.br/parcerias-digitais-eleicoes/assets/arquivos/memorando_google.pdf.

BRASIL. Tribunal Superior Eleitoral. Memorando de Entendimento-TSE nº 54/2020. 2020e. Disponível em: https://www.justicaeleitoral.jus.br/parcerias-digitais-eleicoes/assets/arquivos/memorando_tiktok.pdf.

BRASIL. Tribunal Superior Eleitoral. Memorando de Entendimento-TSE nº 38/2020. 2020f. Disponível em: https://www.tse.jus.br/comunicacao/noticias/arquivos/tse-memorando-entendimento-twitter/@@display-file/file/memorando_twitter.pdf.

BRASIL. Tribunal Superior Eleitoral. Programa de Enfrentamento à Desinformação com Foco nas Eleições 2020. Brasília, TSE, 2021a. Disponível em: <https://www.justicaeleitoral.jus.br/desinformacao/arquivos/Programa_de_enfrentamento_resultados.pdf>.

BRASIL. Tribunal Superior Eleitoral. Portaria nº 510, de 04 de agosto de 2021. Institui o Programa Permanente de Enfrentamento à Desinformação no âmbito da Justiça Eleitoral e disciplina sua execução. 2021b. Disponível em: https://www.tse.jus.br/legislacao/compilada/prt/2021/portaria-no-510-de-04-de-agosto-de-2021.

BRASIL. Tribunal Superior Eleitoral. Memorando de Entendimento-TSE nº 23/2021. 2021c. Disponível em: https://www.tse.jus.br/comunicacao/noticias/arquivos/assinatura-de-acordos-plataformas-digitais/memorando-tse-e-twitter/@@display-file/file/MoU%2520TSE_Twitter.pdf.

BRASIL. Tribunal Superior Eleitoral. Programa Permanente de Enfrentamento à Desinformação no âmbito da Justiça Eleitoral : plano estratégico : eleições 2022. 2022a. Disponível em: <https://www.justicaeleitoral.jus.br/desinformacao/arquivos/Programa_de_enfrentamento_resultados.pdf>.

BRASIL. Tribunal Superior Eleitoral. Memorando de Entendimento-TSE nº 04/2022. 2022b. Disponível em: https://www.justicaeleitoral.jus.br/desinformacao/arquivos/termos-de-cooperacao-plataformas-digitais/mou-whatsapp.pdf.

BRASIL. Tribunal Superior Eleitoral. Memorando de Entendimento-TSE nº 03/2022. 2022c. Disponível em: https://www.justicaeleitoral.jus.br/desinformacao/arquivos/termos-de-cooperacao-plataformas-digitais/facebook-e-instagram.pdf.

BRASIL. Tribunal Superior Eleitoral. Memorando de Entendimento-TSE nº 1/2022. 2022d. Disponível em: https://www.justicaeleitoral.jus.br/desinformacao/arquivos/termos-de-cooperacao-plataformas-digitais/mou-google.pdf.

BRASIL. Tribunal Superior Eleitoral. Memorando de Entendimento-TSE nº 2/2022. 2022e. Disponível em: https://www.justicaeleitoral.jus.br/desinformacao/arquivos/termos-de-cooperacao-plataformas-digitais/mou-tik-tok.pdf.

BRASIL. Tribunal Superior Eleitoral. Termo Aditivo ao Memorando de Entendimento-TSE nº 2/2022. 2022f. Disponível em: https://www.justicaeleitoral.jus.br/desinformacao/arquivos/termos-de-cooperacao-plataformas-digitais/termo-aditivo-tik-tok.pdf.

BRASIL. Tribunal Superior Eleitoral. Programa Permanente de Enfrentamento à Desinformação no âmbito da Justiça Eleitoral: relatório de ações e resultados eleições 2022. 2023. Disponível em: <https://www.justicaeleitoral.jus.br/desinformacao/arquivos/Relatorio_de_acoes_e_resultados_DIGITAL_Seprev_OK_FINAL__1_.pdf>. Acesso em: 19 jan. 2026.

BRASIL. Tribunal Superior Eleitoral. Programa Permanente de Enfrentamento à Desinformação no âmbito da Justiça Eleitoral : plano estratégico eleições 2024. 2024a. Disponível em: <https://www.justicaeleitoral.jus.br/desinformacao/arquivos/programa-permanente-de-enfrentamento-a-desinformacao-2024.pdf>. Acesso em: 19 jan. 2026.

BRASIL. Tribunal Superior Eleitoral. Programa Permanente de Enfrentamento à Desinformação no âmbito da Justiça Eleitoral: relatório de ações e resultados : eleições 2024. 2024b. Disponível em: <https://www.justicaeleitoral.jus.br/desinformacao/arquivos/programa-de-acoes-e-resultados-2024.pdf>. Acesso em: 19 jan. 2026.

BRASIL. Tribunal Superior Eleitoral. Memorando de Entendimento-TSE nº 29/2024. 2024c. Disponível em: https://www.tse.jus.br/comunicacao/arquivos/memorando-de-entendimento-tse-facebook-desinformacao-eleicoes-2024-2/@@display-file/file/TSE-memorando-entendimento-desinformacao-facebook-2024.pdf. Acesso em: 19 jan. 2026.

BRASIL. Tribunal Superior Eleitoral. Memorando de Entendimento-TSE nº 33/2024. 2024d. Disponível em: https://www.tse.jus.br/comunicacao/arquivos/memorando-de-entendimento-tse-google-brasil-internet-desinformacao-eleicoes-2024-2/@@display-file/file/TSE-memorando-entendimento-desinformacao-google-2024.pdf. Acesso em: 19 jan. 2026.

BRASIL. Tribunal Superior Eleitoral. Memorando de Entendimento-TSE nº 32/2024. 2024e. Disponível em: https://www.tse.jus.br/comunicacao/arquivos/memorando-de-entendimento-tse-x-desinformacao-eleicoes-2024-2/@@display-file/file/TSE-memorando-entendimento-desinformacao-x-2024.pdf. Acesso em: 19 jan. 2026.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 2024. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Brasília, DF, 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 10 dez. 2025.

ECONOMIST INTELLIGENCE UNIT (EIU). Democracy Index 2024: What's wrong with representative democracy? 2024. Disponível em: https://www.eiu.com/n/campaigns/democracy-index-2024/. Acesso em: 10 dez. 2025.

FERREIRA, Lucia Maria Teixeira. A dimensão objetiva do direito fundamental à proteção de dados pessoais: perfilamento e microdirecionamento de propaganda político-eleitoral digital por provedores de aplicação de internet. Rio de Janeiro: Lumen Juris, 2025.

FRAZÃO, Ana. Função social da empresa: repercussões sobre a responsabilidade civil de controladores e administradores de S/As. Rio de Janeiro: Renovar, 2011.

FRAZÃO, Ana. Parecer: dever geral de cuidado das plataformas diante de crianças e adolescentes. São Paulo: Instituto Alana, 2021. Disponível em: https://alana.org.br/wp-content/uploads/2022/11/Parecer-Ana-Frazao.pdf. Acesso em: 10 dez. 2025.

ÍNDIA. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Índia: Ministry of Electronics and Information Technology, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Acesso em: 10 dez. 2025.

JUNQUILHO, Tainá Aguiar et al. (Org.). Construindo consensos: deep fakes nas eleições de 2024 relatório das decisões dos TREs sobre deep fakes. Brasília: Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa: Laboratório de Governança e Regulação de Inteligência Artificial, 2024.

MARTINS-COSTA, Judith. A boa-fé no direito privado: critérios para sua aplicação. 2. ed. São Paulo: Saraiva Educação, 2019.

MENKE, Fabiano; GOULART, Guilherme Damasio. Segurança da informação e vazamento de dados. In: DONEDA, Danilo; MENDES, Laura Schertel; RODRIGUES JR, Otávio Luiz; SARLET, Ingo Wolfgang (Coord.), BIONI, Bruno (Coord. Executivo). Tratado de proteção de dados pessoais. 1. ed. Rio de Janeiro: Forense, 2021.

REINO UNIDO. Online Safety Act (OSA). Londres, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 10 dez. 2025.

TEPEDINO, Gustavo. Notas sobre a função social dos contratos. In: TEPEDINO, Gustavo. Temas de direito civil, t. III. Rio de Janeiro: Renovar, 2009.

UNIÃO EUROPEIA. Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Bruxelas, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. Acesso em: 10 dez. 2025.

WOODS, Lorna; PERRIN, William. Online harm reduction: a statutory duty of care and regulator. Carnegie UK Trust, Reino Unido, abr. 2019. Disponível em: https://carnegieuk.org/publication/online-harm-reduction-a-statutory-duty-of-care-and-regulator/. Acesso em: 10 dez. 2025.

PARTE II - ANÁLISE DOS DEVERES IMPOSTOS AOS PROVEDORES DE APLICAÇÃO DE INTERNET PELA RESOLUÇÃO TSE N. 23.610/2019, COM A ATUALIZAÇÃO DA RESOLUÇÃO TSE N. 23.732/2024

2.1 ADEQUAÇÃO DE POLÍTICAS E DOCUMENTOS (ART. 9º-D, I)

Stefani Juliana Vogel

> **Art. 9º-D. É dever do provedor de aplicação de internet, que permita a veiculação de conteúdo político-eleitoral, a adoção e a publicização de medidas para impedir ou diminuir a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam atingir a integridade do processo eleitoral, incluindo:**
> **I - a elaboração e a aplicação de termos de uso e de políticas de conteúdo compatíveis com esse objetivo.**
> **[...]**

2.1.1 VISÃO GERAL E OBJETIVOS

Objetivo: O art. 9º-D, inciso I, introduzido pela Resolução TSE n.º 23.732/2024, estabelece como dever dos provedores de aplicação de internet a "elaboração e aplicação de termos de uso e de políticas de conteúdo compatíveis" com o objetivo de impedir ou diminuir a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam atingir a integridade do processo eleitoral".

A norma pretende alinhar a arquitetura contratual e procedimental das plataformas (termos, políticas e fluxos internos) ao interesse público eleitoral, impondo-lhes deveres de coerência normativa e efetividade operacional. Em outras palavras, o dispositivo não exige apenas a existência de regras escritas, mas sua adequação material e funcional ao objetivo de proteger a integridade informacional do pleito.

Guia de Perguntas:

1) Os termos de uso e as políticas de conteúdo mencionam, de forma expressa, a proteção à integridade do processo eleitoral?

2) As empresas demonstram como aplicam essas políticas e documentos (manuais internos, equipes, logs, procedimentos de revisão humana)?

3) As regras são comunicadas de forma clara aos usuários?

4) As medidas previstas visam impedir ou reduzir (não apenas reagir) à circulação de conteúdos inverídicos ou descontextualizados?

5) As plataformas mantêm registro público (transparência ativa) das ações tomadas com base nessas regras?

6) O conteúdo das políticas cita ou se harmoniza com os memorandos de entendimento firmados com a Justiça Eleitoral em 2024?

21.2 BASE NORMATIVA (BRASIL)

TSE Res. 23.732/2024, Art. 9º-D, inciso I: o caput do dispositivo estabelece que é dever do provedor de aplicação "a adoção e a publicização de medidas para impedir ou diminuir a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam atingir a integridade do processo eleitoral", incluindo, no inciso I, "a elaboração e a aplicação de termos de uso e de políticas de conteúdo compatíveis com esse objetivo"

Contexto regulatório adjacente: O TSE firmou, em 2024, memorandos de entendimento com plataformas digitais (Meta, Google, TikTok, X, YouTube e outros), estabelecendo canais de resposta prioritária e planos de contingência contra desinformação. Esses instrumentos materializam o dever de "adequação de políticas e documentos" e podem ser considerados evidência de conformidade ao inciso I (Brasil, 2024a).

O Supremo Tribunal Federal, no RE 1.037.396 (Tema 987) e no RE 1.057.258 (Tema 533), julgados em junho de 2025, estabeleceu que plataformas podem ser responsabilizadas independentemente de ordem judicial prévia quando se omitem diante de conteúdos manifestamente ilícitos, como discursos de ódio, incitação à violência ou manipulação dolosa da informação (Brasil, 2025). A decisão redefiniu o alcance do art. 19 do Marco Civil da Internet, impondo dever de diligência reforçada e políticas preventivas, parâmetros que se refletem diretamente no art. 9º-D, I.

Além disso, em dezembro de 2023, o STF confirmou a constitucionalidade da resolução do TSE voltada ao combate à desinformação, reconhecendo a competência normativa da Justiça Eleitoral para regular condutas em plataformas digitais durante o pleito (Brasil, 2024b).

Esse conjunto jurisprudencial sustenta que os termos de uso e políticas devem ser projetados para a prevenção, e não apenas para a reação, a conteúdos potencialmente danosos à lisura eleitoral.

21.3 METODOLOGIA DE *BENCHMARKING*

Seleção de jurisdições: UE (DSA + diretrizes eleitorais), Reino Unido (*Online Safety Act* + códigos/guia da Ofcom) e Índia (*IT Rules*/2021 e alterações).

Unidades de comparação: Os critérios abaixo derivam diretamente do inciso I (elaboração e aplicação) e são agrupados em 5 eixos:

1) Clareza normativa (texto): o grau de precisão, transparência e inteligibilidade dos termos de uso e políticas de conteúdo aos usuários em relação a conteúdos falsos ou manipulados podem afetar as eleições.

2) Aplicação e coerência procedimental: propõe-se verificar se as plataformas executam o que está escrito nos documentos.

3) Fluxo e prazos: para avaliar se as normas internas das plataformas (termos, políticas de moderação e relatórios) fixam tempos definidos para agir diante de conteúdo ilícito

ou desinformativo, responder denúncias e rever decisões.

4) Transparência: mede a presença de seções públicas ou relatórios periódicos com dados sobre moderação eleitoral, número de remoções, critérios.
Revisão e *accountability* textual: verificar se há compromissos de revisão dos documentos antes de eleições ou após auditorias.

Critério	União Europeia - Digital Service Act (DSA)*	Reino Unido - *Online Safety Act* (OSA)	Índia – *IT Rules* 2021
Clareza normativa (texto)	Art. 14 (DSA) - Terms and conditions (DSA): Determina que os provedores de serviços intermediários indiquem de forma clara, compreensível e não-discriminatória suas políticas de moderação, critérios para remoção e restrição de conteúdos, e como esses critérios são aplicados. Devem respeitar direitos fundamentais, especialmente liberdade de expressão e informação. Corresponde ao dever de elaborar termos e políticas de conteúdo claras e compatíveis com o objetivo público (no caso brasileiro, integridade eleitoral). Ambos exigem coerência textual e previsibilidade das regras internas.	SS. 71 e 72 OSA: Provedores de grandes serviços ("Category 1 services") devem: a) agir exclusivamente conforme os termos de serviço, não podendo remover conteúdo, restringir acesso ou banir usuários fora das regras explicitadas nesses documentos; b) redigir tais termos de forma "clara e acessível", detalhando políticas, tecnologias proativas de moderação e critérios de bloqueio.	Rule 3(1)(a)-(b) exige que o intermediário publique, de forma proeminente, em seu site ou aplicativo, as regras, políticas de privacidade e termos de uso, em inglês ou em qualquer idioma listado no Anexo VIII da Constituição indiana, na língua escolhida pelo usuário. Os termos devem informar claramente o que é proibido, inclusive informações falsas, enganosas ou identificadas como "fake" pelo governo (3(1)(b)(v)).

Aplicação e coerência procedimental	Art. 20 (DSA) - Sistema interno de gestão de reclamações: As plataformas devem manter um sistema interno eficaz para receber e tratar reclamações de usuários contra decisões de moderação, de forma atempada, não discriminatória, diligente e não arbitrária, revogando decisões infundadas "sem demora injustificada" Art. 22, n.º 1 (DSA) - Sinalizadores de confiança (trusted flaggers): As plataformas devem adotar "medidas técnicas e organizativas necessárias" para garantir que notificações de sinalizadores de confiança sejam prioritárias e decididas sem demora indevida. Art. 37 (DSA) - Auditoria independente anual: As VLOPs e VLOSEs estão sujeitas a auditorias independentes anuais, a expensas próprias, para avaliar o cumprimento das obrigações do Regulamento, devendo cooperar plenamente e garantir acesso a dados e instalações. Art. 35 (DSA) - Medidas de mitigação de riscos sistêmicos: Obriga as VLOPs/VLOSEs a adotar "medidas apropriadas, proporcionais e eficazes" para mitigar riscos identificados (inclusive impactos sobre processos eleitorais) dentro de prazos razoáveis. Art. 14(6) (DSA) - aplicação diligente: As restrições nos termos devem ser aplicadas de modo diligente, objetivo e não-discriminatório.	§ 71(1)-(2): impõe o dever de operar "proportionate systems and processes" para garantir que as ações de moderação sejam consistentes com os termos; o § 72 reforça a obrigação de aplicar tais disposições de modo coerente e não discriminatório.	Rule 3(1)(c)-(d) e Rule 4(8) determinam que a plataforma aplique seus termos de modo coerente, inclusive informando ao usuário os motivos de remoção de conteúdo e oferecendo oportunidade de contestação antes da exclusão definitiva. Há também o dever de conservar os registros e cooperar com autoridades (Rule 3(1)(g)-(j)).
Fluxo e prazos	Art. 16 (DSA) - mecanismo de notificação e ação (notice-and-action): mpõe que as plataformas disponibilizem mecanismos eficazes para receber notificações de conteúdos ilegais e atuem "sem demora indevida" após recebê-las, comunicando as decisões às partes envolvidas. Art. 20 (DSA) - sistema interno de tratamento de reclamações: cria a obrigação de um sistema interno e gratuito de tratamento de reclamações, para contestar decisões de moderação, devendo o processo ser conduzido de forma diligente, não arbitrária e em prazo razoável.	§ 160 e o § 159 determinam que a OFCOM publique relatórios anuais avaliando se os provedores respondem a denúncias e reclamações de maneira clara, fácil e "timely" (em tempo razoável).	Rule 3(2)(a): o Grievance Officer deve reconhecer a reclamação em 24 h e resolvê-la em até 15 dias, e em casos de conteúdo sensível (como nudez ou deepfakes), remover em até 72 h. Rule 3(2)(b): exige mecanismo técnico de denúncia e rastreio do status da reclamação.

Revisão e *accountability* textual	Art. 14 (2) (DSA) - Revisão e atualização dos termos e condições: dever de informam os destinatários do serviço de quaisquer alterações significativas dos termos e condições. Art. 37 (DSA) - Accountability pós-auditoria: As plataformas devem submeter-se a auditorias independentes anuais para avaliar o cumprimento do presente regulamento [...] e publicar um relatório de auditoria e um plano de ação corretiva. Considerando 87 (DSA): Determina que VLOPs e VLOSEs adaptem e apliquem os seus termos e condições e ajustem seus fluxos internos e processos de moderação, garantindo rapidez e qualidade no tratamento de notificações.	O § 34 e o § 47-49 impõem à OFCOM revisar códigos de prática e exigir que plataformas mantenham políticas atualizadas, coerentes com os resultados de auditorias e avaliações de risco. Além disso, o § 164 autoriza a OFCOM a publicar relatórios sobre segurança on-line e conformidade, fortalecendo a prestação de contas periódica.	Rule 3(1)(f): o intermediário deve informar periodicamente - ao menos uma vez por ano - sobre alterações de suas políticas, reforçando a atualização textual. Rule 4(4): exige revisão humana periódica das ferramentas automatizadas de moderação para verificar viés e precisão, com relatório de resultados. Rule 4(9): o governo pode solicitar informações adicionais e relatórios sobre conformidade.

* Communication C/2024/3014 – Guidelines for VLOPs and VLOSEs on the application of the DSA in the electoral context (União Europeia, 2024).

2.1.4 BENCHMARK INTERNACIONAL (SÍNTESE COMPARATIVA)

União Europeia (UE)

DSA com Diretrizes eleitorais (União Europeia, 2024) impõe avaliação/mitigação de riscos sistêmicos em contexto eleitoral e medidas proporcionais, além de relato público de resultados. A arquitetura textual europeia fornece o *benchmark* mais direto para avaliar o cumprimento do art. 9º-D, I da Resolução TSE 23.732/2024, que exige termos e políticas compatíveis com a integridade informacional do processo eleitoral, ou seja, compreensíveis, previsíveis e publicamente verificáveis.

Communication C/2024/3014 – Guidelines for VLOPs and VLOSEs on the application of the DSA in the electoral context

Interpreta os arts. 34-35 e exige que, antes e durante eleições, as plataformas adaptem seus termos de serviço e planos de mitigação para preservar a integridade dos pleitos; prevê cooperação com autoridades eleitorais e relatórios pré-eleitorais. É o espelho mais direto do art. 9º-D, I: impõe a obrigação de ajustar políticas e termos de uso à finalidade de proteger a integridade eleitoral (União Europeia, 2024).

Reino Unido (RU)

Online Safety Act (OSA/2023) e guias/códigos da Ofcom consolidam deveres de cuidado, avaliações de risco, transparência e *enforcement* escalável (multas até 10% do faturamento global). Disposições que se relacionam com o art. 9º-D, I da Resolução TSE 23.732/2024: §§ 71-72 – dever de termos claros e acessíveis; §§ 71-72 – proibição de agir fora dos termos; proporcionalidade; §§ 159-160 – relatórios sobre resposta *"timely"*; § 77 – relatórios anuais públicos; §§ 34, 47, 164 – revisão de códigos e relatórios periódicos (Reino Unido, 2023).

Índia (Sul Global)

IT Rules/2021 (Intermediary Guidelines & Digital Media Ethics Code) configura o paradigma do Sul Global mais próximo do modelo brasileiro: combinam obrigações de clareza textual, celeridade, transparência periódica e responsabilização pública; exigem governança de políticas internas semelhante à corregulação brasileira (TSE - plataformas); reforçam que o documento (termos/políticas) é um instrumento regulatório, não apenas contratual, devendo ser atualizado, claro e verificável (Índia, 2021).

21.5 INTERPRETAÇÃO DO ART. 9º-D, I (PROPOSTAS)

Os termos e políticas exigidos pelo art. 9º-D, I devem ser compreendidos não apenas como cláusulas contratuais, mas como instrumentos de governança democrática, com função regulatória delegada. Assim, o TSE pode exigir:

- linguagem acessível e inteligível, inclusive em português claro e não jurídico;
- publicação permanente e rastreável (versões anteriores arquivadas);
- seções específicas de integridade eleitoral, em destaque e com glossário próprio.

Efeito prático: o termo de uso passa a ter função normativa pública, permitindo responsabilização por descumprimento.

O inciso I deve ser lido em conjunto com o dever implícito de execução diligente e não-discriminatória. O TSE, ao fiscalizar, deve exigir evidências de aplicação coerente, tais como:
relatórios de moderação específicos sobre conteúdos eleitorais;

- comprovação de que decisões seguiram critérios objetivos e previamente divulgados;
- registro de eventuais exceções e suas justificativas.

Efeito prático: a obrigação de "elaborar e aplicar" torna-se verificável, evitando políticas meramente declarativas (paper compliance).

A compatibilidade exigida pelo art. 9º-D, I inclui também adequação temporal: políticas de integridade eleitoral devem conter SLA normativo, isto é, prazos máximos de resposta para:

- denúncias de desinformação verificadas;

- comunicações oficiais do TSE;
- apelações de usuários.

Efeito prático: o TSE pode interpretar que a ausência de prazos definidos nos termos caracteriza descumprimento parcial do inciso I.

O inciso I não autoriza censura preventiva: sua execução deve observar proporcionalidade, transparência e revisão. Toda política compatível deve incluir:

- critérios de proporcionalidade na moderação;
- mecanismos de recurso e contestação;
- auditoria independente de equívocos ou excessos.

Efeito prático: o TSE consolida uma interpretação compatibilizadora, evitando abusos de moderação e garantindo legitimidade democrática.

2.1.6 EVIDÊNCIAS E ESTUDOS DE CASO

Acordos do TSE com plataformas digitais

O TSE firmou, em agosto de 2024, memorandos de entendimento com plataformas para "combater mentiras nas Eleições 2024". As plataformas se comprometeram a colaborar, adotar providências e agir com transparência. Esse tipo de acordo funciona como mecanismo de corregulação indireta: obriga práticas (termos, moderação, relatórios) de modo informal, mas vinculado ao regime eleitoral (Brasil, 2024a).

Sistema de Alertas de Desinformação Eleitoral (Siade/SIADE)

O TSE mantém um sistema onde cidadãos podem denunciar fatos notoriamente inverídicos ou descontextualizados ao órgão eleitoral. Esse sistema atua como canal de interlocução institucional, força uma resposta ou verificação pública, o que se aproxima do dever de aplicação de políticas compatíveis (Brasil, [202-?]b).

Decisão do STF sobre a resolução do TSE não configurar censura prévia

No STJ/STF houve manifestação de que a norma do TSE para combate à desinformação (em especial os acordos ou resoluções) não configura censura prévia automática, o que indica que o STF reconheceu algum grau de controle e compatibilidade do TSE com liberdade de expressão (Brasil, [202-?]a).

Estudo acadêmico sobre desinformação nas eleições de 2022

Estudo recente avaliou as *"misinformation claims"* durante as eleições de 2022 no Brasil em plataformas como WhatsApp, Twitter e Kwai, examinando como o TSE utilizou *chatbots, tiplines* e linkagem a checagens de fatos para mitigar esses fluxos (Hale et al., 2024).

Esse tipo de evidência empírica demonstra que o TSE já atua no que poderíamos chamar de aplicação tácita de políticas de integridade informacional, ainda que não citando formalmente o art. 9º-D, I.

21.7 RECOMENDAÇÕES (NORMATIVAS E OPERACIONAIS)

Transformar termos e políticas em instrumentos de governança pública

O TSE deve editar orientação interpretativa reconhecendo que termos de uso e políticas de conteúdo constituem documentos regulatórios - e não meramente contratuais.
Estabelecer requisitos mínimos de conteúdo das políticas eleitorais

Por resolução ou instrução complementar, definir elementos mínimos que devem constar dos termos de uso:

- regras sobre tratamento de *deepfakes* e conteúdos sintéticos;
- protocolos de rotulagem e checar fatos;
- prazos de resposta a alertas oficiais do TSE;
- canais de apelação e revisão de moderação.

Incluir obrigação de revisão pré-eleitoral e pós-pleito das políticas

Determinar que, até 60 dias antes do pleito, as plataformas enviem ao TSE e divulguem publicamente uma atualização ou relatório de integridade eleitoral, com ajustes de termos e processos; e, até 60 dias após, divulguem relatório avaliativo com dados de impacto e planos de melhoria.

Criação de painel público de integridade digital

Instrumento desejável de transparência ativa e centralizada reunindo relatórios, termos e estatísticas das plataformas, com atualização em tempo real durante as eleições.

21.8 RISCOS, SALVAGUARDAS E DIREITOS

Riscos

Categoria	Descrição	Exemplos concreto	Consequências
Risco de censura indevida	Aplicação desproporcional ou automatizada de filtros, removendo críticas legítimas ou sátiras.	Moderação automática com IA que rotula ironias como desinformação.	Violação à liberdade de expressão e ao debate público.
Risco de omissão das plataformas	Políticas genéricas ou ineficazes que não previnem a circulação de conteúdo sabidamente falso.	Falta de seções específicas sobre integridade eleitoral nos termos de uso.	Aumento da desinformação e impacto na confiança do processo.
Risco de captura política ou uso instrumental	Pressões externas que direcionem a moderação para favorecer determinado grupo.	Remoção seletiva de conteúdos por denúncias coordenadas.	Violação da isonomia eleitoral e abuso de poder informacional.
Risco de opacidade e falta de prestação de contas	Falta de transparência sobre critérios de remoção, algoritmos e decisões automatizadas.	Relatórios incompletos ou sem dados de tempo médio de resposta.	Impossibilidade de auditoria pública ou científica.
Risco de discriminação algorítmica	Sistemas automatizados que priorizam certos conteúdos por viés de treinamento.	Algoritmos que amplificam narrativas polarizadoras.	Reforço de estigmas, polarização e manipulação cognitiva.
Risco de insegurança jurídica	Ausência de parâmetros claros sobre o dever de compatibilidade e sua fiscalização.	Divergência de interpretações sobre o alcance do art. 9º-D, I.	Incerteza para plataformas e instabilidade regulatória.

Salvaguardas

Tipo	Base normativa	Mecanismo proposto	Finalidade
Salvaguarda procedimental	DSA art. 14(5-6); ***Online Safety Act*** § 72	Exigir notificação prévia ao usuário e direito de recurso em caso de remoção de conteúdo eleitoral.	Garantir contraditório e proporcionalidade.
Salvaguarda temporal	*IT Rules* 2021 Rule 3(2)(a)	Definir prazos diferenciados (24 h, 72 h, 15 dias) e fluxos documentados de resposta.	Evitar omissões e atrasos que prejudiquem o debate.
Salvaguarda de transparência ativa	DSA arts. 15 e 23	Publicação periódica de relatórios de moderação eleitoral com dados e metodologia.	Assegurar controle público e científico.
Salvaguarda de revisão e auditoria	DSA arts. 35 e 37	Prever revisões pré e pós-eleitorais dos termos e auditorias independentes.	Garantir coerência e atualização das políticas.
Salvaguarda de proporcionalidade e liberdade de expressão	DSA art. 63; Constituição art. 5º, IV e IX	Avaliar impacto das medidas de moderação sobre o discurso legítimo.	Evitar censura e assegurar pluralismo.
Salvaguarda de cooperação institucional	Res. TSE 23.732/2024 arts. 9º-E e 9º-F	Estabelecer canais diretos e protocolos de resposta entre plataformas e o TSE.	Reforçar corregulação e rapidez em casos críticos.

REFERÊNCIAS

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade n.º 7.261. Relator: Min. Edson Fachin. Brasília, DF, 2024b. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6507787. Acesso em: 10 dez. 2025.

BRASIL. Supremo Tribunal Federal. Informação à sociedade: RE 1.037.396 (Tema 987) e 1.057.258 (Tema 533) responsabilidade de plataformas digitais por conteúdo de terceiros. Brasília: STF, 2025. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/Informac807a771oa768SociedadeArt19MCI_vRev.pdf. Acesso em: 10 dez. 2025.

BRASIL. Supremo Tribunal Federal. STF confirma validade de norma do TSE voltada ao combate à desinformação durante processo eleitoral. Brasília, DF: Notícias STF, [202-?]a. Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-confirma-validade-de-norma-do-tse-voltada-ao-combate-a-desinformacao-durante-processo-eleitoral/. Acesso em: 10 dez. 2025.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 2019. Dispõe sobre propaganda eleitoral. Brasília, DF, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 10 dez. 2025

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 2024. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Brasília, DF, 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 10 dez. 2025.

BRASIL. Tribunal Superior Eleitoral. Confira a íntegra dos acordos com plataformas digitais para combater mentiras nas Eleições 2024. Brasília, DF: Notícias TSE, 2024a. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Agosto/confira-a-integra-dos-acordos-com-plataformas-digitais-para-combater-mentiras-nas-eleicoes-2024-1. Acesso em: 10 dez. 2025.

BRASIL. Tribunal Superior Eleitoral. Sistema de Alertas Eleições. Brasília, DF, [202-?]b. Disponível em: https://www.tse.jus.br/eleicoes/sistema-de-alertas. Acesso em: 10 dez. 2025.

COMISSÃO EUROPEIA. Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065. Official Journal of the European Union, [S. l.], 2024. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403014. Acesso em: 10 dez. 2025.

HALE, Scott A. et al. Fighting misinformation during the Brazilian elections: evidence from the 2022 fact-checking ecosystem. arXiv [preprint], 2024. Disponível em: https://arxiv.org/abs/2401.02395. Acesso em: 10 dez. 2025.

ÍNDIA. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Índia: Ministry of Electronics and Information Technology, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Acesso em: 10 dez. 2025.

OFCOM. Protecting people from illegal harms online: statement & codes. Londres: Ofcom, 2024. Disponível em: https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/statement-protecting-people-from-illegal-harms-online. Acesso em: 10 dez. 2025.

OFCOM. Transparency reporting: consultation (2024–2025) e Final Transparency Guidance (21 jul. 2025). Londres: Ofcom, 2025. Disponível em: https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/transparency-reporting. Acesso em: 10 dez. 2025.

PRESS INFORMATION BUREAU. IT Rules & misinformation/deepfakes. Índia: Press Information Bureau, 2024. Disponível em: https://pib.gov.in. Acesso em: 10 dez. 2025.

REINO UNIDO. Online Safety Act (OSA). Londres, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 10 dez. 2025.

REINO UNIDO. Online Safety Act: explainer. Londres: Gov.uk, [2025?]. Disponível em: https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Bruxelas, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. Acesso em: 10 dez. 2025.

2.2 ADOÇÃO E PUBLICIZAÇÃO DE MEDIDAS PARA IMPEDIR OU DIMINUIR A CIRCULAÇÃO DE FATOS NOTORIAMENTE INVERÍDICOS OU GRAVEMENTE DESCONTEXTUALIZADOS QUE POSSAM ATINGIR A INTEGRIDADE DO PROCESSO ELEITORAL (ART. 9º-D)

Bárbara Pontalti

Art. 9º-D. É dever do provedor de aplicação de internet, que permita a veiculação de conteúdo político-eleitoral, a adoção e a publicização de medidas para impedir ou diminuir a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam atingir a integridade do processo eleitoral, incluindo:
I - a elaboração e a aplicação de termos de uso e de políticas de conteúdo compatíveis com esse objetivo;
II - a implementação de instrumentos eficazes de notificação e de canais de denúncia, acessíveis às pessoas usuárias e a instituições e entidades públicas e privadas;
III – o planejamento e a execução de ações corretivas e preventivas, incluindo o aprimoramento de seus sistemas de recomendação de conteúdo;
IV - a transparência dos resultados alcançados pelas ações mencionadas no inciso III do caput deste artigo;
V – a elaboração, em ano eleitoral, de avaliação de impacto de seus serviços sobre a integridade do processo eleitoral, a fim de implementar medidas eficazes e proporcionais para mitigar os riscos identificados, incluindo quanto à violência política de gênero, e a implementação das medidas previstas neste artigo;
VI – o aprimoramento de suas capacidades tecnológicas e operacionais, com priorização de ferramentas e funcionalidades que contribuam para o alcance do objetivo previsto no caput deste artigo.
[...]

2.2.1 VISÃO GERAL E OBJETIVOS

Objetivo: analisar o alcance jurídico e prático dos deveres de adoção e publicização de medidas voltadas à contenção de fatos notoriamente inverídicos ou gravemente descontextualizados no contexto eleitoral, previstos no *caput* do art. 9º-D da Resolução.

Ressalta-se que esta pesquisa tem como foco central as medidas voltadas à prevenção e à redução da desinformação eleitoral, conforme o *caput* do dispositivo, sendo os incisos correspondentes objeto de análise por outros pesquisadores.

Guia de Perguntas:

1) Qual o alcance normativo do dever de adoção e publicização de medidas previsto no caput do art. 9º-D?

2) De que forma as medidas adotadas podem ser publicizadas e comunicadas ao público e às autoridades, e quais parâmetros de transparência e *accountability* poderiam ser incorporados à norma brasileira?

3) Quais lacunas persistem na regulamentação brasileira e quais aprimoramentos normativos e operacionais podem ser sugeridos, à luz das boas práticas internacionais,

para fortalecer a integridade informacional do processo eleitoral?

4) Existem mecanismos eficazes de auditoria interna e supervisão externa capazes de verificar o cumprimento dessas medidas pelas plataformas?

2.2.2 BASE NORMATIVA (BRASIL)

TSE Res. 23.610, Art. 9º-D, *caput* – Impõe aos provedores de aplicação de internet que permitam a veiculação de conteúdo político-eleitoral o dever de adotar e publicizar medidas eficazes para impedir ou reduzir a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam comprometer a integridade do processo eleitoral (Brasil, 2019b). Em outras palavras, o dispositivo cria uma obrigação ativa e transparente para as plataformas digitais: elas não podem permanecer inertes diante da desinformação eleitoral, devendo implementar mecanismos preventivos e corretivos (e dar visibilidade a essas ações) de modo a assegurar um ambiente informacional mais íntegro, confiável e compatível com os direitos fundamentais e com o pleito democrático.

Contexto regulatório adjacente: A Constituição Federal de 1988, em seu artigo 170, consagra o princípio da função social na ordem econômica, de modo que as empresas que atuam no Brasil devem orientar suas atividades para a obtenção de benefícios para a coletividade (Brasil, 1988).

No campo infraconstitucional, o Código Civil de 2002 estabelece, em seu artigo 421, que a liberdade contratual deve respeitar a função social do contrato, reforçando o equilíbrio entre autonomia privada e interesse coletivo (Brasil, 2002).

Posteriormente, o Marco Civil da Internet (Lei n.º 12.965/2014), principal diploma legal sobre o uso da internet no Brasil, surgiu com o propósito de reafirmar a finalidade social da rede (art. 2º, VI) (Brasil, 2014). Além disso, determinou que os agentes devem ser responsabilizados de acordo com suas atividades (art. 3º, VI) e reconheceu a internet como instrumento de promoção do desenvolvimento humano, econômico, social e cultural (art. 6º).

O artigo 19 do MCI previa que os provedores de aplicação somente poderiam ser responsabilizados por danos decorrentes de conteúdo gerado por terceiros mediante descumprimento de ordem judicial específica. Contudo, o STF declarou a parcial inconstitucionalidade do dispositivo, entendendo que a exigência de decisão judicial prévia deve ser ponderada conforme o caso concreto. Dessa forma, a Suprema Corte consolidou um entendimento que amplia o dever de cuidado das plataformas e reconhece a eficácia de notificações extrajudiciais em certas hipóteses.

Diante da gravidade da desinformação no contexto eleitoral, o TSE estabeleceu, por meio da Resolução n.º 23.714 de 2022, diretrizes específicas para enfrentar a disseminação de conteúdos inverídicos que comprometam a integridade do processo eleitoral. A norma prevê a remoção imediata de conteúdo pelas redes sociais, mediante decisão fundamentada, com multa entre R$ 100 mil e R$ 150 mil por hora em caso de descumprimento (art. 2º), evidenciando a preocupação com a atuação das plataformas digitais.

Além disso, o art. 4º da Resolução determina que a produção sistemática de desinformação autoriza a suspensão temporária de perfis, contas ou canais mantidos em mídias sociais.

Ademais, destacam-se iniciativas institucionais complementares, como o Programa Permanente de Enfrentamento à Desinformação (PPED), criado pelo TSE em 2021; o Centro Integrado de Enfrentamento à Desinformação e Defesa da Democracia (CIEDDE), instituído em 2024 para promover a cooperação entre a Justiça Eleitoral, órgãos públicos e plataformas digitais; e o Sistema de Alertas de Desinformação Eleitoral (SIADE), que permite o envio de denúncias por cidadãos. O STF, por sua vez, mantém o Programa de Combate à Desinformação, voltado a ações educativas, checagem de fatos e articulação institucional.

2.2.3 METODOLOGIA DE *BENCHMARKING*

- **Seleção de jurisdições: UE (DSA), Reino Unido (OSA), Índia (*IT Rules*).**

- **Unidades de comparação (possíveis critérios):**

    - dever de medidas proativas e de mitigação de riscos: esta unidade examina o dever das plataformas de implementar políticas internas destinadas a prevenir ou reduzir a disseminação de desinformação eleitoral, antes mesmo de qualquer determinação judicial.

    - estruturas internas de governança e auditoria: esta unidade avalia a existência de mecanismos internos de supervisão e verificação, como programas de compliance, auditorias internas e funções corporativas responsáveis por garantir a conformidade com as normas eleitorais.

    - cooperação e comunicação institucional com autoridades estatais: observa como os marcos comparados estruturam a cooperação entre plataformas e órgãos públicos, especialmente em contextos eleitorais e de integridade informacional.

    - publicização, transparência e relatórios de impacto: trata da forma como as medidas adotadas são comunicadas ao público e às autoridades. Examina também a qualidade e a compreensibilidade das informações publicizadas, verificando se os regimes analisados impõem formatos padronizados e linguagem acessível, por exemplo.

	União Europeia - *Digital Service Act* (DSA)	Mecanismo proposto	Finalidade
Publicização, transparência e relatórios de impacto	Art. 34, 1, c + Considerando 82: definem os riscos sistêmicos relevantes, incluindo "efeitos negativos reais ou previsíveis nos processos democráticos, no discurso cívico e nos processos eleitorais, bem como na segurança pública". Art. 35: Determina que as VLOPs/VLOSEs adotem medidas razoáveis, proporcionadas e eficazes, adaptadas aos riscos identificados no art. 34º, incluindo: - Adaptação de interfaces e termos e condições; - Melhoria de processos de moderação e sistemas algorítmicos; - Ajustes em sistemas de publicidade; - Cooperação com sinalizadores de confiança, códigos de conduta e protocolos de crise; - Medidas de sensibilização e informação ao público.	Em sua introdução, o OSA adota o princípio do *safe by design*, o qual exige que os serviços sejam projetados e operados reduzindo riscos antes de sua ocorrência. Seção 2: impõe obrigações específicas às plataformas que permitem interação entre usuários, prevenindo a circulação de conteúdos ilegais. Expressa a exigência de atuação proativa. Seção 9: impõe às plataformas o dever de realizar avaliações de risco, base para o exercício responsável do *duty of care.* Seção 10: complementa a anterior, detalhando o dever de implementar medidas de mitigação proporcionais. Seção 17: Estabelece deveres de proteger conteúdos de importância democrática. É esclarecida a necessidade de sistemas e processos proporcionais, designados para assegurar a liberdade de expressão de conteúdos democráticos. Esses sistemas e processos devem ser aplicados de maneira semelhante para opiniões políticas diversas.	A Rule 1 determina que os intermediários devem impedir a disseminação de informações falsas ou enganosas, incluindo aquelas que induzam o destinatário a erro sobre a origem da mensagem ou que sejam patentemente falsas ou não verdadeiras. Essa regra não trata apenas de diligência reativa, mas de gestão e mitigação de riscos estruturais. Rule 3: consolida o núcleo do dever de diligência, ao exigir que intermediários cumpram padrões de transparência, informem usuários suas regras de uso e utilizem-se de esforços razoáveis para que estes não publiquem informações de diversos tipos, incluindo desinformação ou conteúdo incorreto, inverídico ou falso, ou verificada como falsa pelo Governo. Rule 4: determina que os intermediários devem empregar ferramentas tecnológicas para identificar proativamente conteúdo de estupro, abuso sexual infantil ou idêntico a material previamente removido. A Rule 4 também exige que o intermediário implemente mecanismos para supervisão humana apropriada e uma revisão periódica das ferramentas automatizadas (avaliando precisão, imparcialidade, vieses e impacto na privacidade/segurança).

Estruturas internas de governança e auditoria	Art. 37: exige que as VLOPs e VLOSEs sejam submetidas, às suas próprias expensas e ao menos uma vez ao ano, a auditorias independentes sobre o cumprimento das obrigações legais, incluindo mitigação de riscos e políticas de transparência. Art. 41: determina que os fornecedores de VLOPs e VLOSEs instituam uma Função de Verificação da Conformidade independente das suas funções operacionais. Os responsáveis por essa função devem: - Organizar e supervisionar as atividades relacionadas às auditorias independentes (art. 37.º); - Assegurar a identificação e comunicação de todos os riscos sistêmicos (art. 34.º) e garantir a adoção de medidas de mitigação razoáveis, proporcionadas e eficazes (art. 35.º); - Informar e aconselhar a direção e os funcionários quanto às obrigações decorrentes do DSA, monitorar o cumprimento dessas obrigações e acompanhar os compromissos assumidos nos códigos de conduta e protocolos de crise. Art. 45: valoriza os códigos de conduta como instrumentos que auxiliam na correta aplicação do regulamento, considerando os desafios de resposta aos diferentes tipos de conteúdos ilegais. Art. 48: preve a criação de protocolos de crise, voltados à coordenação de respostas rápidas e eficazes em situações excepcionais, reforçando o dever de cuidado ampliado das plataformas nesses contextos.	Seção 23: impõe o dever de manter registros detalhados das avaliações de risco, o que cria uma trilha de auditoria interna necessária à fiscalização posterior pela Ofcom. Seção 41: reconhece os códigos de conduta como instrumentos para estabelecer balizas e critérios de aplicação dos deveres de cuidado. Seções 104–105: tratam da possibilidade de a Ofcom determinar auditorias independentes (*reports by skilled persons*), o que reforça o eixo de governança.	A Rule 4 estabelece obrigações mais rigorosas para os significant social media intermediaries, exigindo a nomeação de três agentes responsáveis pelo cumprimento das normas: - um *Chief Compliance Officer*, residente na Índia e encarregado de assegurar a conformidade legal, respondendo pessoalmente em caso de descumprimento (Rule 4(1)(a)); - um *Nodal Officer,* disponível 24 horas por dia para comunicação direta com autoridades públicas (Rule 4(1)(b)); e - um *Resident Grievance Officer*, responsável pela gestão do sistema interno de reclamações (Rule 4(1)(c)). Rule 9(3): Estabelece o regime de governança de três níveis para garantir a adesão ao Código de Ética: Nível I (Autorregulação do Editor), Nível II (Órgão de Autorregulação) e Nível III (Mecanismo de Supervisão do Governo Central).

Cooperação e comunicação institucional com autoridades estatais	Art. 48: prevê a elaboração de protocolos de crise coordenados entre plataformas, autoridades competentes e a Comissão Europeia, destinados a responder a situações extraordinárias. O Art. 49º marca o início do Capítulo IV do DSA. Esta seção concentra-se nas estruturas e mecanismos necessários para a supervisão e o cumprimento do Regulamento, incluindo a cooperação entre as autoridades. Art. 49: dispõe que os Estados-Membros devem designar autoridades competentes e um coordenador dos serviços digitais, responsáveis pela supervisão dos prestadores de serviços intermediários e pela execução do DSA. Art. 50: determina que os coordenadores dos serviços digitais atuem de forma imparcial, transparente e independente. Art. 51: confere aos coordenadores dos serviços digitais poderes de investigação e requisição de informações junto às plataformas e a terceiros, permitindo a obtenção de dados necessários para avaliar o cumprimento das obrigações do DSA.	O OSA impõe um dever legal de cooperação e assistência das plataformas à Ofcom, autoridade responsável pela supervisão e aplicação da lei. Seção 100: autoriza a Ofcom a emitir avisos de informação (information notices), pelos quais pode exigir que os provedores forneçam quaisquer dados ou documentos necessários ao exercício das suas funções de regulação e fiscalização. Seção 104: determina que, quando a Ofcom iniciar uma investigação formal sobre eventual descumprimento de obrigações, o provedor deve cooperar integralmente com o processo, fornecendo todas as informações e esclarecimentos solicitados. Seção 107: permite que a Ofcom emita avisos de auditoria (audit notices), obrigando as plataformas a permitir a realização de auditorias destinadas a verificar se estão em conformidade com os requisitos aplicáveis. Em síntese, a cooperação com a Ofcom é mandatória e constitui parte essencial da governança regulatória do OSA, garantindo a transparência e a eficácia da supervisão pública sobre as plataformas digitais.	Ainda sobre o regime de governança de três níveis, destacam-se aqui: O Nível II (Rule 12) prevê um órgão de autorregulação, chefiado por um juiz aposentado ou pessoa eminente, responsável por supervisionar a observância do Código de Ética, orientar os publishers e apreciar recursos não resolvidos no Nível I. O Nível III (Rules 13 e 14) institui o mecanismo de supervisão governamental, coordenado pelo Ministério da Informação e Radiodifusão, que cria o Comitê Interdepartamental com representantes de vários Ministérios. Esse Comitê analisa queixas e pode recomendar medidas como advertências, pedidos de retratação ou remoção de conteúdo. Rule 14(1), (5): prevê a constituição de um Comitê Interdepartamental composto por representantes de diversos Ministérios, além de especialistas convidados. O Comitê se reúne periodicamente para analisar queixas relativas à violação do Código de Ética e formular recomendações ao Ministério, que podem incluir advertências, pedidos de retratação, inclusão de avisos ou a remoção ou modificação de conteúdo.

Publicização, transparência e relatórios de impacto	Art. 15: prevê a elaboração de relatórios anuais de transparência por todos os prestadores de serviços intermediários, contendo informações sobre o número de remoções de conteúdo, decisões automatizadas e demais medidas de moderação aplicadas. Art. 42: impõe às VLOPs e VLOSEs a publicação de relatórios semestrais reforçados, com dados detalhados sobre recursos humanos alocados à moderação, idiomas cobertos, indicadores de precisão, bem como a divulgação dos resultados das auditorias e avaliações de risco realizadas. Art. 40: assegura às autoridades competentes e pesquisadores independentes o acesso a dados necessários para fins de supervisão, investigação e avaliação de impacto das medidas adotadas pelas plataformas.	Seções 10 e 27: ambas tratam da transparência quanto aos riscos identificados pelas plataformas, mas em níveis distintos. Enquanto a Seção 10 exige que essas informações sejam resumidas nos termos de serviço, voltando-se à transparência informacional dirigida aos próprios usuários, a Seção 27 impõe a publicização ampla das conclusões da avaliação de risco, por meio de uma declaração pública, voltada à sociedade e às autoridades regulatórias. Seção 22: prevê a obrigação de publicar avaliações de impacto destinadas a analisar os efeitos das medidas de segurança sobre os direitos fundamentais dos usuários. Seção 77: determina que os provedores enviem relatórios de transparência à Ofcom e os tornem públicos, observando o formato e os prazos definidos pelo órgão regulador. Seção 159: impõe à Ofcom o dever de produzir e publicar relatórios próprios de transparência, com base nas informações recebidas dos provedores sob a Seção 77, consolidando e divulgando boas práticas e dados relevantes sobre o cumprimento das obrigações legais.	Rule 4(1)(d): Intermediários significativos devem publicar um relatório de compliance mensal, detalhando queixas recebidas e ações tomadas. Rule 19(1), (3): determinam que editores e órgãos de autorregulação façam divulgação completa e transparente das queixas recebidas e resolvidas, devendo ainda o editor preservar os registros do conteúdo transmitido por, no mínimo, sessenta dias, a fim de disponibilizá-los às autoridades quando solicitado.

2.2.4 BENCHMARK INTERNACIONAL (SÍNTESE COMPARATIVA)

União Europeia - DAS

Art. 15: impõe a todos os prestadores de serviços intermediários a elaboração de relatórios anuais de transparência, com informações sobre o número de conteúdos removidos, decisões automatizadas e demais medidas de moderação aplicadas.

Art. 34, 1, c + Considerando 82: definem os riscos sistêmicos relevantes, incluindo "efeitos negativos reais ou previsíveis nos processos democráticos, no discurso cívico e nos processos eleitorais, bem como na segurança pública".

Art. 35: determina que as VLOPs e VLOSEs adotem medidas razoáveis, proporcionadas e eficazes, adaptadas aos riscos identificados no art. 34º. Essas medidas compreendem:
a adaptação de interfaces e termos e condições;
o aperfeiçoamento de processos de moderação e de sistemas algorítmicos;
ajustes em sistemas de publicidade;
a cooperação com sinalizadores de confiança, adesão a códigos de conduta e protocolos de crise;
além da implementação de iniciativas de sensibilização e informação ao público.

Art. 37: impõe que as VLOPs e VLOSEs sejam submetidas, às suas próprias expensas e ao menos uma vez por ano, a auditorias independentes destinadas a avaliar o cumprimento das obrigações legais, especialmente quanto à mitigação de riscos e à transparência das políticas aplicadas.

Art. 40: assegura às autoridades competentes e pesquisadores independentes o acesso a dados essenciais para fins de supervisão, investigação e avaliação de impacto das medidas adotadas.

Art. 41: estabelece a obrigação de criação de uma Função de Verificação da Conformidade, independentemente das áreas operacionais da empresa. Os responsáveis por essa função devem:
organizar e supervisionar as atividades relacionadas às auditorias independentes (art. 37.º);
identificar e comunicar riscos sistêmicos (art. 34.º), garantindo a adoção de medidas de mitigação proporcionais e eficazes (art. 35.º);
e orientar a alta gestão e os colaboradores quanto às obrigações decorrentes do DSA, assegurando o cumprimento das normas e o acompanhamento dos compromissos firmados em códigos de conduta e protocolos de crise.

Art. 42: exige que as VLOPs e VLOSEs publiquem relatórios semestrais detalhados, contendo dados sobre os recursos humanos alocados à moderação, idiomas cobertos, indicadores de precisão e resultados das auditorias e avaliações de risco.

Art. 45: reconhece os códigos de conduta como instrumentos fundamentais para a aplicação coerente do regulamento, diante da complexidade e diversidade dos conteúdos ilegais e dos riscos informacionais.

Art. 48: prevê a criação de protocolos de crise, voltados à coordenação de respostas rápidas e eficazes em situações excepcionais, reforçando o dever de cuidado ampliado das plataformas nesses contextos.

Art. 49: dispõe que os Estados-Membros devem designar autoridades competentes e um Coordenador dos Serviços Digitais, responsáveis pela supervisão das plataformas e pela execução do DSA.

Art. 50: determina que os Coordenadores dos Serviços Digitais atuem de forma imparcial, transparente e independente.

Art. 51: confere aos Coordenadores poderes de investigação e requisição de informações junto às

plataformas e a terceiros, permitindo a coleta de dados necessários para aferir o cumprimento das obrigações estabelecidas no DSA.

Reino Unido - *Online Safety Act* (OSA)

O OSA adota o princípio do safe by design, segundo o qual os serviços devem ser projetados e operados para reduzir riscos antes de sua ocorrência, incorporando a prevenção como eixo estruturante do dever de cuidado (Reino Unido, 2023).

Seção 2: impõe obrigações específicas às plataformas que permitem interação entre usuários, estabelecendo o dever de prevenir a circulação de conteúdos ilegais e de atuar proativamente para proteger os usuários de danos.

Seção 9: determina a realização de avaliações periódicas de risco, que constituem a base para o exercício responsável do *duty of care.*

Seção 10: complementa a anterior ao detalhar o dever de implementar medidas de mitigação proporcionais aos riscos identificados, incluindo ajustes em design, algoritmos e mecanismos de moderação.

Seção 17: estabelece deveres de proteção do conteúdo de importância democrática, impondo às plataformas o uso de sistemas e processos proporcionais que assegurem a livre expressão política e a diversidade de opiniões. A moderação deve ocorrer de forma neutra e equilibrada, evitando discriminação de visões ideológicas distintas.

Seção 22: prevê a obrigação de publicar avaliações de impacto que analisem os efeitos das medidas de segurança sobre os direitos fundamentais dos usuários, especialmente quanto à liberdade de expressão e à privacidade.

Seção 23: impõe o dever de manter registros detalhados das avaliações de risco, criando uma trilha de auditoria interna indispensável à fiscalização posterior pela Ofcom.

Seção 27: reforça o dever de transparência ao exigir a publicização de uma declaração que sintetize as conclusões das avaliações de risco, de modo a garantir acesso público às informações sobre os riscos enfrentados pelos usuários.

Seção 41: reconhece os códigos de conduta como instrumentos essenciais para definir balizas, critérios e boas práticas na aplicação dos deveres de cuidado.

Seção 77: determina que os provedores elaborem e publiquem relatórios de transparência, nos moldes e prazos definidos pela Ofcom, com dados sobre remoções de conteúdo, mecanismos de denúncia, respostas e ações corretivas.

Seções 100, 104 e 107: consagram o dever de cooperação obrigatória das plataformas com a Ofcom, autoridade responsável pela supervisão e aplicação da lei.

A Seção 100 autoriza a emissão de information notices, que obrigam os provedores a fornecer todos os dados e documentos necessários ao exercício das funções regulatórias;

A Seção 104 determina que, quando a Ofcom iniciar investigação formal, o provedor deve cooperar integralmente, prestando informações e esclarecimentos;

A Seção 107 permite à Ofcom emitir audit notices, impondo a realização de auditorias compulsórias para verificar o cumprimento das obrigações legais.

Seção 159: impõe à Ofcom o dever de consolidar e divulgar relatórios públicos próprios, com base nas informações enviadas pelos provedores, sistematizando boas práticas e indicadores de cumprimento das obrigações legais.

Índia - *IT Rules* 2021

Rule 1: determina que os intermediários devem adotar medidas para impedir a disseminação de informações falsas ou enganosas, incluindo aquelas que induzam o destinatário a erro quanto à origem da mensagem ou que sejam manifestamente falsas ou não verdadeiras. A norma não se limita à diligência reativa, mas introduz uma lógica de gestão e mitigação preventiva de riscos estruturais.

Rule 3: consolida o núcleo do dever de diligência ao exigir que os intermediários cumpram padrões de transparência, informem claramente aos usuários suas regras de uso e envidem esforços razoáveis para evitar a publicação de conteúdos ilícitos ou nocivos. Entre os conteúdos vedados incluem-se a desinformação ou conteúdo incorreto, inverídico ou falso, ou verificado como falso pelo Governo.

Rule 4: estabelece obrigações mais rigorosas para os significant social media intermediaries, impondo a adoção de ferramentas tecnológicas proativas para identificar conteúdos de estupro, abuso sexual infantil ou materiais idênticos aos previamente removidos.

Rule 4(4): exige que os intermediários implementem mecanismos de supervisão humana apropriada *(appropriate human oversight)* e realizem revisões periódicas das ferramentas automatizadas, avaliando sua precisão, imparcialidade, vieses e impacto sobre a privacidade e segurança dos usuários.

Rule 4(1): impõe aos significant social media intermediaries a nomeação de três agentes responsáveis pela conformidade legal, com funções específicas:

- um *Chief Compliance Officer*, residente na Índia e pessoalmente responsável pela observância das normas (Rule 4(1)(a));
- um *Nodal Officer*, disponível 24 horas por dia para comunicação direta com autoridades públicas (Rule 4(1)(b)); e
- um *Resident Grievance Officer*, encarregado de gerir o sistema interno de reclamações (Rule 4(1)(c)).

Rule 4(1)(d): determina que os intermediários significativos publiquem relatórios mensais de compliance, detalhando o número de queixas recebidas, ações tomadas e resultados obtidos.

Rule 9(3): institui um regime de governança em três níveis destinado a assegurar a adesão ao Código de Ética, composto por:

- Nível I – Autorregulação do Editor;
- Nível II – Órgão de Autorregulação; e
- Nível III – Mecanismo de Supervisão do Governo Central.

Rule 12(2) e (4): disciplinam o Nível II, determinando que o Órgão de Autorregulação seja presidido por um juiz aposentado ou pessoa de reputação ilibada, com a função de supervisionar a adesão ao Código de Ética, julgar apelações de Nível I e emitir orientações ou pareceres consultivos.

Rule 13(1) e 14(1): tratam do Nível III, referente ao Comitê Interdepartamental *(Inter-Departmental Committee)*, composto por representantes de diversos Ministérios, incluindo Lei e Justiça e Assuntos Internos, responsável por ouvir queixas, deliberar e formular recomendações ao Governo Central.

Rule 14(5): reforça a periodicidade das reuniões do Comitê, assegurando a continuidade da supervisão pública e do escrutínio institucional sobre o cumprimento das normas.

Rule 19(1) e (3): impõem aos editores e órgãos de autorregulação o dever de divulgar de forma verdadeira e completa as queixas recebidas e resolvidas, além de preservar registros dos conteúdos transmitidos por, no mínimo, sessenta dias, para eventual disponibilização às autoridades competentes.

2.2.5 INTERPRETAÇÃO DO ART. 9º-D (PROPOSTAS)

Alexandre de Moraes caracteriza os grupos políticos que disseminam desinformação na internet como representantes do "novo populismo digital extremista". Segundo o autor, esses grupos utilizam as plataformas digitais para a propagação massiva de notícias fraudulentas, discursos de ódio e ideais antidemocráticos. Diante desse cenário, ele enfatiza a necessidade de avanços legislativos e de uma atuação mais eficaz da Justiça para conter esse fenômeno cada vez mais presente (Moraes, 2025).

A relevância desse problema se torna ainda mais evidente diante do amplo uso das redes sociais pela população brasileira. Nas Eleições de 2024 havia mais de 155 milhões de eleitores aptos. No mesmo período, o Brasil registrava 144 milhões de usuários ativos em redes sociais , equivalentes a cerca de 92% do eleitorado. Em outros termos, nove em cada dez votantes frequentam pelo menos uma plataforma digital (Brasil, [202-?]).

Além dos textos normativos citados anteriormente, destacam-se as ferramentas criadas para combater a desinformação. Todavia, embora reconheça a importância dos esforços coletivos realizados até aqui, o presente trabalho não tem por objetivo detalhar as soluções já existentes, mas questionar os pontos que ainda carecem de aprimoramento no enfrentamento à desinformação.

O art. 9º-D da Resolução representa um avanço relevante ao reconhecer a corresponsabilidade das plataformas digitais na preservação da integridade do processo eleitoral e da democracia. O dispositivo impõe aos provedores de aplicação que permitam a veiculação de conteúdo político-eleitoral o dever de adotar e publicizar medidas destinadas a impedir ou reduzir a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam comprometer a legitimidade das eleições.

Sob o ponto de vista sistêmico e principiológico, o dispositivo concretiza o dever constitucional de proteção da democracia e do direito à informação, ao mesmo tempo em que reafirma a função social das plataformas digitais como agentes relevantes no espaço público informacional contemporâneo.

Contudo, a interpretação do dispositivo exige um maior entendimento acerca dos dois verbos-núcleo do caput: “adotar” e “publicizar”.

Dessa forma, passa-se, agora, à interpretação sugerida do art. 9º-D, *caput,* referente à adoção e publicização de medidas para impedir ou diminuir a circulação de desinformação eleitoral.

“Adoção”

A adoção de medidas deve ser compreendida como um dever ativo e contínuo, que vai além da simples moderação de conteúdo. Envolve a implementação de políticas internas, auditorias periódicas e mecanismos de governança que permitam a detecção e mitigação precoce de desinformação.

Inspirando-se nas práticas internacionais, como as obrigações de mitigação de riscos previstas nos arts. 34 e 35 do DSA e os *duties of care* do OSA, esse dever não pode ser entendido como pontual ou meramente declaratório. Ele exige gestão contínua de riscos informacionais, incorporando rotinas de auditoria interna, planos de mitigação, sistemas de alerta e procedimentos de resposta rápida.

“Publicização”:

Já a publicização das medidas conecta-se ao princípio da transparência ativa. Sua efetividade depende da existência de instrumentos verificáveis e acessíveis, como relatórios públicos, dashboards de moderação e avaliações de impacto. Tanto o OSA (Seções 27 e 77) quanto as *IT Rules (Rule 4(1)(d) e Rule 19(1))* exigem que as plataformas publiquem relatórios periódicos sobre queixas, remoções e ações de *compliance* - o que reforça a *accountability* institucional e permite que autoridades e usuários monitorem o cumprimento dos deveres legais.

Além disso, observa-se que tanto OSA quanto as *IT Rules* não se limitam a impor deveres de autorregulação às plataformas, mas estabelecem estruturas externas de supervisão que garantem o cumprimento efetivo das normas.

No caso britânico, a Ofcom desempenha um papel central como órgão regulador independente, responsável por monitorar, auditar e exigir relatórios das plataformas (Seções 100, 104 e 107). A existência dessa autoridade de fiscalização autônoma confere transparência verificável e coerência regulatória ao sistema, reduzindo a margem de discricionariedade das empresas e reforçando a *accountability* pública.

Na Índia, o modelo é ainda mais complexo: as *IT Rules* preveem três níveis de governança (autorregulação do editor, órgão de autorregulação e mecanismo governamental de supervisão). Comparativamente, o Brasil ainda carece de instâncias análogas de acompanhamento e verificação, seja em caráter técnico (auditorias independentes), seja institucional (órgão fiscalizador externo à plataforma). A ausência desses mecanismos de governança limita a efetividade do art. 9º-D, uma vez que a adoção e a publicização das medidas permanecem sujeitas exclusivamente à autorregulação corporativa, sem garantias de monitoramento contínuo, padrões de transparência ou coerência entre diferentes plataformas.

2.2.6 EVIDÊNCIAS E ESTUDOS DE CASO

Embora tenha sido realizada uma busca em decisões do TSE e dos Tribunais Regionais Eleitorais, não foram encontrados julgados que tratem especificamente da (ausência de) adoção e publicização de medidas voltadas à redução da desinformação eleitoral. Essa ausência jurisprudencial reforça a necessidade de maior clareza normativa sobre o tema, bem como de mecanismos efetivos de fiscalização. Observa-se que, apesar de existir um dever de agir imposto às plataformas, não há uma supervisão estruturada sobre o cumprimento dessas obrigações, o que contribui para a baixa judicialização da matéria.

Recomendações (normativas e operacionais)

- Definição de parâmetros de publicização: estabelecer periodicidade mínima (ex.: semestral ou anual) para publicação das medidas adotadas; determinar formato padronizado, que permita comparação entre plataformas (ex.: modelo de relatório público digital); Indicar local obrigatório de divulgação.

- Relatórios periódicos de conformidade: exigir relatórios públicos contendo indicadores mensuráveis sobre: número de conteúdos moderados, tempo médio de resposta, parcerias com verificadores, investimento em moderação e resultados de mitigação.

- Auditorias internas e externas: imposição de auditorias independentes, preferencialmente conduzidas por entidades técnicas, para verificar a veracidade dos dados divulgados. Além disso, prever auditorias internas obrigatórias em ano eleitoral, com relatórios enviados ao TSE e às autoridades competentes.

- Governançacompartilhada:adotarummodelodecorregulação(governo+plataformas), inspiradoemexperiênciascomoOfcom(ReinoUnido)eDigitalServicesCoordinator(UE).

- Transparência: além de garantir publicação integral das auditorias e relatórios em formato acessível ao público e à imprensa, estabelecer sanções administrativas graduadas em caso de omissão ou publicação de informações falsas ou incompletas

- Evitar a autorregulação simbólica: sem fiscalização efetiva e métricas claras, o dever de agir tende a se tornar autorregulação simbólica, esvaziando o propósito normativo do art. 9º-D.

Riscos, salvaguardas e direitos

Riscos:

- Assimetria de poder informacional, que pode concentrar nas plataformas o papel de definir o que constitui “desinformação”;

- Falta de padronização das medidas adotadas, o que dificulta a fiscalização e o controle social;

- Publicização meramente formal ou simbólica, sem conteúdo verificável ou mensurável;

- Risco de exposição indevida de dados pessoais ou de informações estratégicas sob o pretexto de transparência.

Salvaguardas recomendadas:

- Padronização tanto da adoção quanto da publicização: as medidas de mitigação da desinformação devem seguir critérios uniformes de estrutura, metodologia e mensuração, definidos por órgão técnico ou em cooperação com o TSE. Para a adoção, isso inclui parâmetros mínimos de avaliação de risco, etapas de implementação e periodicidade de revisão. Para a publicização, devem ser fixados formatos acessíveis, indicadores verificáveis e periodicidade definida.

- Garantir supervisão independente e auditorias regulares, voltadas à verificação da efetividade tanto das medidas adotadas quanto das informações publicizadas.

- Prever responsabilidade em caso de omissão ou falsidade, de modo a reforçar o caráter vinculante do dever de agir e divulgar.

- Toda coleta, tratamento e divulgação de dados decorrentes das obrigações do art. 9º-D deve observar os princípios da minimização de dados, finalidade e anonimização, conforme a LGPD. O dever de transparência não pode se sobrepor ao direito à privacidade.

REFERÊNCIAS

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 dez 2025.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 2019. Dispõe sobre propaganda eleitoral. Brasília, DF, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 10 dez. 2025

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 2024. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Brasília, DF, 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 10 dez. 2025.

BRASIL. Tribunal Superior Eleitoral. Estatísticas do Eleitorado. Bsília, DF, [202-?]. Disponível em: https://www.tse.jus.br/eleicoes/estatisticas/estatisticas-de-eleitorado/eleitorado. Acesso em: 10 dez. 2025.
COMISSÃO EUROPEIA. The strengthened code of practice on disinformation 2022. [S. l.]: Comissão Europeia, 2022. Disponível em: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened--code-practice-disinformation. Acesso em: 10 dez. 2025.

ÍNDIA. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Índia: Ministry of Electronics and Information Technology, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Acesso em: 10 dez. 2025.

KEMP, Simon. Digital 2024: Brazil. Datareportal, 2024. Disponível em: https://datareportal.com/reports/digital-2024-brazil. Acesso em: 10 dez. 2025.

MORAES, Alexandre de. Democracia e Redes Sociais: desafio de combater o populismo digital extremista. Barueri: Atlas, 2025. p. 32.

REINO UNIDO. Online Safety Act (OSA). Londres, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Bruxelas, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. Acesso em: 10 dez. 2025.

2.3 CADASTRO (ART. 29, § 9°)

Ian Ferrare Meier

Art. 29. É vedada a veiculação de qualquer tipo de propaganda eleitoral paga na internet, excetuado o impulsionamento de conteúdos, desde que identificado de forma inequívoca como tal e contratado exclusivamente por partidos políticos, federações, coligações, candidatas, candidatos e representantes (Lei n.º 9.504/1997, art. 57-C, caput).
[...]
§ 9º O provedor de aplicação que pretenda prestar o serviço de impulsionamento de propaganda conforme o § 3º deste artigo deverá se cadastrar na Justiça Eleitoral, nos termos previstos na Resolução deste Tribunal que regula representações, reclamações e direito de resposta.

23.1 VISÃO GERAL E OBJETIVOS

Objetivo: realizar análise comparada do §9º do art. 29, da Resolução n.º 23.610/2024 do Tribunal Superior Eleitoral, com eventuais obrigações previstas em outras jurisdições.

Guia de perguntas:

Sobre o §9º do art. 29: Quais são as semelhanças e diferenças dos normativos do Brasil, União Europeia, Reino Unido e Índia em matéria de necessidade de cadastro na justiça eleitoral por provedor de aplicação que pretende prestar o serviço de impulsionamento de propaganda?

Base normativa (Brasil)

Resolução n.º 23.610/2024, do Tribunal Superior Eleitoral

Sobre o §9º do art. 29: a previsão, simples e objetiva, busca criar a obrigação para o provedor de aplicação que possui interesse em oferecer e prestar o serviço de impulsionamento de conteúdo propagandístico. Este conteúdo, ainda, deve estar de acordo com o §3º do mesmo artigo, que prevê que o impulsionamento deve ser contratado diretamente com provedor da aplicação de internet com sede e foro no país, ou de sua filial, sucursal, escritório, estabelecimento ou representante legalmente estabelecida(o) no país e apenas com o fim de promover ou beneficiar candidatas e candidatos ou suas agremiações, vedada a realização de propaganda negativa (Brasil, 2019).

Metodologia de *benchmarking*

- Seleção de jurisdições: UE (DSA), Reino Unido (OSA) e Índia (*IT Rules*).
- Unidade de comparação: Sobre o §9º do art. 29: existe, nos normativos, a exigência de cadastro na justiça eleitoral por provedor de aplicação que pretende prestar o serviço de impulsionamento de propaganda?

Unidades de comparação	União Europeia - *Digital Service Act* (DSA)	Reino Unido - *Online Safety Act* (OSA)	Índia – *IT Rules*
Exigência de cadastro na justiça eleitoral por provedor de aplicação que pretende prestar o serviço de impulsionamento de propaganda	Não exige	Não exige	Não exige

Benchmark internacional (síntese comparativa)

União Europeia (DSA):

Quanto à exigência do provedor interessado em prestar serviço de impulsionamento de propaganda se cadastrar na justiça eleitoral, a normativa da União Europeia não faz qualquer previsão (União Europeia, 2022).

Reino Unido (OSA):

Quanto à exigência do provedor interessado em prestar serviço de impulsionamento de propaganda se cadastrar na justiça eleitoral, a normativa do Reino Unido não faz qualquer previsão (Reino Unido, 2023).

Índia (*IT Rules*):

Quanto à exigência do provedor interessado em prestar serviço de impulsionamento de propaganda se cadastrar na justiça eleitoral, a normativa da Índia não faz qualquer previsão (Índia, 2021).

Interpretação do §9º do art. 29

O §9º do art. 29 deve ser compreendido como um instrumento de *accountability* institucional e rastreabilidade digital voltado à governança do impulsionamento de propaganda eleitoral. O dispositivo condiciona a prestação desse serviço ao cadastro prévio do provedor de aplicação na Justiça Eleitoral, conferindo transparência e previsibilidade à atuação das plataformas digitais durante o período eleitoral. Sua interpretação deve tomar como base a proteção da integridade informacional do processo democrático e eleitoral, uma vez que o impulsionamento é hoje uma das principais formas de amplificação de mensagens políticas. Assim, o §9º cria uma porta de entrada regulatória: apenas provedores cadastrados podem oferecer impulsionamento, permitindo à Justiça Eleitoral identificar quem intermedeia fluxos financeiros e algoritmos de visibilidade de conteúdo político. Interpretado sistematicamente, o §9º não se limita à burocratização formal do cadastro, mas impõe às plataformas um dever de compliance eleitoral contínuo, com atualização de dados, canais de contato oficiais e compromisso de transparência técnica e financeira, permitindo auditoria, responsabilização e prevenção de práticas de desinformação e disparos ilegais.

Evidências e estudos de caso

Não foram encontrados casos relevantes para este tópico.

Recomendações (normativas e operacionais)

- Definir, em resolução que atualizaria a redação do normativo do TSE, quais provedores de aplicação estão obrigados ao cadastro. O impulsionamento de propaganda pode ocorrer em plataformas de redes sociais, mecanismos de busca, serviços de streaming, aplicativos de mensagens e marketplaces de publicidade digital. A clareza quanto ao escopo evita lacunas regulatórias e impede que intermediários informacionais escapem da obrigação por meio de estruturas técnicas ou contratuais.

- Determinar que o registro junto à Justiça Eleitoral seja atualizado a cada eleição ou sempre que houver alteração de controle societário, políticas de transparência, local de armazenamento de dados ou modelo de impulsionamento. Essa obrigação assegura a confiabilidade e rastreabilidade contínua das plataformas.

- Criar um repositório público e pesquisável no portal do TSE com a lista de provedores cadastrados, contendo informações básicas como: (i) nome da empresa; (ii) país de origem; (iii) URL principal; (iv) responsável de contato; e (v) status do cadastro (ativo, suspenso, revogado). Essa medida garante *accountability* e auditabilidade social, permitindo que campanhas e cidadãos verifiquem se um serviço de impulsionamento possui legitimidade para a atividade.

- Vincular o cadastro à assinatura de um termo de compromisso que obrigue o provedor a: (i) preservar logs de impulsionamento por tempo determinado, (ii) responder a requisições da Justiça Eleitoral em prazo reduzido, (iii) publicar relatórios de transparência eleitoral contendo a quantidade de anúncios impulsionados, e origem dos mesmos e o volume financeiro movimentado, e (iv) adotar protocolos de moderação compatíveis com as normas de propaganda eleitoral.

- Prever a suspensão temporária ou definitiva do cadastro em caso de descumprimento das obrigações de transparência, de fornecimento de dados ou de veiculação de impulsionamentos irregulares. Nesses casos, o Tribunal Superior Eleitoral deve divulgar, de forma pública, os casos de provedores suspensos ou inabilitados.

- Criar um portal público de denúncia de anúncios pagos veiculados por provedores não cadastrados.

- O Tribunal Superior Eleitoral deve elaborar e divulgar guias operacionais para provedores sobre as novas obrigações.

Riscos, salvaguardas e direitos

Riscos

A ausência de cadastro ou o registro incompleto de provedores de impulsionamento pode gerar ambientes de opacidade informacional, dificultando a identificação da origem dos anúncios, do responsável financeiro e dos critérios algorítmicos de exibição. Essa lacuna favorece práticas de propaganda irregular, uso de intermediários ocultos e impulsionamentos transnacionais não rastreáveis.

Na ausência de registro público e padronizado, a Justiça Eleitoral enfrenta obstáculos para rastrear fluxos de patrocínio, verificar contratos e aplicar sanções. Isso gera risco de impunidade digital e fragiliza a legitimidade das eleições.

Salvaguardas

O Tribunal Superior Eleitoral deve manter um cadastro eletrônico unificado com dados básicos dos provedores autorizados, em formato aberto (Open Data), permitindo consultas públicas e integração com sistemas de auditoria e de denúncia.

O cadastro deve vincular o provedor a registros de CNPJ, dados bancários e contratos de impulsionamento, garantindo trilhas verificáveis entre o anunciante e o serviço prestado.
Estabelecer protocolos de cooperação entre TSE, ANPD, Banco Central e Receita Federal para verificação cruzada de transações financeiras, uso de dados e identidade dos anunciantes.

Direitos

O cidadão tem direito de saber quem pagou, por que pagou e por que foi alcançado por determinado conteúdo impulsionado. Qualquer eleitor deve poder consultar, de forma simples e acessível, se determinado serviço ou plataforma está regularmente cadastrado na Justiça Eleitoral, prevenindo fraudes e propaganda irregular. Todos os candidatos e partidos devem ter acesso isonômico aos provedores cadastrados, em condições de transparência e previsibilidade de custos, assegurando a paridade durante o pleito.

REFERÊNCIAS

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 2019. Dispõe sobre propaganda eleitoral. Brasília, DF, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 10 dez. 2025

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 2024. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Brasília, DF, 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 10 dez. 2025.

ÍNDIA. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Índia: Ministry of Electronics and Information Technology, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Acesso em: 10 dez. 2025.

REINO UNIDO. Online Safety Act (OSA). Londres, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Bruxelas, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. Acesso em: 10 dez. 2025.

2.4 CANAIS DE DENÚNCIA (ART. 9º-D, II)

Bruna Ammon Lisbôa

> **Art. 9º-D. É dever do provedor de aplicação de internet, que permita a veiculação de conteúdo político-eleitoral, a adoção e a publicização de medidas para impedir ou diminuir a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam atingir a integridade do processo eleitoral, incluindo: [...]**
> **II - a implementação de instrumentos eficazes de notificação e de canais de denúncia, acessíveis às pessoas usuárias e a instituições e entidades públicas e privadas;**
> **[...]**

24.1 VISÃO GERAL E OBJETIVOS

Objetivo: interpretar o alcance do Art. 9º-D, II (o que é "instrumentos eficazes" e "acessíveis") e comparar com boas práticas e obrigações em outras jurisdições.

Guia de Perguntas:

- Quais requisitos mínimos um canal cumpre para ser "eficaz" e "acessível"?
- Quais prazos e fluxos de tratamento são razoáveis?
- Que métricas e transparência se espera dos provedores?
- Como prevenir abuso do canal (fraudes, mass reporting) sem desestimular denúncias legítimas?

24.2 BASE NORMATIVA (BRASIL)

TSE Res. 23.732/2024, Art. 9º-D, II:

obriga implementação de canais de denúncia e instrumentos de notificação para reduzir fatos notoriamente inverídicos/descontextualizados no processo eleitoral. O referido artigo estabelece como dever do provedor de aplicação de internet que permite a veiculação de conteúdo político-eleitoral a "implementação de instrumentos eficazes de notificação e de canais de denúncia, acessíveis às pessoas usuárias e a instituições e entidades públicas e privadas".[6]

Contexto regulatório adjacente:

Nesse debate, é importante considerar as recentes decisões do Supremo Tribunal Federal, que têm relativizado a interpretação estrita do art. 19 do Marco Civil da Internet (Braasil, 2014). Em 2025, por exemplo, a Corte entendeu que, em determinadas situações, as plataformas podem ser responsabilizadas por não agir diante de notificações extrajudiciais de conteúdos manifestamente ilícitos, elevando assim o seu dever de cuidado e diligência. Esse entendimento reforça a leitura de que os canais de denúncia previstos no art. 9º-D não devem ser apenas formais, mas efetivos mecanismos de resposta imediata e verificável (Agência Brasil, 2025).

6 É dever do provedor de aplicação de internet, que permita a veiculação de conteúdo político-eleitoral, a adoção e a publicização de medidas para impedir ou diminuir a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam atingir a integridade do processo eleitoral, incluindo: II - a implementação de instrumentos eficazes de notificação e de canais de denúncia, acessíveis às pessoas usuárias e a instituições e entidades públicas e privadas (Incluído pela Resolução n.º 23.732/2024) (Brasil, 2024).

2.4.3 METODOLOGIA DE *BENCHMARKING*

Seleção de jurisdições: UE (DSA), Reino Unido, Índia (*IT Rules*)

A comparação internacional proposta concentra-se em "canais de denúncia" e obrigações conexas que asseguram sua efetividade na seara prática: A) acessibilidade; B) usabilidade; C) fluxo e prazos; D) devido processo; E) transparência; F) integrações; G) mitigações de abuso; H) governança & *accountability*. O recorte privilegia três jurisdições com arranjos regulatórios robustos e influentes: União Europeia (DSA), Reino Unido (OSA) e Índia (*IT Rules*, 2021).

A UE/DSA foi escolhida por oferecer um quadro normativo horizontal e escalonado (com obrigações acrescidas para plataformas muito grandes), que se tornou referência global (União Europeia, 2022); o Reino Unido/OSA aprofunda o enfoque em segurança por design e na governança regulatória (Ofcom), com forte atenção a fluxos de reclamação e transparência (Reino Unido, 2023); por fim, a Índia/*IT Rules* foi incluída por integrar o Sul Global, apresentar semelhanças socioeconômicas com o Brasil e articular prazos, trilhas recursais e métricas públicas que destacam e podem solucionar dilemas operacionais próximos aos brasileiros (Índia, 2021).

Sob essa ótica, "canais de denúncia" não são apenas um ponto de entrada para *reports*, em verdade, constituem um mecanismo de diligência que precisa convergir com as políticas, fluxos, prazos, justificativas de decisão, prestação de contas e mitigação de abusos. É uma cadeia completa, do clique inicial à decisão final auditável, que permite avaliar se o canal é, de fato, eficaz (reduz riscos e desinformação com respostas céleres e proporcionais) e acessível (usável por pessoas e instituições em condições diversas, sem barreiras linguísticas, técnicas ou de desenho).

Unidades de comparação (possíveis critérios)

- Acessibilidade (idioma local, *mobile*, deficiência, anonimato/identificação);
- Usabilidade (n.º de cliques, clareza do formulário, upload de provas, recibo de protocolo);
- Fluxo e prazos (triagem, moderação e razões de decisão/remoção);
- Devido processo (aviso ao denunciado, statement of reasons, recurso);
- Transparência (dashboards, relatórios, repositórios de anúncios);
- Integrações (trusted flaggers, mediação, autoridades);
- Mitigações de abuso (*rate-limits*, autenticidade, sanções a denunciações temerárias);
- Governança & *accountability* (responsável interno, auditoria, avaliação de risco.

Unidades de comparação	União Europeia - *Digital Service Act* (DSA)	Reino Unido - *Online Safety Act* (OSA)	Índia – *IT Rules*
Acessibilidade	Art. 16 DSA: obrigação de mecanismos de notice & action acessíveis a qualquer usuário; requisitos mínimos para formular denúncias estruturadas (inclui idioma local e acessibilidade).	OSA, ss. 9, 11, 65-67 + guias da Ofcom: obrigação de plataformas proverem sistemas fáceis de uso, adequados a crianças, mobile-friendly	*IT Rules* 2021, Rule 3(2)(a): plataforma deve ter "grievance mechanism" claramente visível, em idioma local e inglês
Usabilidade	Art. 16(2) DSA: notificação deve permitir incluir URL, descrição e anexos; formulário estruturado.	Ofcom Codes (2024 draft): reporte deve ser claro, em linguagem simples, e permitir upload de evidências.	*IT Rules* 2021, Rule 3(2)(a-b): denúncia deve conter dados básicos (conteúdo, usuário, descrição); formulário estruturado é exigido.
Fluxo e prazos (SLAs)	OSA, ss. 9 e 67: prazo de resposta será detalhado em códigos da Ofcom; foco em remoção rápida de conteúdos ilegais e proteção infantil.	OSA, ss. 9 e 67: prazo de resposta será detalhado em códigos da Ofcom; foco em remoção rápida de conteúdos ilegais e proteção infantil.	*IT Rules* 2021, Rule 3(2)(a): reclamações devem ser respondidas em até 15 dias
Devido processo	Art. 17 DSA: obrigação de enviar ao usuário afetado statement of reasons; Art. 20: canal interno de recurso.	OSA, s. 65 + Ofcom Codes: obrigação de permitir recurso e comunicação clara ao usuário.	*IT Rules* 2021, Rule 3(2)(b-c): prevê recurso em 3 níveis (plataforma → Grievance Officer → judicial).
Transparência	Art. 15 DSA: relatórios semestrais obrigatórios sobre denúncias recebidas e decisões; dashboards públicos.	OSA, ss. 67-69: Ofcom pode exigir relatórios de cumprimento sobre canais de queixa.	*IT Rules* 2021, Rule 4(d): obriga relatórios mensais de queixas e medidas tomadas.
Integrações	Art. 22 DSA: criação de trusted flaggers; Art. 21: resolução extrajudicial de disputas; integração com autoridades.	OSA, ss. 65-67: integração via Ofcom como autoridade reguladora.	*IT Rules* 2021, Rule 3(2)(j): Grievance Officer deve responder ao governo e às autoridades competentes.
Mitigações de abuso	Art. 16(5) + 22 DSA: medidas contra abuso de notificações; prioridade a trusted flaggers.	OSA + Ofcom Codes: exigem proteção contra mass reporting e mecanismos antiabuso.	*IT Rules* 2021, Rule 3(2)(k): prevê sanções contra denúncias falsas ou abusivas.
Governança & accountability	Arts. 34-35 DSA: avaliação de risco anual; Art. 37: auditorias independentes.	OSA, ss. 9 e 69: supervisão contínua da Ofcom; multas em caso de falha.	*IT Rules* 2021, Rule 4(c): nomeação obrigatória de Grievance Officer; responsabilidade direta.

Benchmark internacional (síntese comparativa)

União Europeia – DAS

Sistema de "Notice & Action" (Art. 16 DSA)

Estabelece canais de denúncia eletrônicos e acessíveis para qualquer pessoa reportar conteúdos ilegais;

- Define padrões processuais detalhados para recebimento, análise e resposta às notificações;
- (ii.i) Notificações devem conter: Localização exata do conteúdo (ex: URL). Descrição das razões jurídicas ou factuais da alegação de ilegalidade. Dados de contato do denunciante (nome e e-mail, com exceção em casos de exploração sexual infantil). Declaração de boa-fé quanto à veracidade das informações. Busca equilibrar acessibilidade e precisão, evitando denúncias genéricas ou abusivas.
- autoriza inclusão de anexos, descrição e URL em formulário estruturado.
- prevê medidas contra abusos de notificações (como denúncias fraudulentas ou infundadas).
- Garantias de devido processo
- Art. 17: obrigação de enviar ao usuário afetado um "statement of reasons" (declaração de motivos) quando há remoção, bloqueio ou desmonetização;
- Art. 20: estabelece canal interno de recurso (internal complaint-handling system) para contestar decisões;
- (ii.i) Deve ser célere, não discriminatório e diligente;
- (ii.ii) Caso o recurso seja aceito, a decisão deve ser revertida sem demora indevida.
- Art. 21: cria mecanismos de resolução extrajudicial de disputas, oferecendo alternativa adicional para reparação.

Transparência e relatórios públicos (Art. 15): plataformas devem publicar relatórios periódicos (anuais ou semestrais), com:

- número de ordens de autoridades e prazos médios de resposta;
- quantidade de avisos de usuários e trusted flaggers;
- uso de moderação automatizada e métricas de acurácia;
- dados sobre reclamações e reversões de decisão.

Relatórios devem ser legíveis por máquina e publicamente acessíveis, permitindo auditoria da diligência das plataformas.

***Trusted Flaggers* e mitigação de abusos**

- Art. 22: cria a figura dos trusted flaggers - entidades certificadas com prioridade no tratamento das denúncias.
- Interpretação conjunta: Art. 16 + 22: estabelecem mecanismos contra notificações abusivas, incluindo possibilidade de suspender denunciantes reincidentes.
- Governança, risco e auditorias
- Art. 34: plataformas de grande porte devem realizar avaliações anuais de risco

(por exemplo, riscos sistêmicos de desinformação ou segurança).
- Art. 35: impõe medidas de mitigação proporcionais aos riscos identificados.
- Art. 37: exige auditorias independentes periódicas, reforçando a *accountability* e supervisão regulatória.

Reino Unido – *Online Safety Act* (OSA)

Sistema de "Safety by Design" e Canais de Denúncia

O OSA *(Online Safety Act)* parte do princípio de *"safety by design"* - os serviços devem ser concebidos e operados proporcionalmente ao risco e ao porte da plataforma.

A Parte 1 da lei impõe aos provedores o dever de gerenciar riscos ligados a conteúdos ilegais e prejudiciais, com foco especial na proteção de crianças.

Define que canais de denúncia e reclamação devem ser:

- (iii.i) *"Easy to access, easy to use (including by children) and transparent"* (ss. 46(2)(c), 77(2)(c));
- (iii.2) Disponíveis em termos de serviço claros e acessíveis, detalhando políticas e processos de tratamento de reclamações (ss. 46(3), 77(3));
- (iii.3) Complementados por informações públicas sobre tecnologias proativas de moderação e conformidade (ss. 17(7), 22(12), 69(7), 75(7), 87(2)).
- Termos e declarações devem ser claros e acessíveis (ss. 18(8), 22(8), 69(8), 75(8), 87(2)).

Regras específicas incluem:

- (v.i) Procedimento para reclamações sobre conteúdo jornalístico (s. 41(3));
- (v.2) Deveres especiais para casos de usuários infantis falecidos (Sch. 8, para. 14).

Obrigações de Resposta e Fluxos de Tratamento

OSA não impõe prazos fixos (como 24h), mas exige rapidez e proporcionalidade.

- s. 16(3)(a): medidas para minimizar o tempo de exposição de conteúdos ilegais prioritários.
- s. 16(3)(b): obrigação de remoção rápida do conteúdo ilegal.
- s. 67(3)(b): serviços de busca devem garantir que usuários não encontrem conteúdo ilegal rapidamente.

Em casos graves (terrorismo, exploração infantil): A Ofcom pode exigir uso de tecnologias credenciadas para identificação e remoção célere (s. 121(2)(a)(iii); s. 121(3)(a)(ii)).

Reclamações sobre conteúdo jornalístico devem levar à restauração rápida em caso de erro (ss. 42(1)(b), 42(2)(b)).

Para usuários infantis falecidos, respostas devem ser *"timely"* (em tempo hábil) (Sch. 8, para. 14; Sch. 4, paras. 4(c), 5(c)).

Garantias de Devido Processo

Embora o OSA não detalhe *"statements of reasons"* como o DAS garante procedimentos claros e acessíveis nos termos de serviço. Reforça a necessidade de transparência e proporcionalidade em todas as medidas adotadas. Determina proteção à liberdade de expressão e privacidade na aplicação das medidas de segurança (ss. 50(2), 50(3), 51(a)-(b)).

Transparência e Relatórios Públicos

A Ofcom é o núcleo da transparência no OSA: Deve publicar relatórios anuais de transparência com boas práticas do setor (s. 159(3)). Pode exigir que provedores das Categorias 1, 2A e 2B publiquem relatórios anuais completos e precisos (s. 176(4); Sch. 8). Esses relatórios incluem: Incidência de conteúdo ilegal e prejudicial (Sch. 8, paras. 1, 2, 23, 24); Uso de algoritmos e tecnologias proativas (Sch. 8, paras. 8-9, 27); Verificação de identidade dos usuários (Sch. 8, para. 11); Medidas de alfabetização midiática (Sch. 8, paras. 19, 35).

Obrigação adicional de publicar impact assessments sobre liberdade de expressão e privacidade (s. 52(6)(b)).

Mitigação de Abusos e Integridade Processual

- OSA e Ofcom Codes exigem: Proteção contra mass reporting e práticas abusivas (ss. 16(2), 28(1)(d), 67(2), 70(10)); Proporcionalidade em todas as medidas de moderação e denúncia.
- Proteção à liberdade de expressão e privacidade é princípio transversal (ss. 50(2), 50(3), 51(a)-(b)).
- Previsão de infrações penais para fornecimento de informações falsas à Ofcom, reforçando integridade do sistema (s. 109(1); Sch. 12, para. 18(1)(c); s. 265(3)).

Governança e *Accountability*

A Ofcom exerce papel central na governança do OSA: Pode emitir e revisar códigos de prática (s. 115(1)); Fiscaliza continuamente os provedores (ss. 9, 69); Exige relatórios e aplica sanções (multas, obrigações adicionais); Supervisiona diretamente os canais de denúncia e queixa.

Essa centralização regulatória fortalece o enforcement e assegura que os mecanismos de denúncia sejam auditáveis e sujeitos a escrutínio público permanente.

Índia - *IT Rules*

Sistema de Reclamações e Canais de Denúncia

As *IT Rules (Information Technology [Intermediary Guidelines and Digital Media Ethics Code] Rules)* estruturam um sistema de três níveis para reclamações:

- Nível 1 - Provedor (Grievance Officer da própria plataforma);
- Nível 2 - Órgão autorregulador (para setores específicos como notícias e jogos online);

- Nível 3 – Supervisão governamental, via Grievance Appellate Committee (GAC).

Rule 3(2)(a): todos os intermediários devem manter, visivelmente em seus sites e aplicativos, um canal de reclamações em inglês e idioma local, com: nome e dados de contato de um Grievance

Officer residente no país; formulário estruturado para submissão da queixa; Campos obrigatórios: identificação do conteúdo (URL), usuário envolvido e descrição clara da infração (Rule 3(2)(a-b)).

A acessibilidade é garantida por: Disponibilidade bilíngue (inglês + idioma local); Visibilidade pública das informações; Estrutura padronizada de envio de queixas.

Obrigações de Resposta e Prazos

As *IT Rules* se destacam por prazos fixos e vinculantes, o que diferencia o modelo indiano dos sistemas europeu e britânico:

- Confirmação de recebimento (acknowledgment): até 24 horas (Rule 3(2)(a)(i));
- Resposta final / resolução: até 15 dias (Rule 3(2)(a)(i));
- Casos urgentes (exposição de nudez, material sexual não consentido): 72 horas (Rule 3(2)(a));
- Remoção por ordem judicial ou notificação governamental: até 36 horas (Rule 3(1)(d)).

O sistema prevê rastreabilidade das queixas por número de ticket/protocolo, permitindo acompanhar o status da reclamação (Rule 4(6)).

Estrutura Recursal e Devido Processo

Três níveis de recurso asseguram escalonamento progressivo e *accountability*: (i) Resposta inicial do Grievance Officer (nível interno da plataforma);(ii) Apelação a um órgão autorregulador, aplicável a certos intermediários (ex.: editores de notícias); (iii) Apelação final ao Grievance Appellate Committee (GAC), criado pelo governo central (Rule 3(2)(b-c) e Rule 3A).

O GAC deve decidir em até 30 dias, e sua decisão deve ser publicada no site da plataforma (Rule 3A (7)).

Estrutura garante: Devido processo (possibilidade real de revisão de decisão); Supervisão externa de caráter público e regulatório.

Transparência e Relatórios Públicos

Intermediários significativos (SSMIs) têm obrigações reforçadas de transparência:

- Devem publicar relatórios mensais de conformidade (Rule 4(1)(d)), contendo: Número de reclamações recebidas; Ações tomadas; Conteúdos removidos proativamente por ferramentas automatizadas.
- Devem permitir rastreamento de reclamações por número único de protocolo (Rule 4(6));
- Devem fornecer razões claras para cada decisão tomada sobre o conteúdo.

Mitigação de Abusos e Integridade Processual

Rule 3(2)(k): prevê medidas contra denúncias falsas ou fraudulentas. O modelo em múltiplos níveis (provedor → autorregulação → governo) atua como barreira contra abusos, pois permite revisão em instâncias superiores. A presença de prazos rígidos e rastreamento transparente reduz riscos de arbitrariedade e negligência.

Governança e *Accountability*

Rule 4(c): exige que intermediários de grande porte nomeiem formalmente um Grievance Officer residente responsável pelo cumprimento das regras.

A governança é compartilhada, mas há supervisão direta do governo central via o GAC.

A arquitetura reflete:

- (i.i) *Accountability* verticalizada (empresa → autorregulação → Estado);
- (i.ii) Responsabilização individualizada (*Grievance Officer* como ponto de contato legal);
- (i.iii) Controle público e institucionalizado da eficácia dos canais de denúncia.

Interpretação do Art. 9º-D, II (propostas)

Em síntese, a interpretação do art. 9º-D, II à luz do *benchmarking* internacional revela a necessidade de o Brasil consolidar padrões verificáveis de acessibilidade, eficácia, transparência e proporcionalidade. Isso inclui a presença constante de um canal de denúncia visível e de fácil uso, com formulário padronizado em português (e, quando aplicável, em idiomas locais), campos mínimos para precisão e envio de evidências, confirmação imediata de recebimento e comunicação motivada da decisão; prazos escalonados e proporcionais à gravidade da infração; relatórios públicos periódicos com métricas uniformes; governança clara com responsável interno e auditorias independentes; e integração com autoridades e sinalizadores de confiança. Somente assim o canal de denúncia deixa de ser um requisito meramente formal e passa a constituir um instrumento efetivo de defesa da integridade eleitoral, alinhando o sistema brasileiro às melhores práticas internacionais sem comprometer os valores democráticos que o fundamentam.

Quais requisitos mínimos um canal cumpre para ser “eficaz” e “acessível”?

Para que um canal de denúncia seja considerado “acessível” e “eficaz” no contexto do art. 9º-D, II, ele deve ser visível, intuitivo, fácil de usar e compatível com dispositivos móveis, disponível em língua portuguesa e, quando aplicável, em idiomas locais, como no caso de comunidades indígenas. A acessibilidade também exige que possa ser acionado por indivíduos e instituições, preferencialmente por meio de formulário estruturado que permita o envio de evidências. Já a eficácia depende da capacidade do canal de impedir ou mitigar rapidamente a circulação de informações falsas ou descontextualizadas que afetem a integridade eleitoral, o que requer a adoção de medidas imediatas de suspensão de impulsionamento e monetização, investigação interna e bloqueio de recirculação de conteúdo ilícito. Em linha com o princípio de *safety by design*, o canal deve combinar facilidade de uso com mecanismos de resposta rápida e verificável, proporcionais ao risco e ao porte do serviço.

Quais prazos e fluxos de tratamento são razoáveis?

Embora a Resolução TSE n.º 23.732/2024 não fixe prazos objetivos, ela impõe o dever de adoção de "providências imediatas e eficazes", o que exige fluxos claros e não arbitrários. O provedor deve confirmar o recebimento da denúncia sem demora indevida, comunicar a decisão final com fundamentação e garantir ao usuário afetado o direito a uma declaração de motivos *(statement of reasons)* e a via recursal interna célere e diligente. À luz do direito comparado, o modelo europeu privilegia a celeridade sem prazos fixos, enquanto o indiano estabelece parâmetros concretos - 24 horas para confirmação, 15 dias para resolução e 72 horas em casos urgentes. Assim, o padrão recomendável para o Brasil é o escalonamento de prazos: 24 horas para conteúdos manifestamente ilícitos ou de risco grave, 72 horas para alta prioridade e até sete dias para casos comuns, sempre com revisão humana e canal interno de recurso, conciliando a flexibilidade do DSA com a objetividade das *IT Rules.*

Que métricas e transparência se espera dos provedores?

A transparência é condição indispensável para transformar diligência em *accountability* e é expressamente exigida pelo inciso IV do art. 9º-D da Resolução TSE. Os provedores, especialmente os de grande porte, devem publicar relatórios periódicos (mensais, semestrais ou anuais) em formato legível por máquina, contendo dados sobre volume de denúncias recebidas, prazos médios de resposta, número de decisões revertidas, uso e precisão das tecnologias de moderação e conteúdos removidos proativamente. Deve ser possível rastrear reclamações por número de protocolo e fornecer as razões das decisões. Em períodos eleitorais, é recomendável a realização de avaliações de impacto sobre a integridade do processo eleitoral, além da nomeação de um responsável interno pela tramitação das denúncias *(Grievance Officer)* e da realização de auditorias independentes periódicas, a fim de assegurar escrutínio regulatório e comparabilidade entre plataformas.

Como prevenir abuso do canal (fraudes, mass reporting) sem desestimular denúncias legítimas?

A prevenção de abusos nos canais de denúncia requer equilíbrio entre o combate a fraudes e a preservação do uso legítimo. Medidas de dissuasão devem incluir a possibilidade de sanções contra denúncias falsas ou repetidamente infundadas, como a suspensão de usuários abusivos, e a exigência de formulários precisos, com URL, descrição jurídica e declaração de boa-fé, para reduzir o incentivo ao mass reporting oportunista. O desenho procedimental deve incorporar autenticação de usuários, limitação de frequência de denúncias e priorização de *trusted flaggers* - entidades certificadas que recebem tratamento preferencial -, promovendo confiança e eficiência. As medidas devem ser proporcionais e assegurar o devido processo, garantindo comunicação motivada das decisões e vias recursais céleres. Por fim, é essencial preservar o princípio da menor interferência no debate democrático, evitando que prazos demasiadamente curtos resultem em over-removal e no enfraquecimento da liberdade de expressão.

Evidências e estudos de caso

Caso C-682/18 e C-683/18 (YouTube/Cyando), julgado pelo Tribunal de Justiça da União Europeia, destacou que as plataformas digitais não possuem obrigação geral de monitorar conteúdos publicados por terceiros. Contudo, elas podem ser responsabilizadas em três situações: (a) se tiverem conhecimento específico da existência de conteúdo ilícito e não agirem prontamente para removê-lo ou bloqueá-lo; (b) se adotarem medidas que possam ser interpretadas como anuência ao uso ilegal

de sua plataforma; ou (c) se selecionarem ou promoverem deliberadamente conteúdos ilegais, por exemplo, ao disponibilizar ferramentas que incentivem ou facilitem a partilha de material proibido (Zingales, 2025).

Caso Moody vs. Netchoice, LLC, analisado pela Suprema Corte dos Estados Unidos, considerou que os algoritmos de moderação de conteúdo configuram uma forma de "expressão" da própria plataforma, equiparável ao trabalho editorial de veículos de imprensa e, portanto, protegida pela Primeira Emenda. A decisão da Corte de Apelações do Terceiro Circuito reforçou que, embora as plataformas sejam responsáveis pelo conteúdo que disponibilizam e moderam, elas também gozam da liberdade de expressão ao decidir como organizar e filtrar esse conteúdo. Assim, sua atuação editorial está protegida constitucionalmente, o que se alinha ao entendimento europeu expresso no caso YouTube/Cyando (Zingales, 2025).

Recomendações (normativas e operacionais)

Requisitos Operacionais e de Acessibilidade (Padrão mínimo brasileiro)

O canal de denúncia deve incorporar um padrão mínimo uniforme, compatível com o art. 9º-D, II, e inspirado nas melhores práticas internacionais. É essencial a presença permanente de um botão "Denunciar", facilmente identificável e acessível em todas as interfaces, inclusive móveis. As denúncias devem ser enviadas por formulário padronizado, com campos obrigatórios que assegurem precisão: identificação exata do conteúdo (URL), descrição jurídica ou factual da irregularidade, possibilidade de envio de evidências e declaração de boa-fé. Após o envio, o sistema deve emitir recibo automático de recebimento, com registro de data e indicação do prazo estimado para resposta. O formulário deve estar em português e, quando aplicável, também em idiomas locais, garantindo inclusão linguística e acesso equitativo. O desenho do canal deve seguir o princípio de *safety by design,* equilibrando simplicidade, clareza e proporcionalidade ao porte e risco do serviço.

Fluxos e Prazos de Tratamento (Celeridade e proporcionalidade)

A tramitação das denúncias deve observar fluxos previsíveis e prazos proporcionais, de modo a assegurar resposta rápida sem comprometer o devido processo. Recomenda-se a adoção de prazos escalonados, tomando por referência o *Digital Services Act* europeu: 24 horas para casos manifestamente ilícitos ou de risco grave; 72 horas para situações de prioridade alta; e até sete dias para análise padrão, sempre acompanhada de via de recurso. O denunciante deve receber confirmação imediata de recebimento e comunicação motivada da decisão final. Essa estrutura combina a agilidade necessária à integridade eleitoral com a prudência exigida pela liberdade de expressão.

Devido Processo e Recurso Interno (Garantia de revisão)

Todo usuário afetado por remoção, bloqueio ou desmonetização deve receber uma declaração de motivos clara e acessível, informando as razões da decisão e as possibilidades de contestação. O provedor deve manter mecanismo interno de recurso, com prazos razoáveis e procedimentos transparentes, garantindo que decisões possam ser revistas por instância humana. Quando o recurso for acolhido, a reversão deve ocorrer sem demora indevida. Esse modelo reforça a confiança dos usuários e concretiza o devido processo como garantia operacional, não apenas formal.

Transparência e Métricas (Prestação de contas pública)

A obrigação de transparência prevista no art. 9º-D, IV deve ser implementada por meio de relatórios periódicos públicos, em formato legível por máquina, contendo métricas sobre o funcionamento dos canais. Recomenda-se a publicação trimestral desses relatórios, com dados sobre o volume de denúncias, prazos médios de resposta, taxas de reversão, medidas proativas e uso de sistemas automatizados de moderação. Em anos eleitorais, a frequência dos relatórios deve ser aumentada, possibilitando acompanhamento contínuo pela Justiça Eleitoral e pela sociedade. A inclusão de um sistema de rastreamento por número de protocolo *(ticket)* reforça a previsibilidade e a confiança no processo.

Governança e Estrutura Interna (Responsabilidade e controle)

Os provedores devem manter uma estrutura formal de governança voltada à tramitação de denúncias. É recomendável a nomeação de um responsável interno (residente no país) encarregado de garantir a conformidade com o art. 9º-D, II, com seus dados de contato disponíveis publicamente. Devem ser realizadas auditorias independentes periódicas para avaliar a efetividade do canal e, em anos eleitorais, elaborada uma avaliação de impacto sobre a integridade do processo eleitoral, conforme prevê o próprio art. 9º-D, V. Essa estrutura de governança cria linhas claras de responsabilidade e aprimora a confiabilidade do sistema.

Integrações Institucionais e Cooperação (Articulação com autoridades)

A efetividade dos canais de denúncia depende de integração institucional e cooperação contínua. Recomenda-se o estabelecimento de convênios e canais dedicados com órgãos eleitorais e outras autoridades competentes, de modo a agilizar o encaminhamento de casos de relevância pública. Além disso, deve-se fomentar a criação e reconhecimento de sinalizadores de confiança *(trusted flaggers)*, entidades certificadas que recebam prioridade no processamento de denúncias e na comunicação com provedores. Essa articulação aprimora a capacidade de resposta e contribui para uma atuação mais coordenada entre plataformas e instituições.

Prevenção de Abuso (Equilíbrio e proporcionalidade)

Para evitar o uso indevido do canal, como denúncias fraudulentas ou campanhas de *mass reporting,* recomenda-se prever mecanismos de sanção a notificações manifestamente infundadas, inclusive a suspensão temporária de denunciantes abusivos. Ao mesmo tempo, o sistema deve proteger o uso legítimo, exigindo precisão nas denúncias e priorizando canais institucionais verificados. Quando possível, medidas graduais como rotulagem, limitação de alcance ou desmonetização devem ser preferidas à remoção total, preservando a liberdade de expressão. O devido processo e a proporcionalidade devem orientar todas as respostas, de modo que o canal sirva à integridade eleitoral sem restringir o debate democrático.

2.4.8 RISCOS, SALVAGUARDAS E DIREITOS

Devido processo: O devido processo é uma salvaguarda fundamental que se tornou aplicável também às decisões de moderação de conteúdo nas relações entre plataformas e usuários. Para concretizar este direito, é necessário institucionalizar mecanismos que garantam fundamentação das decisões *(statements of reasons)*, notificação ao usuário afetado e a oportunidade de recurso aces-

sível. O Art. 17 do DSA europeu é uma referência, pois exige que o provedor encaminhe ao usuário impactado uma "declaração de motivos" clara, explicando a decisão de remoção, bloqueio ou desmonetização. Adicionalmente, o DSA exige sistemas internos de tratamento de reclamações (Art. 20) pelos quais os usuários possam contestar medidas.

Liberdade de expressão & proporcionalidade (remover impulsionamento x manter conteúdo com rótulo, quando adequado): O principal risco da celeridade exigida nos canais de denúncia é o *over-removal,* que pode resultar em censura indireta e enfreamento do discurso legítimo. A salvaguarda central é a proporcionalidade, que exige que qualquer restrição à liberdade de expressão seja necessária e proporcional. No contexto digital, isso implica privilegiar medidas menos restritivas. Em vez de proceder à remoção total, pode ser mais adequado limitar o impulsionamento de conteúdo ou rotulá-los com informações adicionais, quando o caso permitir. A atuação da Justiça Eleitoral deve ser realizada "com a menor interferência possível no debate democrático".

Privacidade/LGPD: minimização de dados no ato da denúncia; retenções e logs proporcionais: A aplicação prática dos canais de denúncia pode gerar impactos sobre a proteção de dados pessoais. A interpretação das normas deve caminhar lado a lado com as garantias de proteção de dados. No desenho dos canais, o DSA, por exemplo, exige que o aviso inclua os dados de contato do denunciante (nome e e-mail), exceto em casos de exploração sexual infantil, sugerindo a minimização dos dados coletados. Além disso, o OSA exige a proteção da privacidade dos usuários ao aplicar medidas de segurança. A necessidade de retenções e logs para fins de *accountability* (como o rastreamento por número de protocolo e relatórios de transparência), deve seguir o princípio da proporcionalidade.

REFERÊNCIAS

AGÊNCIA BRASIL. Entenda a decisão do STF sobre responsabilização das redes sociais. Brasília, 2025. Disponível em: https://agenciabrasil.ebc.com.br/justica/noticia/2025-06/entenda-decisao-do-stf-sobre-responsabilizacao-das-redes-sociais. Acesso em: 11 dez. 2025.

ANGELI, Alzira Ester. Accountability e internet numa perspectiva comparada: a atuação digital das controladorias públicas na América Latina. 2017. Dissertação (Mestrado em Ciência Política) – Universidade Federal do Paraná, Curitiba, 2017.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 dez 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 dez. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. Modelo de Política de Gestão de Registros (Logs) de Auditoria. Versão 2.2. Brasília, DF: MGI, 2024.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 2019. Dispõe sobre propaganda eleitoral. Brasília, DF, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 10 dez. 2025

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 2024. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Brasília, DF, 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 10 dez. 2025.

BRAVO, Jorge dos Reis. Liberdade de expressão na era digital: a reconfiguração de um direito humano? Revista EMERJ, Rio de Janeiro, v. 23, n. 1, p. 81-95, 2021.

ENCARNAÇÃO, Paulo Vitor Faria da. A inconstitucionalidade parcial do art. 19 do Marco Civil da Internet: liberdade de expressão, responsabilidade das plataformas digitais e proteção de direitos fundamentais. Ribeirão Preto, SP: Migalhas, 2025.

FERREIRA, Rafaela. Direito ao devido processo: de onde vem a aposta da regulação de plataformas? IRIS-BH, 2023. Disponível em: https://irisbh.com.br/direito-ao-devido-processo-de-onde-vem-a-aposta-da-regulacao-de-plataformas/. Acesso em: 10 dez. 2025.

GONZALES, Alexandre Arns; BÜLOW, Marisa von. Entre resistência e concessão de transparência: as plataformas digitais colaboraram com as eleições? Revista de Sociologia e Política, v. 32, p. 1-24, 2024. DOI: 10.1590/1678-98732432e018.

ÍNDIA. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Índia: Ministry of Electronics and Information Technology, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Acesso em: 10 dez. 2025.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (Ed.). Educação em um cenário de plataformização e de economia dos dados: problemas e conceitos. São Paulo: Comitê Gestor da Internet no Brasil, 2022.

NYABOLA, Nanjala. Digital democracy, analogue politics: how the internet era is transforming Kenya. Londres: Zed Books, 2018.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Conselho de Direitos Humanos. Report of the detailed findings of the Independent International Fact-Finding Mission on Myanmar. Myanmar: Human Rights Council, 2018. Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/277/04/PDF/G1827704.pdf?OpenElement. Acesso em: 11 dez. 2024.

PARSLEY0_0. O YouTube precisa obrigar os criadores de conteúdo de IA a rotular seus vídeos claramente, e nos dar a opção de escondê-los. Reddit, 2025. Disponível em: https://www.reddit.com/r/youtube/comments/1ct20g8/o_youtube_precisa_obrigar_os_criadores_de/. Acesso em: 11 dez. 2025.

REINO UNIDO. Online Safety Act (OSA). Londres, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 10 dez. 2025.

ROY, S. BJP may have created a monster with its troll army, but Amit Shah understands it may turn on them one day. HuffPost, 2017. Disponível em: https://www.huffpost.com/archive/in/entry/bjp-may--have-created-a-monster-with-its-troll-army-but-amit-shah-understands-it-may-turn-on-them-one--day_a_23204198. Acesso em: 11 dez. 2024.

SILVA, T.; SANTOS, N. Monitoramento dos sites de redes sociais nas eleições brasileiras de 2010. In: MARQUES, F. P. J. A.; SAMPAIO, R. C.; AGGIO, C. (Org.). Do clique à urna: internet, redes sociais e eleições no Brasil. Salvador: EDUFBA, 2013. p. 402-421.

SOUZA, Carlos Eduardo Rehbein de; EUGÊNIO, Letizia Manuella Serqueira; ARAÚJO, Nelcileno Virgílio de Souza. Da Europa ao Brasil: um estudo comparativo entre o GDPR e a LGPD. In: Anais do Workshop sobre as Implicações da Computação na Sociedade, 2025. Cuiabá: SBC, p. 80-123.

UNIÃO EUROPEIA. Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Bruxelas, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. Acesso em: 10 dez. 2025.

ZINGALES, Nicolo et al. TSE, plataformas digitais e desinformação: conceitos relevantes e comentários sobre as Resoluções do TSE. Rio de Janeiro: Lumen Juris, 2025.

2.5 CORREÇÃO E PREVENÇÃO E PROTEÇÃO DE DADOS (ART. 9º-D, III E IV)

Juliana Costa

Art. 9º-D. É dever do provedor de aplicação de internet, que permita a veiculação de conteúdo político-eleitoral, a adoção e a publicização de medidas para impedir ou diminuir a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam atingir a integridade do processo eleitoral, incluindo: (Incluído pela Resolução n.º 23.732/2024)
[...]
III – o planejamento e a execução de ações corretivas e preventivas, incluindo o aprimoramento de seus sistemas de recomendação de conteúdo; (Incluído pela Resolução n.º 23.732/2024)
IV - a transparência dos resultados alcançados pelas ações mencionadas no inciso III do caput deste artigo; (Incluído pela Resolução n.º 23.732/2024).

25.1 VISÃO GERAL E OBJETIVOS

Objetivo: elaborar um texto exemplificativo e expositivo abordando os requisitos apresentados como adoção e publicização de medidas da desinformação, relacionados ao planejamento e a execução de ações corretivas e preventivas visando o aprimoramento dos provedores de aplicação de internet em relação aos sistemas de recomendação e de conteúdo relacionado a um melhor direcionamento do conteúdo político-eleitoral e que o planejamento e a execução destas ações tragam resultados transparentes, garantindo *accountability*.

Guia de Perguntas:

- O que é um provedor de aplicação de internet para fins eleitorais?
- Quais são as medidas para impedir ou diminuir a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam atingir a integridade do processo eleitoral?
- Como se realizam o planejamento e a execução de ações corretivas e preventivas com vistas a evitar a propagação de desinformação eleitoral?
- De que maneira é possível o aprimoramento dos sistemas dos provedores de aplicação da internet?
- Como pode ser comprovada a transparência dos resultados alcançados pelas ações corretivas e preventivas, incluindo o aprimoramento de seus sistemas de recomendação de conteúdo?

25.2 BASE NORMATIVA (BRASIL)

Constituição Federal de 1988 - Garantia dos direitos fundamentais como a privacidade, a intimidade, a honra e a imagem (Art. 5º, X), que são a base para toda a discussão sobre proteção de dados (Brasil, 1988).

Lei Geral de Proteção de Dados (LGPD) - Lei n.º 13.709/2018 – Definição de dados pessoais, estabelecimento de princípios, direitos dos titulares, obrigações dos agentes de tratamento, deveres de transparência e boas práticas (Brasil, 2018).

TSE Res. 23.732/2024, Art. 9º-D, III e IV - obriga a realização de planejamento e a execução de ações corretivas e preventivas, incluindo o aprimoramento de seus sistemas de recomendação de conteúdo eleitoral (Brasil, 2024).

Marco Civil da Internet - Lei n.º 12.965/2014 - princípios basilares para o uso da internet no Brasil, proteção da privacidade em ambientes online (Brasil, 2014).

Código Civil - Lei n.º 10.406/2002 - Proteção dos direitos de personalidade, vida privada e aplicação em situações caracterizadoras de Responsabilidade Civil (Brasil, 2002).

Contexto regulatório adjacente: **Resolução TSE n.º 23.610 / 2019, Lei n.º 9.504/1997 (Lei das Eleições) - em especial os arts. que conferem ao TSE competência para regulamentar propaganda eleitoral, Código Eleitoral (Lei n.º 4.737/1965) - art. 323,** Cartilha TSE/FGV sobre desinformação, decisões do TSE sobre responsabilização das plataformas, que elevam o dever de cuidado e resposta a notificações extrajudiciais em certos casos (Brasil, 1965, 1997).

2.5.3 METODOLOGIA DE *BENCHMARKING*

Seleção de jurisdições: UE (DSA), Reino Unido, Canadá (*Canada Elections Act*), Austrália (*Authorisation* em comunicações eleitorais), Estados Unidos (FEC 11 CFR 110.11 (*disclaimers* e regras de internet) e iniciativas tipo *Honest Ads Act* (padrões de transparência para anúncios online), Índia - *Voluntary Code of Ethics* com plataformas (ECI) e materiais oficiais sobre redes sociais/*"fake news" - IT Rules*, México – estrutura do INE para acesso e regras de mídia eleitoral (referência regional).

Unidades de comparação (possíveis critérios):

- Acessibilidade: clareza do acesso do cidadão/partes às regras e canais (linguagem simples, materiais didáticos, canais para denúncia/consulta). Evidências: cartilhas, FAQs, portais).
- Usabilidade: facilidade de uso dos fluxos digitais (denunciar, pedir remoção/correção, consultar repositórios de anúncios) e padrões de UX. Evidências: formulários, repositórios (p.ex. ad registries no Canadá).
- Fluxo e prazos (SLAs para análise/remoção/contestação; previsibilidade em períodos eleitorais (janelas, urgência). Evidências: prazos nas normas/guias e comunicados oficiais.
- Devido processo: garantias a denunciados e denunciantes (notificação, contraditório, recurso; bases de remoção claras). Evidências: guias de aplicação/decisões.
- Transparência: rotulagem/*imprint*, *disclaimer* do patrocinador, arquivos públicos de anúncios, relatórios de risco/medidas. Evidências: DSA, *UK digital imprints*, FEC, registros no Canadá.
- Integrações: cooperação com plataformas (APIs, ofícios eletrônicos), interoperabilidade entre justiça eleitoral/autoridades e provedores. Evidências: códigos de conduta, fluxos com plataformas (ex.: Índia).
- Mitigações de abuso: limites a microtargeting político, *IA/deepfakes*, repetidores de desinformação; obrigações de arquivo, rastreabilidade, riscos sistêmicos. Evidências: Reg. (UE) 2024/900; DSA; novidades do TSE 2024.
- Governança & *accountability*: quem decide, como presta contas (relatórios, auditorias, sanções, precedentes). Evidências: decisões/sentenças, multas (p.ex., caso na Austrália sobre ausência de autorização em posts).

2.5.4 *BENCHMARK* INTERNACIONAL (SÍNTESE COMPARATIVA)

União Europeia – DAS

Lei dos Serviços Digitais (DSA) - Regulamento (UE) 2022/2065: Foca na responsabilidade das plataformas. O Artigo 34º exige que as VLOPs realizem avaliações de risco anuais sobre como seus serviços podem ser usados para disseminar conteúdo ilegal ou manipular processos eleitorais. Com base nessa avaliação, o Artigo 35º as obriga a implementar medidas de mitigação "razoáveis, proporcionais e eficazes". Isso inclui, por exemplo, adaptar seus sistemas de moderação de conteúdo e algoritmos de recomendação antes, durante e após um período eleitoral (União Europeia, 2022).

DSA (Artigos 15, 24 e 42): Impõe obrigações de transparência. As plataformas devem publicar relatórios detalhando suas atividades de moderação de conteúdo (quantos conteúdos foram removidos, por qual motivo, etc.).

As VLOPs devem manter um repositório público de toda a publicidade veiculada (Artigo 39º), informando quem pagou pelo anúncio, o valor e os parâmetros de segmentação utilizados. Além disso, devem fornecer acesso aos seus dados a pesquisadores e reguladores para auditoria externa (Artigo 40º), permitindo uma análise independente da eficácia de suas medidas contra a desinformação (Comissão Europeia, 2024).

Código de Práticas sobre Desinformação (UE): Embora voluntário, este código, assinado pelas principais plataformas, estabelece compromissos para desmonetizar fontes de desinformação, aumentar a transparência da publicidade política e capacitar os usuários a identificar conteúdo falso (Comissão Europeia, 2022).

Canadá

O Canadá possui uma abordagem setorial, com leis distintas para os setores público e privado:

- *Canada Elections Act* – s. 325.1: plataformas on-line que vendem espaço publicitário devem manter e publicar repositório/registro de anúncios políticos e partidários (Canadá, [202-?]).
- Proteção de dados por partidos federais
- Partidos devem publicar política de proteção de dados (requisitos detalhados na CEA, com reforços recentes via projetos C-47/C-65); OPC + *Elections Canada* emitiram orientações conjuntas para essas políticas.
-

Austrália

Partidos políticos possuem uma isenção significativa:

- *Commonwealth Electoral* Act 1918, s. 321D: exige declaração de autorização em comunicações eleitorais (fonte/autor). A AEC publica guias práticos (Austrália, 1918).

Desinformação - dever das plataformas:

- Código Australiano de Prática sobre Desinformação e Misinformação (DIGI): voluntário, com relatórios de transparência supervisionados pela ACMA; proposta de lei para poderes mandatórios foi retirada em 2024.

Estados Unidos

Transparência de propaganda:

- FEC - 11 CFR §110.11 *(disclaimers)*: anúncios/"*public communications*" (incluindo internet) devem identificar o pagador e informações de autorização; regra de 2022 atualizou exigências para ambientes on-line (Estados Unidos, [20--?]).

Proteção de dados:

- Não há lei federal geral de proteção de dados aplicável a campanhas; o tema é regulado por leis setoriais/estaduais (p.ex., privacidade da Califórnia), práticas da FTC e autorregulação. (Sem um dever federal específico de mitigação de desinformação por provedores, à luz da Primeira Emenda).

Índia

Deveres de intermediários (provedores) e mitigação:

- *IT Rules 2021 (Intermediary Guidelines and Digital Media Ethics Code)*, c/ alterações 2022-2023: devida diligência, mecanismos de queixa, remoção após ordem e maior responsabilização de *"Significant Social Media Intermediaries"*. Regulam remoções e transparência de processos, com efeitos diretos em períodos eleitorais.
- *Voluntary Code of Ethics (2019):* plataformas firmaram com a Election Commission of India compromissos de resposta célere a solicitações, transparência e cooperação durante o pleito.

Proteção de dados:

- *Digital Personal Data Protection Act,* 2023: regime transversal de proteção de dados (bases legais, consentimento, direitos, deveres do controlador), aplicável a tratamento de dados em campanhas e por plataformas

México

Proteção de dados no âmbito eleitoral

- LFPDPPP (privados) e LGPDPPSO (sujeitos obrigados): regem proteção de dados; no âmbito eleitoral, o INE possui Reglamento en Materia de Protección de Datos Personales e políticas específicas para o Padrón/Lista Nominal.

Transparência/propaganda e combate à desinformação

- LGIPE estrutura regras de propaganda e procedimentos eleitorais; o INE vem celebran-

do parcerias e programas com plataformas/OSC para alfabetização midiática e redução de desinformação (p.ex., Soy Digital com a Meta).
- Não há, hoje, um dever geral legal explícito imposto às plataformas para remover "notoriamente inverídicos" em âmbito federal; a atuação tem sido via cooperação, diretrizes e enforcement de regras eleitorais de conteúdo patrocinado/transmissão.).

25.5 INTERPRETAÇÃO DO ART. 9º, INCISO III E IV À LUZ DO *BENCHMARKING* INTERNACIONAL

A Resolução TSE n.º 23.732/2024 apresenta a correlação mais direta e textual, dado o foco explícito e detalhado na proteção da integridade do processo eleitoral brasileiro contra desinformação. O DSA, por sua vez, oferece um arcabouço normativo para a União Europeia que cobre os mesmos conceitos, aplicando-os às grandes plataformas de forma sistêmica.

O DSA estabelece obrigações de gestão de riscos sistêmicos para as Plataformas em Linha de Muito Grande Dimensão (VLOPs) e Motores de Pesquisa em Linha de Muito Grande Dimensão (VLOSEs), que abrangem precisamente a desinformação e os processos eleitorais.

Considerando (82): Define explicitamente a terceira categoria de riscos sistêmicos que deve ser avaliada pelas grandes plataformas, correlacionando-se com a integridade do processo eleitoral: Considerando (84): Enfatiza a inclusão de informações não ilegais que contribuem para esses riscos, o que abrange os "fatos notoriamente inverídicos ou gravemente descontextualizados":

- Artigo 34.º, n.º 1, alínea c): Exige a avaliação diligente e anual dos riscos sistêmicos decorrentes de seus serviços, incluindo os "efeitos negativos reais ou previsíveis no discurso cívico e nos processos eleitorais".
- Artigo 35.º, n.º 1: Impõe a adoção de medidas de atenuação adaptadas aos riscos sistêmicos identificados, o que engloba as "ações corretivas e preventivas":
- Artigo 35.º, n.º 1, alínea d): Aborda diretamente a necessidade de aprimoramento tecnológico:
- Considerando (88): Reforça a diligência na adaptação dos sistemas algorítmicos:
- Artigo 42.º, n.º 4: Obriga as VLOPs/VLOSEs a transmitirem e disponibilizarem ao público os resultados da gestão de riscos, garantindo a transparência:

O *Online Safety Act* do Reino Unido aborda a necessidade de combater a desinformação e garantir a transparência das medidas tecnológicas (Tecnologia Proativa) e a gestão de riscos, embora não utilize a terminologia "processo eleitoral" de forma tão específica nas obrigações citadas.

- Seção 165 (1A)(e) e (1B): Impõe deveres de educação midiática à OFCOM, visando mitigar a exposição do público à desinformação:
- Seção 588, (4) e (7): Trata da publicização de medidas e sistemas internos (correlato ao aprimoramento de sistemas e transparência):

25.6 EVIDÊNCIAS E ESTUDOS DE CASO

Brasil

- Eleições Presidenciais de 2022 - Desinformação no WhatsApp e Telegram: As eleições presidenciais brasileiras de 2022 foram marcadas por intensa disseminação de desinformação através de aplicativos de mensagens criptografadas, especialmente WhatsApp e Telegram.
- Acordos TSE-Plataformas Digitais para as Eleições de 2024: Em agosto de 2024, o TSE firmou memorandos de entendimento com as principais plataformas digitais (Meta, Google, TikTok, X, Telegram, LinkedIn e Kwai) para combater a desinformação nas eleições municipais.

Índia

- Eleições Gerais de 2024 - Deepfakes e Desinformação Gerada por IA: As eleições gerais indianas de 2024 *(Lok Sabha)* foram marcadas pelo uso massivo de deepfakes e conteúdo gerado por IA para influenciar eleitores.
- WhatsApp vs. Governo da Índia - Regra de Rastreabilidade (*IT Rules* 2021): Em maio de 2021, o WhatsApp processou o governo indiano contestando a constitucionalidade da regra de rastreabilidade prevista nas Information Technology *(Intermediary Guidelines and Digital Media Ethics Code)* Rules, 2021.
- Uso de WhatsApp *"Pramukhs"* em Campanhas Políticas: Partidos políticos indianos desenvolveram redes sofisticadas de administradores de grupos do WhatsApp (chamados *"Pramukhs"*) para disseminar propaganda política e, em alguns casos, desinformação.

Reino Unido

- *Cambridge Analytica* - Facebook Data Breach (2016-2018): O escândalo *Cambridge Analytica* representa um dos casos mais emblemáticos de uso indevido de dados pessoais para manipulação eleitoral, afetando tanto as eleições presidenciais dos EUA (2016) quanto o referendo do Brexit no Reino Unido (2016).

União Européia

- Comissão Europeia vs. TikTok - Violação do DSA (Dezembro 2024): Em 16 de dezembro de 2024, a Comissão Europeia abriu procedimento formal contra o TikTok por suspeita de violação do DSA.
- Romênia Cancela Eleições por Interferência Estrangeira (Dezembro 2024) : Em 6 de dezembro de 2024, a Romênia tornou-se o primeiro país da UE a cancelar uma eleição devido a interferência estrangeira em plataformas digitais.
- Deepfakes nas Eleições Europeias - Aplicação do *AI Act:* As eleições europeias de 2024 testemunharam uso significativo de deepfakes, levantando questões sobre a aplicação do futuro *EU AI Act*.

25.7 RECOMENDAÇÕES (NORMATIVAS E OPERACIONAIS)

Resolução TSE n.º 23.732/2024 (Brasil): Dever de adoção e publicização de medidas para impedir ou diminuir a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam atingir a integridade do processo eleitoral.

- Art. 9º-D, caput: Estabelece um dever de diligência explícito para provedores que veiculam conteúdo político-eleitoral, tornando mandatório o combate à desinformação que afete a integridade eleitoral.
- Planejamento e a execução de ações corretivas e preventivas, incluindo o aprimoramento de seus sistemas de recomendação de conteúdo.
- Art. 9º-D, inciso III: Requer o aperfeiçoamento de sistemas algorítmicos (sistemas de recomendação), reconhecendo o papel desses sistemas na amplificação ou diminuição da circulação de desinformação.

A transparência dos resultados alcançados pelas ações mencionadas.

- Art. 9º-D, inciso IV: Impõe a publicização dos resultados das ações corretivas e preventivas, fundamental para a responsabilização e o controle público da eficácia da mitigação de riscos.
- Dever de Cuidado e Avaliação de Risco.
- Art. 9º-D, § 4º e inciso V: As medidas decorrem da função social e do dever de cuidado do provedor. O provedor deve elaborar, em ano eleitoral, uma avaliação de impacto de seus serviços sobre a integridade do processo eleitoral para implementar medidas eficazes de mitigação.

Relação com Dados Pessoais e Privacidade:

- Art. 33-B, inciso I; Art. 33-D: Embora o dever de diligência (Art. 9º-D) não seja diretamente sobre proteção de dados, o sistema de recomendação (inciso III) se baseia em perfilamento. O Art. 33-B exige acesso facilitado às informações sobre o tratamento de dados usados para perfilamento de usuários com vistas ao microdirecionamento da propaganda eleitoral. O Relatório de Impacto à Proteção de Dados (RIPD) (Art. 33-D) é exigido em casos de alto risco que envolvam tratamento em larga escala e uso de tecnologias inovadoras para perfilamento de eleitoras e eleitores.

Regulamento (UE) 2022/2065 ***(Digital Services Act - DSA)***

O DSA não aborda a desinformação como conteúdo ilegal em si, mas sim como um risco sistémico que afeta os processos democráticos, impondo obrigações de gestão de risco e transparência de sistemas algorítmicos às Plataformas em Linha de Muito Grande Dimensão (VLOPs) e aos Motores de Pesquisa em Linha de Muito Grande Dimensão (VLOSEs).

- Recomendação Normativa e Operacional (Foco em Sistemas e Transparência)
- Risco Sistémico (Integridade Eleitoral e Desinformação):
- Considerando (82); Artigo 34.º, n.º 1, alínea c): Classifica explicitamente os efeitos nega-

tivos nos processos democráticos e eleitorais como uma categoria de risco sistémico que deve ser avaliada. Considerando (84) exige atenção especial à difusão de "conteúdos enganosos ou suscetíveis de induzir em erro, como a desinformação".

Planejamento e execução de ações corretivas e preventivas:

- Artigo 35.º, n.º 1: Obriga VLOPs/VLOSEs a adotarem medidas de atenuação razoáveis, proporcionadas e eficazes, adaptadas aos riscos sistêmicos identificados, respeitando os direitos fundamentais.

Aprimoramento de sistemas de recomendação de conteúdo:

- Considerando (88); Artigo 35.º, n.º 1, alínea d): Requer diligência para "testar e, se necessário, adaptar os seus sistemas algorítmicos, nomeadamente os seus sistemas de recomendação".

Transparência e publicização dos resultados:

- Artigo 42.º, n.º 4; Artigo 37.º: VLOPs/VLOSEs devem publicar e transmitir relatórios com os resultados da avaliação dos riscos (Art. 34.º) e as medidas de atenuação implementadas (Art. 35.º). As plataformas estão sujeitas a auditorias independentes anuais para verificar o cumprimento dessas obrigações.

Relação com Proteção de Dados (Mitigação de Riscos Algorítmicos):

- Artigo 38.º; Considerando (118): Impõe uma medida crucial para a privacidade: VLOPs/VLOSEs que utilizam sistemas de recomendação devem oferecer pelo menos uma opção que não se baseie na definição de perfis (na aceção do RGPD), dando ao usuário controle sobre a coleta de dados e a personalização. Isso mitiga o risco de que o perfilamento direcionado (que pode ser usado para desinformação) seja a única opção.

***Online Safety Act* 2023 (Reino Unido)**

O OSA exige que as plataformas (especialmente as de Categoria 1 e 2A) lidem com riscos de conteúdo e priorizem a proteção da privacidade e dos direitos democráticos ao fazê-lo.

- Recomendação Normativa e Operacional (Foco em Sistemas e Transparência)
- Combate à Desinformação/Fatos Inverídicos:
- Seção 610, (1A)(e); Seção 152: OFCOM deve tomar medidas para aumentar a conscientização pública e a compreensão sobre a natureza e o impacto da desinformação e misinformation, e reduzir a exposição a elas. Menciona o Comité Consultivo sobre desinformação e misinformation.

Adoção e publicização de medidas (Sistemas Proativos):

- Seção 577 (7); Seção 571 (7): Impõe o dever de incluir nas declarações públicas (Termos de Serviço/Declaração) informações sobre qualquer tecnologia proativa utilizada para cumprir os deveres de segurança (incluindo o tipo de tecnologia, quando é utilizada e

como funciona). Isso se correlaciona com o “aprimoramento de seus sistemas” e “publicização de medidas”.

Planejamento de ações preventivas (Avaliação de Impacto):

- Seção 574 (4) e (6): Exige que os serviços de Categoria 1 realizem e publiquem avaliações de impacto (impact assessments) ao definirem medidas e políticas de segurança, ligando-se ao “planejamento e execução de ações preventivas”.

Relação com Proteção de Dados (Sistemas de Controle):

- Seção 573 (3); Seção 602 (j): As medidas e políticas de segurança devem ter “particular atenção à importância de proteger os usuários contra uma violação de qualquer disposição estatutária ou regra legal relativa à privacidade”, incluindo o tratamento de dados pessoais. O risco de violação de privacidade também deve ser considerado ao impor o uso de tecnologia proativa (algorítmica) para detecção de conteúdo.

25.8 RISCOS, SALVAGUARDAS E DIREITOS

TSE 23.732/2024 (Brasil)

- Art. 9º-D, III (Aprimoramento de sistemas de recomendação) ; Art. 9º-D, V (Avaliação de Impacto Eleitoral/Violência política de gênero) ; Art. 9º-D, IV (Transparência de resultados)
- Art. 33-D (RIPD obrigatório em alto risco/perfilamento) ; Art. 33-B, I (Acesso a dados de perfilamento para microdirecionamento)

DSA (UE) 2022/2065

- Art. 35.º, n.º 1, alínea d) (Adaptação de sistemas de recomendação) ; Considerando (82), (84) (Risco sistêmico: desinformação e processos democráticos) ; Art. 42.º, n.º 4 (Transparência da gestão de riscos)
- Art. 38.º (Opção de sistema de recomendação sem perfilamento) ; Art. 26.º, n.º 3 (Proibição de publicidade com dados sensíveis) ; Art. 34.º, n.º 1, alínea b) (Risco aos dados pessoais)

OSA 2023 (Reino Unido)

- Sec. 563(12) e 568(7) (Transparência da tecnologia proativa/algorítmica); Sec. 565(7) (Publicação de medidas para proteger a liberdade de expressão).
- Sec. 564(3) (Dever de proteger os usuários contra violações de privacidade e dados pessoais); Sec. 588(j) (Risco de violação de privacidade por tecnologia proativa); Sec. 565(7) (Dever de publicar medidas para proteger a privacidade) .

REFERÊNCIAS

AL JAZEERA MEDIA INSTITUTE. Elections and misinformation - India case study. AJMI Reports, 2024.

ALVES, M. F. Governança eleitoral da desinformação em plataformas digitais no Brasil (2017-2024). 2025. Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) - Universidade Federal de Santa Catarina, Florianópolis, 2025. Disponível em: https://repositorio.ufsc.br/handle/123456789/265993. Acesso em: 11 dez. 2025.

AUSTRÁLIA. Commonwealth Electoral Act 1918. Austrália: Commonwealth Consolidated Acts, 1918. Disponível em: https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/cea1918233/. Acesso em: 11 dez. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Tribunal Superior Eleitoral. Guia orientativo sobre tratamento de dados pessoais em campanhas eleitorais. Brasília, DF, 2022.

BRASIL. Código Eleitoral - Lei nº 4.737, de 15 de julho de 1965. Disponível em: https://www.tse.jus.br/legislacao/codigo-eleitoral/codigo-eleitoral-1/codigo-eleitoral-lei-nb0-4.737-de-15-de-julho-de-1965. Acesso em: 11 dez. 2025.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 out. 2025.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 dez. 2025.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 2019. Dispõe sobre propaganda eleitoral. Brasília, DF, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 10 dez. 2025

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 2024. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Brasília, DF, 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 10 dez. 2025.

BRASIL. Tribunal Superior Eleitoral. Relatório de ações e resultados – Eleições 2022. Brasília, DF: TSE, 2023.

BRASIL. Tribunal Superior Eleitoral. Acesse a íntegra dos acordos com plataformas digitais para combater mentiras nas eleições 2024. Notícias TSE, Brasília, 2024.

CADWALLADR, C.; GRAHAM-HARRISON, E. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian, [S. l.], 2018.

CANADÁ. Canada Elections Act. Governo do Canadá, [202-?]. Disponível em: https://laws-lois.justice.gc.ca/eng/acts/e-2.01/. Acesso em: 11 dez. 2025.

COMISSÃO EUROPEIA. The strengthened code of practice on disinformation 2022. [S. l.]: Comissão Europeia, 2022. Disponível em: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation. Acesso em: 10 dez. 2025.

COMISSÃO EUROPEIA. Commission opens formal proceedings against TikTok under the Digital Services Act. Press Release IP/24/6487, 2024.

COMISSÃO EUROPEIA. Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065. Official Journal of the European Union, [S. l.], 2024. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403014. Acesso em: 10 dez. 2025.

D'ANDREA, A.; FUSACCHIA, G.; D'ULIZIA, A. Policy review: countering disinformation in the digital age - policies and initiatives to safeguard democracy in Europe. Information Polity, [S. l.], 2025.

FIELDFISHER. UK law in the era of global platforms: how does the Online Safety Act apply? Insights, [S. l.], 2025.

FRAGALE, Mauro; GRILLI, Valentina. Deepfake, deep trouble: the European AI Act and the fight against AI-generated misinformation. Columbia Journal of European Law, 2024. Disponível em: https://cjel.law.columbia.edu/preliminary-reference/2024/deepfake-deep-trouble-the-european-ai-act-and-the-fight-against-ai-generated-misinformation/. Acesso em: 11 dez. 2025.

GONZALES, A. A.; BÜLOW, M. Entre resistência e concessão de transparência: as plataformas digitais colaboraram com as eleições? Revista de Sociologia e Política, [S. l.], v. 32, 2024.

HALE, S. A. et al. Analyzing misinformation claims during the 2022 Brazilian general election. International Journal of Public Opinion Research, [S. l.], v. 36, n. 3, 2024.

ÍNDIA. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Índia: Ministry of Electronics and Information Technology, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Acesso em: 10 dez. 2025.

INTERNET SOCIETY. Traceability in end-to-end encrypted environments. Policy Brief, 2024.

KUMAR, S. Traceability and end-to-end encryption: an analysis of India's intermediary rules mandating traceability. SSRN Electronic Journal, [S. l.], 2022.

MOZILLA FOUNDATION. Party politics and WhatsApp Pramukhs - India case study. Global Elections Casebook, 2024.

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE. Impact of the Digital Services Act: a Facebook case study. Riga, [S. l.], 2025.

OFCOM. Ofcom issues update on Online Safety Act investigations. Press Release, [S. l.], 2025.

PARLAMENTO EUROPEU. Mis- and disinformation on social media and related risks to elections. At a Glance, [S. l.], 2024.

REINO UNIDO. Online Safety Act (OSA). Londres, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 10 dez. 2025.

ROSSINI, P. et al. Explaining beliefs in electoral misinformation in the 2022 Brazilian election: the role of ideology, political trust, social media, and messaging apps. Harvard Kennedy School Misinformation Review, 2023.

SHUKLA, A. K.; TRIPATHI, S. AI-generated misinformation in the election year 2024: measures of European Union. Frontiers in Political Science, [S. l.], v. 6, 2024.

STOCKWELL, S. AI-enabled influence operations: threat analysis of the 2024 UK and European elections. Centre for Emerging Technology and Security, Alan Turing Institute, 2024.

UNIÃO EUROPEIA. Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Bruxelas, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. Acesso em: 10 dez. 2025.

ESTADOS UNIDOS. Code of Federal Regulations (CFR). Legal Information Institute, [20--?]. Disponível em: https://www.law.cornell.edu/cfr/text/11/110.11. Acesso em: 11 dez. 2025.

WHITE & CASE. European Commission publishes “DSA Elections Toolkit” to support digital services. Alert, [S. l.], 2025.

WILSON, R. Cambridge Analytica, Facebook, and influence operations: a case study and anticipatory ethical analysis. European Conference on Cyber Warfare and Security, 2019.

WORLD ECONOMIC FORUM. Year of elections: lessons from India’s fight against AI-generated misinformation. WEF Stories, 2024.

2.6 FUNÇÃO SOCIAL E DEVER DE CUIDADO (ART. 9º-D, §§ 1º, 2º E 4º, E ART. 32, PARÁGRAFO ÚNICO)

Marina Lucena e Bárbara Pontalti

Art. 9º-D. É dever do provedor de aplicação de internet, que permita a veiculação de conteúdo político-eleitoral, a adoção e a publicização de medidas para impedir ou diminuir a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam atingir a integridade do processo eleitoral, incluindo:

I - a elaboração e a aplicação de termos de uso e de políticas de conteúdo compatíveis com esse objetivo;

II - a implementação de instrumentos eficazes de notificação e de canais de denúncia, acessíveis às pessoas usuárias e a instituições e entidades públicas e privadas;

III – o planejamento e a execução de ações corretivas e preventivas, incluindo o aprimoramento de seus sistemas de recomendação de conteúdo;

IV - a transparência dos resultados alcançados pelas ações mencionadas no inciso III do caput deste artigo;

V – a elaboração, em ano eleitoral, de avaliação de impacto de seus serviços sobre a integridade do processo eleitoral, a fim de implementar medidas eficazes e proporcionais para mitigar os riscos identificados, incluindo quanto à violência política de gênero, e a implementação das medidas previstas neste artigo;

VI – o aprimoramento de suas capacidades tecnológicas e operacionais, com priorização de ferramentas e funcionalidades que contribuam para o alcance do objetivo previsto no caput deste artigo.

§ 1º É vedado ao provedor de aplicação, que comercialize qualquer modalidade de impulsionamento de conteúdo, inclusive sob a forma de priorização de resultado de busca, disponibilizar esse serviço para veiculação de fato notoriamente inverídico ou gravemente descontextualizado que possa atingir a integridade do processo eleitoral.

§ 2º O provedor de aplicação, que detectar conteúdo ilícito de que trata o caput deste artigo ou for notificado de sua circulação pelas pessoas usuárias, deverá adotar providências imediatas e eficazes para fazer cessar o impulsionamento, a monetização e o acesso ao conteúdo e promoverá a apuração interna do fato e de perfis e contas envolvidos para impedir nova circulação do conteúdo e inibir comportamentos ilícitos, inclusive pela indisponibilização de serviço de impulsionamento ou monetização.

§ 3º A Justiça Eleitoral poderá determinar que o provedor de aplicação veicule, por impulsionamento e sem custos, o conteúdo informativo que elucide fato notoriamente inverídico ou gravemente descontextualizado antes impulsionado de forma irregular, nos mesmos moldes e alcance da contratação.

§ 4º As providências mencionadas no caput e nos § 1º e 2º deste artigo decorrem da função social e do dever de cuidado dos provedores de aplicação, que orientam seus termos de uso e a prevenção para evitar ou minimizar o uso de seus serviços na prática de ilícitos eleitorais, e não dependem de notificação da autoridade judicial.

Art. 32. Aplicam-se ao provedor de aplicação de internet em que divulgada a propaganda eleitoral de candidato, de partido político ou de coligação as penalidades previstas nesta Resolução se, no prazo determinado pela Justiça Eleitoral, contado a partir da notificação de decisão judicial específica sobre a existência de propaganda irregular, não tomar providências para a cessação

dessa divulgação (Lei n.º 9.504/1997, art. 57-F, caput , c.c. a Lei n.º 12.965/2014, art. 19).
Parágrafo único. O provedor de aplicação de internet só será considerado responsável pela divulgação da propaganda se a publicação do material for comprovadamente de seu prévio conhecimento (Lei n.º 9.504/1997, art. 57-F, parágrafo único).

26.1 VISÃO GERAL E OBJETIVOS

Objetivo: interpretar o alcance do Art. 9º-D, §§ 1º, 2º e 4º, e art. 32, parágrafo único (o que significa "função social" e "dever de cuidado" dos provedores de aplicação) e comparar com boas práticas e obrigações em outras jurisdições.

Guia de Perguntas: Sobre o artigo 9º-D, §§1º, 2º e 4º:

- Quais requisitos mínimos são necessários para configurar uma "providência imediata e eficaz" para fazer cessar o impulsionamento, a monetização e o acesso ao conteúdo?
- Quais prazos são considerados como "razoáveis"?
- O que configura o cumprimento da função social e do dever de cuidado dos provedores de aplicação?

Sobre o artigo 32, parágrafo único:

- Quando se considera que o material publicado é de prévio conhecimento do provedor de aplicação?

26.2 BASE NORMATIVA (BRASIL)

TSE Res. 23.610, Art. 9º-D, §§ 1º, 2º e 4º - veda que o provedor de aplicação que comercialize impulsionamento de conteúdo se utilize desse serviço, incluindo a priorização no resultado de busca, para veicular fato notoriamente inverídico ou gravemente descontextualizado que possa atingir a integridade do processo eleitoral. Quando esse conteúdo for detectado ou houver notificação, deve o provedor adotar providências imediatas e eficazes para cessar o impulsionamento, monetização e o acesso. O §4º esclarece que essas providências se justificam em razão da função social e do dever de cuidado dos provedores de aplicação, que devem atuar para evitar os ilícitos eleitorais.

TSE Res. 23.610, Art. 32, parágrafo único - estabelece uma limitação para a responsabilidade do provedor de aplicação de internet, o qual só será considerado responsável pela divulgação da propaganda se a publicação do material for comprovadamente de seu conhecimento prévio. Contexto regulatório adjacente:

Artigo 170 da Constituição brasileira de 1988: função social na ordem econômica, de modo que as empresas que atuam no Brasil também devem se guiar por tal princípio. Nesse sentido, devem objetivar a obtenção de benefícios para a coletividade (Brasil, 1988).

Código Civil de 2002: a liberdade contratual deve respeitar a função social do contrato (artigo 421) (Brasil, 2002).

Marco Civil da Internet (MCI, Lei n.º 12.965/2014): necessário que o uso da internet no Brasil respeite a finalidade social da rede (artigo 2º, VI). Além disso, os agentes devem ser responsabilizados de acordo com suas atividades (artigo 3º, VI). O artigo 6º também reafirma que a internet deve ser considerada como instrumento para a promoção do desenvolvimento humano, econômico, social e cultural (Brasil, 2014).

Artigo 19 do MCI: previa que o provedor de aplicações de internet somente poderia ser responsabilizado pelos danos de conteúdo gerado por terceiros caso descumprisse ordem judicial específica. No entanto, essa norma foi considerada parcialmente inconstitucional pelo STF, que decidiu pela ponderação dessa necessidade de decisão judicial prévia. Assim, destacam-se as decisões recentes do STF sobre responsabilização das plataformas, que elevam o dever de cuidado e resposta a notificações extrajudiciais em certos casos.

Lei Geral de Proteção de Dados brasileira (LGPD, Lei n.º 13.709/2018): princípios de transparência, segurança e prevenção, além da responsabilização e prestação de contas devem ser considerados pelas empresas que realizam tratamento de dados pessoais (art. 6º, incisos VI, VII, VIII, X) (Brasil, 2018).

Lei das Eleições (Lei n.º 9.504/97): direito de resposta no artigo 58, que deve ser exercido por qualquer veículo de comunicação social. Essa previsão concretiza a ideia de integridade informacional e de dever de cuidado, cumprindo a função social de informar a população de modo devido (Brasil, 1997).

Portaria n.º 351/2023 do Ministério da Justiça e Segurança Pública (MJSP): impõe que as empresas atuem de acordo com o "dever geral de cuidado", derivado do Código Civil e do corolário da boa-fé objetiva, correspondendo a um dever indisponível, que exige uma conduta ativa das partes, de modo e evitar danos aos contratantes na relação obrigacional estabelecida entre usuário e plataforma de rede social (Brasil, 2023).

26.3 METODOLOGIA DE *BENCHMARKING*

Seleção de jurisdições: UE (DSA), Reino Unido (OSA), Índia *(IT Rules).*

Unidades de comparação (possíveis critérios)

Dever de diligência e atuação proativa: cumprindo seu dever de atuar em prol de objetivos sociais como a integridade informacional durante as eleições, há o dever de cuidado e, nesse sentido, desenvolvem-se obrigações de identificar, prevenir e mitigar riscos relacionados a conteúdos ilícitos, desinformativos ou danosos, mesmo sem ordem judicial.

Mecanismos de notificação e ação *("notice and action"):* sistemas internos de recebimento, análise e resposta a notificações de conteúdo ilegal (oriundos dos usuários, autoridades judiciais ou de mecanismos de detecção automática).

Dever de cuidado e responsabilidade compartilhada: alcance do *duty of care* (como previsto no OSA); papel da boa-fé das plataformas e da prevenção de danos.

Avaliação e mitigação de riscos sistêmicos: obrigações de mapeamento e gestão de riscos eleitorais, informacionais e de segurança pública.

Governança e auditorias independentes: deveres de registro, auditoria e prestação de contas sobre as medidas adotadas; existência de autoridades fiscalizadoras.

Critério	União Europeia - *Digital Service Act* (DSA)	Reino Unido - *Online Safety Act* (OSA)	Índia – *IT Rules*
Dever de diligência e atuação proativa	Considerando 2: explicita sobre os requisitos de atuação diligente dos prestadores de serviços intermediários sobre conteúdos ilegais, desinformação e outros riscos sociais. Considerando 22: para que haja isenção de responsabilidade, o prestador deve atuar com diligência na supressão de conteúdos ilegais, seja por notificação de terceiros ou iniciativa própria. Considerando 40: menciona que um ambiente em linha seguro e transparente necessita de um conjunto claro, eficaz, previsível e equilibrado de obrigações de devida diligência dos prestadores. Art. 6: a responsabilidade do prestador quanto às informações armazenadas a pedido do usuário somente se configura após o conhecimento efetivo da ilegalidade. A partir desse momento, impõe-se o dever de agir de forma célere e diligente para suprimir ou restringir o acesso ao conteúdo ilícito, tornando a isenção de responsabilidade condicional ao cumprimento desse dever de atuação imediata. Art. 9: operacionaliza o dever de agir quando houver decisão judicial ou administrativa, mas, interpretado em conjunto com os considerandos anteriores, reforça o caráter de resposta célere e responsável.	Em sua introdução, o OSA adota o princípio do safe by design, o qual exige que os serviços sejam projetados e operados reduzindo riscos antes de sua ocorrência. A Seção 1 estabelece deveres de transparência e accountability, impondo que provedores ajam de modo aberto, responsável e mensurável. É a base normativa do dever de diligência. A Seção 2 impõe obrigações específicas às plataformas que permitem interação entre usuários, prevenindo a circulação de conteúdos ilegais. Expressa a exigência de atuação proativa. A Seção 10 concretiza o dever de diligência ao exigir medidas proporcionais para evitar que usuários encontrem conteúdo ilegal, representando o núcleo do proactive duty.	A Parte 2 define informações sobre a diligência devida dos intermediários e reparação das reclamações. Rule 3: consolida o núcleo do dever de diligência, ao exigir que intermediários cumpram padrões de transparência, informem usuários suas regras de uso e utilizem-se de esforços razoáveis para que estes não publiquem informações de diversos tipos, incluindo: (v) desinformação ou conteúdo incorreto, inverídico ou falso, ou verificada como falsa pelo Governo; (vii) ameaças à integridade da segurança e soberania da Índia ou, de modo geral; (xi) que violem a lei.

Mecanismos de notificação e ação ("notice and action")	Art. 16: cria mecanismos de notificação e ação de possíveis conteúdos ilegais. Segundo o item 3, a notificação ensejará conhecimento efetivo quando um prestador diligente identificar a ilegalidade sem um exame jurídico pormenorizado. Art. 18: amplia o dever de notificação quando houver suspeitas de crime, devendo o prestador de serviços informar a sua suspeita para as autoridades policiais. Art. 20: estabelece sistema interno de gestão de reclamações que possibilite a apresentação de reclamações.	Seção 20: disciplina os mecanismos de notificação e resposta, determinando que usuários possam reportar conteúdos ilegais de forma simples e rápida, e que as plataformas prestem retorno adequado.	Rule 3: sistema de notice and action com prazos estabelecidos: vinte e quatro horas para as queixas serem reconhecidas; quinze dias para solucioná-las. O prazo pode ser reduzido para setenta e duas horas em casos específicos de conteúdos ilícitos. Rule 4: determina que os intermediários devem empregar ferramentas tecnológicas para identificar proativamente conteúdo de estupro, abuso sexual infantil ou idêntico a material previamente removido. Tais medidas precisam ser proporcionais e submetidas a supervisão humana periódica.
Dever de cuidado e responsabilidade compartilhada	Art. 27: exige transparência nos sistemas de recomendação das plataformas, esclarecendo aos usuários os parâmetros utilizados. Art. 34, 1, c + Considerando 82: consagram a ideia de dever de cuidado institucional, impondo às grandes plataformas a obrigação de mitigar riscos aos processos democráticos e à segurança pública. Art. 35: prevê a necessidade de atenuação dos riscos sistêmicos identificados pelas plataformas, com medidas proporcionais, razoáveis e eficazes. Essa é uma previsão que demonstra a operatividade do dever de cuidado. Art. 45: valoriza os códigos de conduta como instrumentos que auxiliam na correta aplicação do regulamento, considerando os desafios de resposta aos diferentes tipos de conteúdos ilegais. Art. 48: prevê protocolos de crise, reforçando o dever de cuidado em situações excepcionais (como eleições).	Seção 9: impõe às plataformas o dever de realizar avaliações de risco, base para o exercício responsável do duty of care. Seção 10: complementa a anterior, detalhando o dever de implementar medidas de mitigação proporcionais. Seção 17: Estabelece deveres de proteger conteúdos de importância democrática. É esclarecida a necessidade de sistemas e processos proporcionais, designados para assegurar a liberdade de expressão de conteúdos democráticos. Esses sistemas e processos devem ser aplicados de maneira semelhante para opiniões políticas diversas. Seção 41: reconhece os códigos de conduta como instrumentos para estabelecer balizas e critérios de aplicação dos deveres de cuidado.	A Rule 4 estabelece obrigações mais rigorosas para os significant social media intermediaries, exigindo a nomeação de três agentes responsáveis pelo cumprimento das normas: - um Chief Compliance Officer, residente na Índia e encarregado de assegurar a conformidade legal, respondendo pessoalmente em caso de descumprimento (Rule 4(1)(a)); - um Nodal Officer, disponível 24 horas por dia para comunicação direta com autoridades públicas (Rule 4(1)(b)); e - um Resident Grievance Officer, responsável pela gestão do sistema interno de reclamações (Rule 4(1)(c)). A Rule 3 ainda estabelece que esse sistema deve reconhecer as queixas em até vinte e quatro horas e solucioná-las em quinze dias, com prazo reduzido para setenta e duas horas em casos específicos de conteúdo ilícito.

Avaliação e mitigação de riscos sistêmicos	Art. 34, 1, c + Considerando 82: definem os riscos sistêmicos relevantes, incluindo "efeitos negativos reais ou previsíveis nos processos democráticos, no discurso cívico e nos processos eleitorais, bem como na segurança pública". Art. 35: impõe a obrigação de avaliar e mitigar esses riscos, com medidas proporcionais e auditáveis. Art. 39: ainda que voltado à transparência publicitária, e não especificamente sobre publicidade eleitoral, contribui para o controle dos riscos informacionais ao exigir clareza sobre conteúdos pagos.	Seção 9: introduz o dever de criação de avaliações de riscos. Seção 10 complementa ao impor medidas de mitigação desses riscos.	A Rule 1 determina que os intermediários devem impedir a disseminação de informações falsas ou enganosas, incluindo aquelas que induzam o destinatário a erro sobre a origem da mensagem ou que sejam patentemente falsas ou não verdadeiras. Essa regra não trata apenas de diligência reativa, mas de gestão e mitigação de riscos estruturais.
Governança e auditorias independentes	Art. 37: realização de auditorias independentes, que também auxiliam na identificação e mitigação dos riscos sistêmicos e na concretização do dever de cuidado das plataformas digitais. Art. 40 – assegura acesso a dados por autoridades e pesquisadores, permitindo controle social e institucional da diligência das plataformas.	Seções 104-105: tratam da possibilidade de a Ofcom determinar auditorias independentes (reports by skilled persons), o que reforça o eixo de governança.	Não há previsão de auditorias independentes periódicas sobre bibliotecas de anúncios ou conformidade eleitoral.

Análise adicional:

Critério	REGULAMENTO (UE) 2024/900 DO PARLAMENTO EUROPEU E DO CONSELHO de 13 de março de 2024 sobre a transparência e o direcionamento da propaganda política
Dever de diligência e atuação proativa	Considerandos 11 e 16: Determinam o dever de diligência para patrocinadores e prestadores de serviços de propaganda política. Considerando 20: plataformas em linha são incentivadas a participar em iniciativas vastas de desmonetização da desinformação, impedindo propaganda política que contenha desinformação. Artigos 11º e 12º: anúncios políticos devem ser declarados dessa forma, sendo exigida a rotulagem e transparência.

Mecanismos de notificação e ação ("notice and action")	Artigo 7º, 3: sempre que o prestador de serviços de publicidade tenha conhecimento sobre a incompletude ou inexatidão da propaganda política, deve contatar o editor. Após, devem pedir que sejam corrigidas, tornando a correção completa e sem demora injustificada. Artigo 7º, 4: Após, devem pedir que sejam corrigidas, tornando a correção completa e sem demora injustificada.
Dever de cuidado e responsabilidade compartilhada	Artigo 12 + Considerando 63: quando são disponibilizados anúncios políticos, essa informação deve ser divulgada de forma transparente ao público. Artigo 12, 2: sempre que houver informação de propaganda política incompleta ou inexata, devem ser completadas ou corrigidas.
Avaliação e mitigação de riscos sistêmicos:	Considerando 46: esclarece que os editores de propaganda política que também sejam VLOPs e VLOSEs segundo o DSA devem identificar, analisar e avaliar os riscos sistêmicos dos serviços de propaganda política, com medidas de atenuação razoáveis, proporcionais e eficazes. Artigo 19, 1, d: como requisito adicional de transparência, exige-se a preparação anual e disponibilização de avaliação anual dos riscos decorrentes das técnicas de direcionamento e distribuição de anúncios e seus impactos para direitos e liberdades fundamentais.
Governança e auditorias independente	Art. 27: estabelece um mecanismo de governança periódica, ao determinar que, a cada dois anos após as eleições para o Parlamento Europeu, a Comissão apresente um relatório público de avaliação e revisão do regulamento. Embora não preveja auditorias independentes, o dispositivo reforça uma lógica de governança regulatória baseada em transparência e accountability, ao impor à Comissão o dever de monitorar e divulgar publicamente os impactos e a eficácia da norma.

Obs.: Em momento posterior, será apresentado o *The Strengthened Code of Practice on Disinformation* (2022) (UE), essencial também para contextualizar o estágio atual da União Europeia no combate à desinformação. O documento reúne uma série de compromissos firmados por plataformas digitais e outros signatários, visando mitigar os impactos das informações falsas no ambiente online. Entre seus principais pontos, destacam-se a desmonetização da desinformação, com mecanismos que restringem a elegibilidade de conteúdos passíveis de monetização; a criação de repositórios e APIs que assegurem transparência sobre anúncios políticos em tempo real períodos eleitorais; e o fortalecimento das ferramentas de verificação e decisão informada pelos usuários diante de conteúdos enganosos.

26.4 *BENCHMARK* INTERNACIONAL (SÍNTESE COMPARATIVA)

União Europeia – DSA

Considerando 2: explicita sobre os requisitos de atuação diligente dos prestadores de serviços intermediários sobre conteúdos ilegais, desinformação e outros riscos sociais.

Considerando 22: para que haja isenção de responsabilidade, o prestador deve atuar com diligência na supressão de conteúdos ilegais, seja por notificação de terceiros ou iniciativa própria.

Considerando 40: menciona que um ambiente em linha seguro e transparente necessita de um conjunto claro, eficaz, previsível e equilibrado de obrigações de devida diligência dos prestadores, assegurando os direitos fundamentais.

- Art. 3, h: definição de "conteúdos ilegais" como informações que não estejam em conformidade com o direito da União Europeia ou de seus Estados-membros.
- Art. 9: decisão de atuação contra conteúdos ilegais quando houver ordem judicial ou administrativa.
- Art. 16: mecanismos de notificação e ação de possíveis conteúdos ilegais. Segundo o item 3, a notificação ensejará conhecimento efetivo quando um prestador diligente identificar a ilegalidade sem um exame jurídico pormenorizado.
- Art. 18: notificação de suspeitas de crime ensejam cuidados ainda maiores, quando o prestador de serviços deve informar a sua suspeita para as autoridades policiais.
- Art. 20: sistema interno de gestão de reclamações que possibilite a apresentação de reclamações.
- Art. 27: transparência nos sistemas de recomendação das plataformas, esclarecendo aos usuários os parâmetros utilizados.
- Art. 34, 1, c + Considerando 82: a terceira categoria de riscos sistêmicos para as VLOPs *(very large online platforms)* e VLOSEs *(very large online search engines)* prevista no DSA são os "efeitos negativos reais ou previsíveis nos processos democráticos, no discurso cívico e nos processos eleitorais, bem como na segurança pública".
- Art. 35: necessidade de atenuação dos riscos sistêmicos identificados pelas plataformas, com medidas proporcionais, razoáveis e eficazes. Essa é uma previsão que demonstra a operatividade do dever de cuidado.
- Art. 37: realização de auditorias independentes, que também auxiliam na identificação e mitigação dos riscos sistêmicos e na concretização do dever de cuidado das plataformas digitais.
- Art. 39: transparência na publicidade. O artigo não trata de maneira específica sobre publicidades eleitorais, mas não se visualiza óbice a essa aplicação.
- Art. 40: possibilidade de acesso a dados para autoridades e pesquisadores habilitados, permitindo maior transparência, monitoramento dos riscos e atuação das plataformas e compreensão mais ampla do cumprimento do dever de cuidado.
- Art. 45: utilidade dos códigos de conduta para a correta aplicação do regulamento, considerando os desafios de resposta aos diferentes tipos de conteúdos ilegais.
- Art. 48: protocolos de crise em casos de riscos para a segurança pública, o que pode ser aplicável em períodos eleitorais.

O DSA também disponibilizou o *DSA Elections Toolkit for Digital Services Coordinators* como um documento base que explora instrumentos, melhores práticas e lições sobre os processos eleitorais.

União Europeia - Regulamento do Parlamento Europeu e do Conselho sobre a Transparência e o Direcionamento da Propaganda Política

Considerandos 11 e 16: dever de diligência para patrocinadores e prestadores de serviços de propaganda política.

Considerando 20: plataformas em linha são incentivadas a participar em iniciativas vastas de desmonetização da desinformação, impedindo propaganda política que contenha desinformação.

- Artigo 7º, 3: sempre que o prestador de serviços de publicidade tenha conhecimento sobre a incompletude ou inexatidão da propaganda política, deve contatar o editor. Após, devem pedir que sejam corrigidas, tornando a correção completa e sem demora injustificada.
- Artigo 7º, 4: Após, devem pedir que sejam corrigidas, tornando a correção completa e sem demora injustificada.
- Artigo 12 + Considerando 63: quando são disponibilizados anúncios políticos, essa informação deve ser divulgada de forma transparente ao público.
- Artigo 12, 2: sempre que houver informação de propaganda política incompleta ou inexata, devem ser completadas ou corrigidas.

União Europeia - Diretrizes da Comissão para atenuação dos riscos sistêmicos para os processos eleitorais

3.2.1 (g): desmonetização dos conteúdos da desinformação pelos fornecedores de VLOPs e VLOSEs, de modo que não haja incentivos financeiros à difusão de desinformação de processos eleitorais.

União Europeia - *The Strengthened Code of Practice on Disinformation 2022*

Compromisso 1: desmonetização da desinformação. Devem ser estipulados mecanismos sobre elegibilidade do conteúdo que deve ser monetizado.

Compromisso 10.1: os signatários se comprometem a criar repositórios de anúncios sobre anúncios políticos em tempo real, principalmente em períodos eleitorais.

Compromisso 11.1: os signatários irão criar APIs e outras interfaces que permitem buscas em tempo real, principalmente em eleições, sobre os anúncios.

Compromisso 12.2: os signatários irão produzir ferramentas e instrumentos para garantir o escrutínio adequado da publicidade política, especialmente durante períodos eleitorais.

Compromisso 22: signatários se comprometem a fornecer aos usuários ferramentas para decisões mais informadas quando houver informações falsas ou enganosas, principalmente em questões relevantes socialmente e de interesse geral.

Compromisso 37.2: signatários concordam em trabalhar com uma força-tarefa específica para avaliar situações de riscos, com resposta rápida em situações como eleições. Haverá coordenação e cooperação durante esses momentos de crise ou eleições.

Compromisso 42: signatários aceitam fornecer, em situações especiais como eleições, informações e dados proporcionais para a Comissão Europeia, incluindo relatórios de monitoramento e do sistema de resposta da força-tarefa.

União Europeia – GDPR

Considerando 56: Se partidos políticos recolherem dados pessoais sobre opinião política dos cidadãos, o tratamento deve ocorrer por motivos de interesse público, estabelecidas garantias adequadas.

- Artigo 9, 2, g: Proibição do tratamento de dados pessoais sobre opiniões políticas, salvo por questões como a necessidade de interesse público.

Reino Unido – *Online Safety Act* (OSA)

A lei, de modo geral, impõe diversos *duties of care* aos provedores digitais (Ohrvik-Stott; Millener, 2019). A ideia foi inicialmente desenvolvida pelos professores Lorna Woods e William Perrin (2019), que sustentam que pessoas e empresas devem ser cuidadosas em suas atividades, já que afetam outras pessoas ou coisas. Se esse cuidado não ocorrer e houver um resultado danoso, haverá consequências legais. Para eles, as redes sociais e aplicativos de mensagem, por exemplo, são espaços públicos, e o que ocorre nesses espaços é resultado de suas decisões corporativas.

- Seção 1: esclarece que há imposição de deveres de transparência e *accountability.*
- Seção 2: considerando as plataformas que permitem a comunicação entre usuários, há deveres relacionados ao conteúdo ilegal.
- Seção 9: dever de criação de avaliações de riscos.
- Seção 10: estabelece o dever dos provedores de estabelecerem medidas proporcionais para evitar que usuários encontrem conteúdos ilegais, mitigando tais riscos.
- Seção 17: Deveres de proteger conteúdos de importância democrática. É esclarecida a necessidade de sistemas e processos proporcionais, designados para assegurar a liberdade de expressão de conteúdos democráticos. Esses sistemas e processos devem ser aplicados de maneira semelhante para opiniões políticas diversas. Além disso, é esclarecido que a ação, nesses casos, significa agir de modo a dar avisos ao usuário, suspendê-lo ou bani-lo do serviço.
- Seção 20: deveres sobre notificação de conteúdos, de modo que o usuário deve conseguir reportar, com facilidade, o conteúdo que considere ilegal, por exemplo.
- Seção 41: utilidade dos códigos de conduta para estabelecer balizas e critérios de aplicação dos deveres de cuidado.
- Parte 10: trata dos casos de comunicações falsas e ameaçadoras. Segundo a seção 179, há crime quando alguém transmite, de modo intencional, informação falsa, com intenção de causar dano. A seção 180 estabelece isenções, a exemplo dos jornalistas.

Índia – *IT Rules 2021*

Parte 2: informações sobre diligência devida dos intermediários e reparação das reclamações.

- Artigo 3: o intermediário, incluindo intermediários de mídia social, devem respeitar os deveres e os requisitos de diligência exigidos. Exemplos: questões de transparência, remoção de conteúdo, informações aos usuários.
- Artigo 3, b: o esforço deve ser para que os usuários não consigam compartilhar conteúdos violadores, de diversos tipos, incluindo (v) desinformação ou conteúdo incorreto, inverídico ou falso, ou verificada como falsa pelo Governo; (vii) ameaças à integridade da segurança e soberania da Índia ou, de modo geral, (xi) que violem a lei.
- Artigo 4: obrigações mais robustas para intermediários considerados significativos, de mídia social e de jogos online.
- Artigo 5: estabelece ainda a necessidade de diligência adicional que deve ser empregada pelo intermediário em casos de conteúdos atuais e notícias.

26.5 INTERPRETAÇÃO DO ART. 9º-D, §§ 1º, 2º E 4º, E ART. 32, PARÁGRAFO ÚNICO (PROPOSTAS)

O conceito de "dever de cuidado" se relaciona com o de "função social" e está presente em algumas normas brasileiras na atualidade. O conceito de "função social" se relaciona com a ideia de que, durante a sua atuação, os entes devem visar o respeito e a promoção de direitos coletivos, e não somente a obtenção de lucros e vantagens internas. Assim, apesar das empresas possuírem como objetivo principal o lucro, o que não se contesta, devem cumprir também função social, incluindo a proteção não somente dos seus *shareholders*, mas dos terceiros interessados, os stakeholders, que incluem os membros da sociedade e das organizações civis. Sua previsão está no artigo 5º, XXIII e no artigo 170 da Constituição Federal de 1988, que, em seu inciso III, prevê que a função social da propriedade é um dos princípios da ordem econômica nacional.

Na questão da desinformação eleitoral, é razoável que a função social seja imposta aos intermediários, que são as plataformas na internet, justamente porque estes são os entes mais bem posicionados na estrutura da internet para endereçar esses problemas, a exemplo da exclusão de conteúdos violadores de direitos das suas plataformas. Assim, a ideia é que a responsabilização das plataformas se baseie no cumprimento do dever de cuidado das empresas de tecnologia, que devem atuar para mitigar riscos, incluindo aqueles relacionados com os potenciais danosos da desinformação.

Em resumo, a ideia central contida nesses princípios é a de que as plataformas digitais que atuam na internet devem pautar suas atividades com responsabilidade e diligência, o que ocorre também no contexto eleitoral. Durante as eleições, os impactos de discursos falsos, mentirosos ou incompletos podem trazer lesões significativas para o processo eleitoral e para a própria democracia, de modo que as empresas devem atuar com maior nível de cuidado ao exibir e promover discursos, concretizando uma função social na sua atuação, a preservação da integridade eleitoral, e não apenas seu objetivo empresarial de obtenção de lucro.

O art. 9º-D, §4º esclarece, de maneira expressa são decorrências diretas da função social e do dever de cuidado dos provedores de aplicação: i) a vedação de comercialização e impulsionamento de conteúdo de conteúdos ilícitos e ii) a sua retirada de circulação caso ocorram. Nesse sentido, os termos de uso devem priorizar a prevenção, evitando ou, ao menos, minimizando que os serviços sejam empregados para o cometimento ou a perpetuação de ilícitos eleitorais.

Nesses casos, para reforçar a necessidade de atuação proativa das plataformas, é esclarecido que não há necessidade de notificação da autoridade judicial. Trata-se de previsão compatível com a decisão recente do Supremo Tribunal Federal sobre a inconstitucionalidade parcial do artigo 19 do Marco Civil da Internet (MCI). Na decisão, o STF mencionou que a exigência de ordem judicial específica já não é suficiente para a proteção dos direitos fundamentais e da democracia. Por isso, os provedores devem atuar imediatamente para retirar conteúdos que configurem crimes graves, bem como para a retirada de crimes em geral, após o recebimento de um pedido de retirada.

O grande propósito do artigo 9º-D e da Resolução n. 23.610 do TSE, de modo geral, é preservar a integridade do processo eleitoral durante as propagandas eleitorais.

No caso da justiça eleitoral, o dever de cuidado e a aplicação da função social se baseiam na compreensão de que devem ser coibidos ilícitos eleitorais e, como consequência, preservada a integridade eleitoral. Um dos meios para cumprir esse fim é preservar a integridade das informações

que circulam durante esses e períodos. Desse modo, devem ser coibidos e minorados os conteúdos, em plataformas digitais, que propaguem conteúdos desinformativos.

No entanto, a Resolução ainda deixa espaços para indeterminações sobre os termos e exigências que são feitas para as plataformas digitais. Por isso mesmo, muitas vezes o TSE atua em conjunto com as próprias plataformas digitais através de acordos, bem como com empresas que atuam realizando a checagem de fatos, nos casos mais complexos.

Passa-se, agora, à interpretação sugerida do Art. 9º-D, §§ 1º, 2º e 4º, e art. 32, parágrafo único:

"Providências imediatas e eficazes":

- Deve haver uma análise da veracidade da informação antes da comercialização, evitando que ela ocorra. Quando o conteúdo ilícito já estiver na plataforma, deve haver uma atuação posterior, após a detecção da própria plataforma ou o recebimento de notificação. Nesses casos, quando identificado conteúdo violador, ele deve ser indisponibilizado. Exige-se assim uma ação prévia das plataformas, no sentido de não permitir tais anúncios e uma ação posterior, de atuação caso esse conteúdo violador esteja disponível.

Prazos que sejam considerados razoáveis: artigo 38, §4º da Resolução determina que o prazo razoável não será inferior a 24 horas[7] para a remoção.

- O artigo 9º-F, §3º[8], define que o prazo de remoção poderá ser inferior a 24 horas, a depender da gravidade da veiculação e das peculiaridades do processo eleitoral. No entanto, não há maiores esclarecimentos sobre quais requisitos são exigidos para esse prazo menor.

Cumprimento da função social e do dever de cuidado

Complexidade da definição. Deve incluir deveres como:

- Cooperação com usuários, Estado e outros entes, como agências de checagem de conteúdo;
- Atuação com diligência na identificação e mitigação dos riscos eleitorais;
- Mecanismos de notificação e ação rápidos e eficazes;
- Desmonetização da desinformação;
- Anúncios ou informações eleitorais ou políticas dever ser completadas ou corrigidas quando houver erro ou incompletude;
- Transparência nos anúncios político-eleitorais (quem fez, valores e informação de que é anúncio);
- Força-tarefa para períodos eleitorais, com atuação mais ampla e rápida.

7 Artigo 38, § 4º A ordem judicial que determinar a remoção de conteúdo divulgado na internet fixará prazo razoável para o cumprimento, não inferior a 24 (vinte e quatro) horas, e deverá conter, sob pena de nulidade, a URL e, caso inexistente esta, a URI ou a URN do conteúdo específico, observados, nos termos do art. 19 da Lei n.º 12.965/2014 , o âmbito e os limites técnicos de cada provedor de aplicação de internet.

8 Art. 9º-F, § 3º A ordem de remoção de conteúdo expedida nos termos deste artigo poderá estabelecer prazo inferior a 24 (vinte e quatro) horas para cumprimento da decisão, considerando a gravidade da veiculação e as peculiaridades do processo eleitoral e da eleição em curso ou a se realizar, e observará os demais requisitos constantes do § 4º do art. 38 desta Resolução. (Incluído pela Resolução n.º 23.732/2024).

Conhecimento prévio do provedor

Esclarece a Resolução que os provedores "não dependem de notificação da autoridade judicial". Assim, compreende-se que devem atuar antes, vedando comercialização e impulsionamento de conteúdos ilícitos e vedados pela lei eleitoral.

Posteriormente, deve ser retirada a circulação indevida, caso ocorra, em caso de:

- Notificação pelos usuários;
- Ordem judicial específica ou
- Não cumprimento dos deveres de diligência (que poderiam ser previstos nos próprios termos de uso, como transparência eleitoral mais ampla e criação de repositório de anúncios, por exemplo).

26.6 EVIDÊNCIAS E ESTUDOS DE CASO

Pesquisa de jurisprudência feita no site do TSE:[9]

Termo de busca: "dever de cuidado":

AgR-AREspEl n.º 060010471. Acórdão CACHOEIRO DE ITAPEMIRIM – ES. Relator(a): Min. André Ramos Tavares. Julgamento: 20/03/2025 Publicação: 01/04/2025. Decisão menciona sobre o "dever geral de cuidado" atinente ao jornalismo, que deve respeitá-lo ou poderá configurar-se como extrapolação no exercício regular do direito de informar, caracterizando abuso.

AgR-REspEl n.º 060010440. Acórdão SÃO CAETANO DO SUL – SP. Relator(a): Min. Floriano De Azevedo Marques. Julgamento: 29/11/2024 Publicação: 28/11/2024 e AgR-REspEl n.º 060003678. Acórdão SANTOS – SP. Relator(a): Min. Floriano De Azevedo Marques. Julgamento: 22/10/2024. Publicação: 22/10/2024. Mencionado sobre a Súmula 30 do TSE, demonstrando que, caso não haja inobservância do dever de cuidado na apuração dos fatos, a Justiça Eleitoral não deve atuar no debate público concedendo direito de resposta, que é excepcional.

RO-El n.º 060429864. Acórdão CURITIBA – PR. Relator(a): Min. Floriano De Azevedo Marques. Julgamento: 21/05/2024 Publicação: 29/08/2025 e RO-El n.º 060417651. Acórdão CURITIBA – PR. Relator(a): Min. Floriano De Azevedo Marques Julgamento: 21/05/2024 Publicação: 29/08/2025. Diferenciação entre uso indevido e irregular dos meios de comunicação (emprego deles de forma distorcida ou apta a fraudar o livre conhecimento do eleitor), o qual não se configura como um dever de cuidado ao postulante.

Termo de busca: "função social"

Utilizando aspas, para busca exata do termo, não foram encontradas decisões significativas. A única encontrada (REspe n.º 060004105 Acórdão JUAZEIRO DO PIAUÍ – PI. Relator(a): Min. Mauro

9 Realizada em: https://jurisprudencia.tse.jus.br/#/jurisprudencia/pesquisa.

Campbell Marques. Julgamento: 15/12/2020 Publicação: 15/12/2020) menciona sobre a função social da propriedade nas atividades de telecomunicações.

Jurisprudência do Tribunal Europeu de Direitos Humanos:

Bradshaw and Others v. The United Kingdom (n.º 15653/22),[10] do Tribunal Europeu dos Direitos Humanos (ECHR), julgada em 22 de julho de 2025. Considerou-se que é dever do Estado proteger os cidadãos da desinformação no contexto eleitoral. Ainda que não de forma expressa, é reconhecido um dever de diligência e cuidado estatal quando há ameaças aos processos eleitorais, de modo que devem investigar alegações possíveis. O Estado argumentou dizendo que já possui legislações e regulações para lidar com essa questão. Na decisão, é mencionado que a democracia constitui um elemento fundamental da "ordem pública europeia" e que pressupõe pluralismo. Assim, os Estados-Membros têm a obrigação de adotar medidas positivas para organizar eleições que assegurem a liberdade de voto do povo. Principalmente em contexto no qual a disseminação da desinformação é capaz de representar uma ameaça significativa para a democracia. Os Estados devem, assim, tomar medidas para defender os valores democráticos, não são obrigados a esperar, antes de intervir, até que uma ameaça à democracia seja suficientemente estabelecida e iminente. Essa atuação deve sempre ser equilibrado com o direito à liberdade de expressão.

26.7 RECOMENDAÇÕES (NORMATIVAS E OPERACIONAIS)

- Criação de força-tarefa das plataformas nos períodos eleitorais, com parcerias com TSE e agências de checagem de fatos, possibilitando respostas de notificação e ação mais rápidas durante esses períodos.
- Termos de uso das plataformas com direcionamento específico para anúncios político-eleitorais e regras de impulsionamento e monetização em períodos eleitorais.
- Proibição ou maior controle de regras da monetização de anúncios eleitorais, com mecanismos de transparência assegurados para pesquisas sobre o assunto por parte dos usuários.
- Relatório de transparência posterior à realização de cada eleição, para avaliação pública e possibilidade de sugestões de melhoria por parte de terceiros interessados.

26.8 RISCOS, SALVAGUARDAS E DIREITOS

Riscos para liberdade de expressão: manifestações devem ocorrer respeitando a proporcionalidade. É possível que a plataforma tenha um rol de ações diversas, a depender do nível de risco e da manifestação. Por exemplo:

- remover impulsionamento ou diminuir o alcance da postagem em alguns casos complexos;

10 Disponível em: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-244218%22]}.

- manter conteúdo com rótulo de “anúncio político”, quando adequado, com informações sobre patrocinadores;
- inserir informações externas para o próprio site do TSE ou outros checadores de conteúdo confiáveis.

Devido processo: deve haver notificações aos usuários quando houver remoção de conteúdo e ser assegurada a possibilidade de defesa aos usuários.

Privacidade/LGPD: minimização de coleta de dados políticos e personalização/microdirecionamento de conteúdo político.

REFERÊNCIAS

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei nº 9.504, de 30 de setembro de 1997. Dispõe sobre normas para as eleições. Brasília, DF: Presidência da República, 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 11 dez. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 out. 2025.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 2019. Dispõe sobre propaganda eleitoral. Brasília, DF, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 10 dez. 2025

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 2024. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Brasília, DF, 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 10 dez. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. Portaria nº351, de 12 de abril de 2023. Dispõe sobre medidas administrativas a serem adotadas no âmbito do Ministério da Justiça e Segurança Pública, para fins de prevenção à disseminação de conteúdos flagrantemente ilícitos, prejudiciais ou danosos por plataformas de redes sociais, e dá outras providências. Brasília, DF: Ministério da Justiça e Segurança Pública, 2023. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/mjsp-edita-portaria-com-novas-diretrizes-para-redes-sociais-apos-ataques-nas-escolas/portaria-do-ministro_plataformas.pdf. Acesso em: 11 dez. 2025.

COMISSÃO EUROPEIA. The strengthened code of practice on disinformation 2022. [S. l.]: Comissão Europeia, 2022. Disponível em: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened--code-practice-disinformation. Acesso em: 10 dez. 2025.

COMISSÃO EUROPEIA. Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065. Official Journal of the European Union, [S. l.], 2024. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403014. Acesso em: 10 dez. 2025.

ÍNDIA. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Índia: Ministry of Electronics and Information Technology, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Acesso em: 10 dez. 2025.

OHRVIK-STOTT, Jacob; MILLENER, Catherine. A digital duty of care. Reino Unido: Doteveryone, 2019. Disponível em: https://doteveryone.org.uk/wp-content/uploads/2019/02/Doteveryone-briefing-a-digital-duty-of-care.pdf. Acesso em: 11 dez. 2025.

REINO UNIDO. Online Safety Act (OSA). Londres, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2026 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). União Europeia, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679. Acesso em: 11 dez. 2025.

UNIÃO EUROPEIA. Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Bruxelas, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2024/900 do Parlamento Europeu e do Conselho de 13 de março de 2024 sobre a transparência e o direcionamento da propaganda política. União Europeia, 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202400900. Acesso em: 11 dez.. 2025.

WOODS, Lorna; PERRIN, William. Online harm reduction: a statutory duty of care and regulator. Carnegie UK Trust, Reino Unido, abr. 2019. Disponível em: https://carnegieuk.org/publication/online-harm-reduction-a-statutory-duty-of-care-and-regulator/. Acesso em: 10 dez. 2025.

2.7 IA E TRANSPARÊNCIA NA PROPAGANDA ELEITORAL (ART. 9º-B, *CAPUT*)

Elaine Gomes dos Santos

Art. 9º-B. A utilização na propaganda eleitoral, em qualquer modalidade, de conteúdo sintético multimídia gerado por meio de inteligência artificial para criar, substituir, omitir, mesclar ou alterar a velocidade ou sobrepor imagens ou sons impõe ao responsável pela propaganda o dever de informar, de modo explícito, destacado e acessível que o conteúdo foi fabricado ou manipulado e a tecnologia utilizada.

27.1 VISÃO GERAL E OBJETIVOS

Objetivo: interpretar o alcance e os deveres decorrentes do art. 9º-B, *caput,* que trata da obrigação de informar a utilização de conteúdo sintético multimídia gerado por Inteligência Artificial (IA) em propagandas eleitorais, assim como comparar com boas práticas internacionais em transparência. Portanto, a análise deve identificar os requisitos mínimos de transparência eleitoral, a fim de coibir a desinformação e manter a higidez do sistema eleitoral.

Guia de Perguntas:

- O que caracteriza "conteúdo sintético multimídia"?
- O que significa "modo explícito, destacado e acessível"?
- Que tipo de manipulação exige aviso obrigatório?
- Como deve ser exibido o aviso (visual, textual, sonoro)?
- Quem possui o dever de informar sobre a utilização de conteúdo sintético - o candidato, a coligação, o provedor ou o criador do material?
- Quais padrões mínimos de transparência exigidos?

27.2 BASE NORMATIVA (BRASIL)

Art. 9º-B, *caput,* Res. TSE 23.610/2019 (incluído pela Res. 23.732/2024): visa garantir transparência e prevenir desinformação eleitoral, impondo obrigação de rotulagem clara de conteúdos artificiais usados em campanhas e propagandas políticas. Saliente-se que §§ 1º, 2º e 3º detalham a vedação à manipulação dos fatos, bem como a obrigação de identificação visual e sonora do aviso (Brasil, 2024).

Contexto regulatório adjacente: O art. 57-B da Lei 9.504/1997 reforça a responsabilidade direta de quem veicula o conteúdo ilegal, bem como aponta a responsabilidade das plataformas na veiculação do conteúdo desinformativo, impondo o dever de cuidado e resposta a notificações extrajudiciais em certos casos (Brasill, 1997).

STF – Repercussão Geral (Temas 987 e 533). Art. 19 do Marco Civil da Internet e dever de cuidado das plataformas: A recente orientação do Supremo Tribunal Federal, ao modular os efeitos do art. 19 do Marco Civil da Internet, reforça o dever de atuação diligente e proativa das plataformas digitais. O Tribunal firmou entendimento de que, em situações envolvendo conteúdo

manifestamente ilícito ou que atente contra bens jurídicos fundamentais - como crimes contra mulheres e crianças, a integridade das instituições democráticas ou a vedação ao discurso de ódio –, as plataformas devem remover ou tornar indisponível o conteúdo mesmo sem ordem judicial, sob pena de responsabilidade civil. Essa interpretação amplia o papel das plataformas, tornando-as agentes responsáveis pela integridade do ambiente informacional e impondo-lhes deveres positivos de monitoramento e resposta.

Nesse contexto, este entendimento se adequa ao art. 9º-B, caput, da Resolução TSE n.º 23.610/2019, no sentido de que este dispositivo cria um dever de transparência ativa quanto à utilização de tecnologias de IA em conteúdos eleitorais. Tanto o referido dispositivo da presente resolução, quanto o entendimento do STF apontam para a superação da ideia de neutralidade das plataformas e constrói um sistema de atribuição de deveres positivos de cuidado, prevenção e transparência.

No caso do STF (Temas 987 e 533), o dever é de agir proativamente diante de conteúdos ilícitos ou que atinjam bens jurídicos fundamentais. No art. 9º-B da Resolução do TSE, o dever é de informar claramente quando há manipulação tecnológica, protegendo o eleitor contra desinformação ou deepfakes, por meio de rotulagem e sinalização explícita de conteúdos gerados por IA. Nesses dois regimes, a transparência é o eixo comum que viabiliza a responsabilização contra ilegalidades, criando um padrão de governança informacional (Brasil, 2025).

27.3 METODOLOGIA DE *BENCHMARKING*

Seleção de jurisdições: UE (DSA), Reino Unido (*Online Safety Act*, 2023 + *Ofcom Codes*), Índia (*IT Rules*).

Unidades de comparação (possíveis critérios):

- Identificação e Rotulagem (aviso padrão unificado, exibição simultânea, fonte legível e em idioma local, acessibilidade para pessoas com deficiência);
- Transparência (relatórios, repositório);
- Responsabilização (responsável direto e indireto).

Critério	União Europeia - *Digital Service Act* (DSA)	Reino Unido - *Online Safety Act* (OSA)	Índia – *IT Rules*
Identificação e Rotulagem	Art. 26, DSA. determina que os anúncios devem ser clareamento identificados, bem como exige a divulgação da identidade do anunciante. Art. 27, DSA. Transparência dos sistemas de recomendação. Obriga plataformas a divulgarem (em seus termos e condições) os principais parâmetros dos algoritmos de recomendação, inclusive para anúncios, e possibilitar que os usuários possam ajustar ou entender tais parâmetros. Esse dispositivo dialoga com a exigência da rotulagem de conteúdos sintéticos ou manipulados em propaganda eleitoral seja realizada de forma explícita e destacada, ou seja, que se informe que conteúdo foi fabricado e qual tecnologia foi usada.	OSA + relatório Ofcom: Rótulos de IA: exigência de inclusão de ícones visíveis e informações (metadados) relacionados ao conteúdo para indicar se foi produzido artificialmente e/ou editado por IA.	*IT Rules* + avisos emitidos pelo MeitY (Ministry of Electronics and IT): recomendações oficiais com a determinação de que as plataformas identifiquem e rotulem conteúdos artificialmente gerados e/ou alterados com ferramentas de IA generativa.

Transparência	Art. 15, DSA. Obrigações de transparência de moderação de conteúdo. exigência de apresentação de relatórios públicos de transparência dos prestadores de serviços intermediários. Embora não se refira especificamente a propaganda eleitoral ou conteúdo sintético, esse mecanismo de accountability e divulgação pública de decisões de moderação converge com o regime de transparência requerido no contexto eleitoral. Art. 39, DSA. Transparência adicional de publicidade. Determina a criação de um repositório público de anúncios, onde serão disponibilizadas informações sobre os anúncios veiculados, o que inclui dados de financiamento, público-alvo etc. Essa exigência se assemelha ao dever das plataformas de agirem proativamente - saber o que está sendo anunciado, quem anuncia, como segmenta - e criar parâmetros de responsabilização.	OSA (9, 65 e 67): dever legal de transparência e segurança digital para plataformas que hospedam ou distribuem conteúdo on-line.	*IT Rules* (Rule 4(d)): obrigação de relatórios mensais/periódicos.
Controle e Responsabilização	Art. 16, DSA: esse artigo prevê que plataformas on-line devem manter mecanismos de "notice & action" eficazes e acessíveis, permitindo a denúncia de conteúdos ilícitos e exigindo transparência sobre sistemas automatizados de moderação e recomendação. Art. 24, DSA: esse dispositivo exige a divulgação de dados relativos a disputas extrajudiciais, cancelamentos por uso indevido, suspensão de contas etc. Esses dispositivos estabelecem a prestação de contas e visibilidade externa de como plataformas operam suas políticas de moderação e relacionamento com usuários, construindo um regime de controle e responsabilização.	OSA (9, 65 e 67): responsabilização decorre do dever legal de transparência e segurança digital.	*IT Rules* 2021, atualizado em 2023 (Rule 3(1)(b)): trata dos deveres dos intermediários digitais acerca proibições de conteúdo ilícito, difamatório ou prejudicial.

Critério	**Regulamento (UE) 2024/900 - sobre a transparência e o direcionamento da propaganda política ("Regulamento de Propaganda Política da UE")**
Identificação e Rotulagem	Art. 11. Rotulagem/Aviso de transparência. Determina que cada anúncio deve acompanhar um aviso de transparência claro, destacando que se trata de um anúncio político e contendo informações como identidade do patrocinador, campanha, se foi sujeito a técnicas de direcionamento e distribuição etc. Esse mecanismo de rotulagem se assemelha com o art. 9º-B da Resolução do TSE quando determina que conteúdos sintéticos em propaganda eleitoral "deverão informar, de modo explícito, destacado e acessível, que o conteúdo foi fabricado e a tecnologia utilizada". O regulamento europeu enfatiza que os usuários saibam que o anúncio é político e quais são os elementos de transparência que o acompanham.

Transparência	Art. 12. Alcance e Transparência. Impõe que os avisos de transparência incluam também informações sobre a identidade do patrocinador, alcance do anúncio, número de visualizações, interações, assim como dados sobre como o anúncio foi distribuído e quantas pessoas o visualizaram. Esse dispositivo se adequa a uma interpretação mais ampla da exigência de transparência do art. 9º-B, pois visa permitir que o eleitor não somente seja informado da manipulação, mas também como ela atua (alcance, nível de manipulação etc.).
Responsabilização	Art. 19. Obrigação de diligência pelos editores de propaganda política. Impõe responsabilidade aos editores para avaliar e mitigar riscos associados aos anúncios políticos que veiculam, inclusive no uso de técnicas de direcionamento e distribuição. Esse dispositivo estabelece o compromisso ativo para evitar manipulações e desinformação. Art. 13. Repositório europeu de anúncios de caráter político. Prevê a criação de um repositório público de anúncios políticos, onde devem ser armazenadas e tornadas públicas as informações exigidas nos avisos de transparência. Esse repositório aponta que a transparência deve implicar no rastreamento público e auditável dos anúncios políticos - quem os financiou, quem os exibiu, público alvo, etc.

Critério	**Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial)**
Identificação e Rotulagem	Art. 50 (4 e 7): inclusão de rótulo acessível indicando que o conteúdo é sintético. O presente artigo reforça o dever de rotulagem e transparência informativa presente no art. 9º-B da Resolução do TSE, que impõe que a propaganda eleitoral com conteúdo sintético ou manipulado contenha indicação explícita de tal manipulação e da tecnologia utilizada.
Transparência	Art. 50 (2): estabelecimento de regras específicas de transparência para sistemas de IA generativa e conteúdos sintéticos. Art. 22. Obrigações de Governança. Determina que os operadores de sistemas de IA de risco elevado estabeleçam um sistema de gestão de risco, identificando, monitorando e mitigando os riscos relacionados à utilização desses sistemas. No âmbito eleitoral, essa obrigação reforça que quem desenvolve ou utiliza IA deve antecipar e informar os riscos de manipulação, desinformação ou dano ao debate democrático - o tipo de intervenção que o Art. 9º-B visa prevenir (quando exige rotulagem clara para evitar desinformação ao eleitor).
Responsabilização	Art. 29 a 39. Relatórios e documentação, auditoria. Imposição do dever de manter documentação técnica, registros de uso, e possibilitar acesso à documentação ou ao código-fonte para autoridades ou auditorias quando necessário. Esses dispositivos se relacionam com o art. 9º-B no sentido de que a exigência eleitoral de transparência não pode ser interpretada de forma restrita (rotulagem ao usuário), mas que o dispositivo prever a criação de mecanismos internos robustos para auditoria, verificação e responsabilização.

2.7.4 *BENCHMARK* INTERNACIONAL (SÍNTESE COMPARATIVA)

União Europeia – DSA

- Art. 15, DSA: exigência de apresentação de relatórios públicos de transparência dos prestadores de serviços intermediários. Embora não se refira especificamente a propaganda eleitoral ou conteúdo sintético, esse mecanismo de *accountability* e divulgação pública de decisões de moderação converge com o regime de transparência requerido no contexto eleitoral.
- Art. 16: mecanismos de notice & action eficazes e acessíveis, permitindo a denúncia de conteúdos ilícitos e exigindo transparência sobre sistemas automatizados de moderação e recomendação.
- Art. 24, DSA: esse dispositivo complementa o art. 15, pois exige a divulgação de dados relativos a disputas extrajudiciais, cancelamentos por uso indevido, suspensão de contas etc. Esses dispositivos estabelecem a prestação de contas e visibilidade externa de como plataformas operam suas políticas de moderação e relacionamento com usuários, construindo um regime de controle e responsabilização.
- Art. 26, DSA: determina que os anúncios devem ser identificados, bem como exige a divulgação da identidade do anunciante.
- Art. 27, DSA: Obriga plataformas a divulgarem (em seus termos e condições) os principais parâmetros dos algoritmos de recomendação, inclusive para anúncios, e possibilitar que os usuários possam ajustar ou entender tais parâmetros. Isso se conecta com a exigência da rotulagem de conteúdos sintéticos em propaganda eleitoral seja realizada de forma explícita e destacada, ou seja, que se informe que conteúdo foi fabricado e qual tecnologia foi usada.
- Art. 39, DSA: Impõe a criação de um repositório público de anúncios, onde serão disponibilizadas informações sobre os anúncios veiculados — o que inclui dados de segmentação, financiamento, público-alvo etc. Essa exigência espelha o dever das plataformas de agirem proativamente - saber o que está sendo anunciado, quem anuncia, como segmenta - e criar parâmetros de responsabilização.

Os dispositivos do DSA estabelecem obrigações similares de rotulagem, descrição da origem e transparência. Ou seja, o modelo europeu oferece uma "inspiração normativa" similar ao que o TSE exige: os anúncios devem conter informações/dados visíveis, identificáveis, explicáveis e auditáveis. Além disso, os mecanismos de relatórios públicos e acesso a dados criam instrumentos institucionais de controle e responsabilização.

Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024

- Art. 22: determina que os operadores de sistemas de IA de risco elevado estabeleçam um sistema de gestão de risco, identificando, monitorando e mitigando os riscos relacionados à utilização desses sistemas. No âmbito eleitoral, essa obrigação reforça que quem desenvolve ou utiliza IA deve antecipar e informar os riscos de manipulação, desinformação ou dano ao debate democrático - o tipo de intervenção que o Art. 9º-B visa prevenir (quando exige rotulagem clara para evitar desinformação ao eleitor).
- Art. 29 a 39: dever de manter documentação técnica, registros de uso, e possibilitar

acesso à documentação ou ao código-fonte para autoridades ou auditorias quando necessário. Isso se relaciona ao Art. 9º-B no sentido de que a exigência eleitoral de transparência não pode ser interpretada de forma restrita (rotulagem ao usuário), mas que o dispositivo prever a criação de mecanismos internos robustos para auditoria, verificação e responsabilização.

- Art. 50: estabelecimento de obrigações, como: incluir rótulo visível, persistente e acessível indicando que o conteúdo é sintético, a fim de coibir manipulação eleitoral e desinformação. Conjugando este artigo com o art. 9º-B da Resolução do TSE, compreende-se que o DSA cria o parâmetro europeu de responsabilidade e rastreabilidade, exigindo que qualquer conteúdo manipulado por IA tenha identificação explícita e canal de contestação.

O Art. 9º-B, *caput*, ao exigir indicação expressa de que o conteúdo é fabricado por IA (e qual tecnologia foi utilizada), encontra fundamento no art. 50 do Regulamento 2024/1689, que impõe transparência informativa para conteúdo gerado por IA. O art. 9º-B da Resolução do TSE tem como princípios estruturantes a transparência e o combate à desinformação, ou seja, a manipulação por IA deve ser revelada ao eleitor.

Formação de arcabouço técnico que sustenta essa transparência efetiva e cria um regime de controle, verificação e responsabilização.

Regulamento (UE) 2024/900 do Parlamento Europeu e do Conselho de 13 de março de 2024

- Art. 11: Determina que cada anúncio deve acompanhar um aviso de transparência claro, destacando que se trata de um anúncio político e contendo informações como identidade do patrocinador, campanha, se foi sujeito a técnicas de direcionamento e distribuição etc. Esse mecanismo de rotulagem dialoga com o art. 9º-B quando determina que conteúdos sintéticos ou manipulados em propaganda eleitoral "deverão informar, de modo explícito, destacado e acessível, que o conteúdo foi fabricado ou manipulado e a tecnologia utilizada". O regulamento europeu enfatiza que os usuários saibam que o anúncio é político e quais são os elementos de transparência que o acompanham.
- Art. 12: impõe que os avisos de transparência incluam também informações sobre alcance do anúncio, número de visualizações, cliques, interações, assim como dados sobre como o anúncio foi distribuído e quantas pessoas o visualizaram.
- Art. 13: prevê a criação de um repositório público de anúncios políticos, onde devem ser armazenadas e tornadas públicas as informações exigidas nos avisos de transparência. Esse repositório sustenta a lógica do Art. 9º-B no sentido de que a transparência deve implicar no rastreamento público e auditável dos anúncios políticos — quem os financiou, quem os exibiu, segmentos de audiência, etc.
- Art. 19: Impõe responsabilidade aos editores para avaliar e mitigar riscos associados aos anúncios políticos que veiculam, inclusive no uso de técnicas de direcionamento e distribuição. Esse dispositivo estabelece o compromisso ativo para evitar manipulações e desinformação.

Reino Unido – *Online Safety Act* (OSA)

O OSA cria o dever legal de transparência e segurança digital para plataformas que hospedam ou distribuem conteúdo on-line.

Embora não mencione diretamente conteúdos produzidos por modelos de IA generativa, as seções 9, 65 e 67, combinadas com os Ofcom Codes of Practice, determinam que as empresas rotulem conteúdos significativamente alterados ou sintéticos, especialmente quando houver potencial de desinformação.

Os relatórios e códigos de conduta da Ofcom tentam preservar a rastreabilidade, garantir que os usuários saibam quando interagem com material sintético e evitar disseminação de desinformação.

Índia – *IT Rules* 2021 + Avisos do Meity

Embora o Rule 3(1)(b) não mencione expressamente inteligência artificial, o seu alcance foi ampliado pelas Diretrizes MeitY de 2024, que introduzem a exigência de rotular ou indicar sempre que um conteúdo tiver sido artificialmente alterado por IA.

Essa diretriz interpreta e complementa o Rule 3(1)(b), impondo que plataformas devem exibir aviso visível sempre que um conteúdo for manipulado digitalmente por IA.

2.7.5 INTERPRETAÇÃO DO ART. 9º-D, II (PROPOSTAS)

"Conteúdo sintético multimídia": abrange qualquer áudio, imagem, vídeo ou combinação alterada por modelos de IA generativa (*deepfake, voice clone, image morphing,* etc.) para criar, substituir, omitir ou sobrepor elementos audiovisuais.

"Dever de informar": dever de transparência ativa, cujo descumprimento configura ilegalidade na propaganda, passível de sanções, como retirada imediata do conteúdo ilegal e penalidades administrativas.

"Modo explícito, destacado e acessível" implica:

- visibilidade mínima (contraste alto, leitura em ≤ 2 s, letras ≥ 5% da altura da tela).
- duração suficiente para leitura integral (≥ 5 s em vídeo ou até o fim, se texto fixo).
- linguagem clara e acessível.
- legenda sonora ou textual em todos os canais (inclusive rádio, podcast, stories).
- recursos de acessibilidade para pessoas com deficiência.

Responsável: é quem veicula ou financia a propaganda - candidato, partido, coligação ou prestador contratado -, independentemente do autor técnico da manipulação.

2.7.6 EVIDÊNCIAS E ESTUDOS DE CASO

Suspensão por falta de aviso de IA (Teresina–PI): decisão que suspendeu o programa eleitoral porque a peça não informava que a música havia sido produzida por IA, como determina a resolução do TSE (DataPrivacy BR Research, 2024).

Publicação de *deepfake* sem rotulagem (São Paulo–SP): no início da campanha, Pablo Marçal publicou um *deepfake* no "X" sem indicar o uso de IA (DataPrivacy BR Research, 2024).

Rotulagem inconsistente entre plataformas (Salvador-BA): o prefeito Bruno Reis postou dois vídeos gerados com IA. Em ambos, o político aparecia com seu rosto sobreposto ao corpo de um homem dançando ao som de seu *jingle* de campanha; no Instagram havia o rótulo "*made with AI*", mas no TikTok não – exemplo clássico de descumprimento prático da regra de rotulagem (DataPrivacy BR Research, 2024).

Ataques com "*deepnudes*" a candidatas (SP, RJ e outras cidades): casos de imagens/vídeos sexuais sintéticos contra mulheres (como, Tabata Amaral) levaram a medidas judiciais e policiais (DataPrivacy BR Research, 2024).

Desinformação e Manipulação com IA: Produção de vídeo com IA que mostrava um suposto abraço entre Tabata Amaral e Pablo Marçal durante um debate televisivo, afirmando falsamente que o coach havia se desculpado por insultos feitos à candidata (DataPrivacy BR Research, 2024).

Desinformação por IA: Circulação de vídeos e áudios manipulados do apresentador William Bonner com elogios e declaração de apoio a candidatos a vereador em diversas cidades (DataPrivacy BR Research, 2024).

27.7 RECOMENDAÇÕES (NORMATIVAS E OPERACIONAIS)

Padrões mínimos sugeridos:

- Aviso padrão unificado: "Conteúdo produzido/manipulado por inteligência artificial";
- Exibição simultânea a todo o conteúdo (ou início e fim de vídeos);
- Fonte legível, de alto contraste e tradução em LIBRAS quando houver vídeo, bem como outros instrumentos de acessibilidade;
- Registro em metadados e protocolo de publicação (para auditoria).
- Boas práticas internacionais adaptáveis:
- Aplicar diretrizes UE sobre rótulo persistente; os anúncios devem ser visíveis, identificáveis, explicáveis e auditáveis;
- Exigir relatórios públicos de peças que usaram IA (semelhante ao transparency dashboard DSA Art. 15);
- Implementação de sistemas de listas verificadas de propagandas com IA.

27.8 RISCOS, SALVAGUARDAS E DIREITOS

Liberdade de expressão e proporcionalidade: distinguir manipulação artística/satírica de distorção factual.

Privacidade/LGPD: evitar exposição indevida de dados biométricos nos exemplos de manipulação, bem como retenções e logs proporcionais.

Prova e rastreabilidade: exigência de armazenamento do arquivo original e logs de geração.

REFERÊNCIAS

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei nº 9.504, de 30 de setembro de 1997. Dispõe sobre normas para as eleições. Brasília, DF: Presidência da República, 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 11 dez. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 out. 2025.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 2019. Dispõe sobre propaganda eleitoral. Brasília, DF, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 10 dez. 2025

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 2024. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Brasília, DF, 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 10 dez. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. Portaria nº351, de 12 de abril de 2023. Dispõe sobre medidas administrativas a serem adotadas no âmbito do Ministério da Justiça e Segurança Pública, para fins de prevenção à disseminação de conteúdos flagrantemente ilícitos, prejudiciais ou danosos por plataformas de redes sociais, e dá outras providências. Brasília, DF: Ministério da Justiça e Segurança Pública, 2023. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/mjsp-edita-portaria-com-novas-diretrizes-para-redes-sociais-apos-ataques-nas-escolas/portaria-do-ministro_plataformas.pdf. Acesso em: 11 dez. 2025.

BRASIL. Supremo Tribunal Federal. Informação à sociedade: RE 1.037.396 (Tema 987) e 1.057.258 (Tema 533) responsabilidade de plataformas digitais por conteúdo de terceiros. Brasília: STF, 2025. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/Informac807a771oa768SociedadeArt19MCI_vRev.pdf. Acesso em: 10 dez. 2025.

COMISSÃO EUROPEIA. The strengthened code of practice on disinformation 2022. [S. l.]: Comissão

Europeia, 2022. Disponível em: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened--code-practice-disinformation. Acesso em: 10 dez. 2025.

COMISSÃO EUROPEIA. Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065. Official Journal of the European Union, [S. l.], 2024. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403014. Acesso em: 10 dez. 2025.

DATAPRIVACY BR RESEARCH. AI in the 2024 Brazilian elections. 2024. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2024/11/AI-in-the-2024-brazilian-elections.pdf. Acesso em: 11 dez. 2025.

ÍNDIA. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Índia: Ministry of Electronics and Information Technology, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Acesso em: 10 dez. 2025.

OFCOM. Protecting people from illegal harms online: statement & codes. Londres: Ofcom, 2024. Disponível em: https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/statement-protecting-people-from-illegal-harms-online. Acesso em: 10 dez. 2025.

OFCOM. Transparency reporting: consultation (2024-2025) e Final Transparency Guidance (21 jul. 2025). Londres: Ofcom, 2025. Disponível em: https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/transparency-reporting. Acesso em: 10 dez. 2025.

REINO UNIDO. Online Safety Act (OSA). Londres, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2026 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). União Europeia, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679. Acesso em: 11 dez. 2025.

UNIÃO EUROPEIA. Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Bruxelas, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2024/900 do Parlamento Europeu e do Conselho de 13 de março de 2024 sobre a transparência e o direcionamento da propaganda política. União Europeia, 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202400900. Acesso em: 11 dez.. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial e altera diversos atos legislativos (Artificial Intelligence Act). Official Journal of the European Union, [S. l.], L 277, 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32024R1689. Acesso em: 11 dez. 2025.

2.8 IMPULSIONAMENTO DIGITAL DE PROPAGANDA ELEITORAL (ART. 28, § 7°-A; ART. 29, § 11)

Bruna Ammon e Tayná Frota

Art. 28. A propaganda eleitoral na internet poderá ser realizada nas seguintes formas (Lei n.º 9.504/1997, art. 57-B, I a IV):
§ 7º-A. O impulsionamento de conteúdo em provedor de aplicação de internet somente poderá ser utilizado para promover ou beneficiar candidatura, partido político ou federação que o contrate, sendo vedado o uso do impulsionamento para propaganda negativa.
Art. 29. É vedada a veiculação de qualquer tipo de propaganda eleitoral paga na internet, excetuado o impulsionamento de conteúdos, desde que identificado de forma inequívoca como tal e contratado exclusivamente por partidos políticos, federações, coligações, candidatas, candidatos e representantes (Lei n.º 9.504/1997, art. 57-C, caput). (Redação dada pela Resolução n.º 23.671/2021)
§ 11. É vedada, desde 48 (quarenta e oito) horas antes até 24 (vinte e quatro) horas depois da eleição, a circulação paga ou impulsionada de propaganda eleitoral na internet, mesmo se a contratação tiver sido realizada antes desse prazo, cabendo ao provedor de aplicação, que comercializa o impulsionamento, realizar o desligamento da veiculação de propaganda eleitoral.

2.8.1 VISÃO GERAL E OBJETIVOS

Objetivo: interpretar o alcance dos Arts. 28 e 29 quanto à propaganda eleitoral na internet, com ênfase: (i) nas permissões e limites do impulsionamento de conteúdo; (ii) na vedação de propaganda paga por atores não autorizados; (iii) na proibição temporal de veiculação paga às vésperas da votação; (iv) e na comparação com boas práticas internacionais de transparência, publicidade política e janelas de blackout eleitoral.

Guia de Perguntas:

- O que caracteriza o impulsionamento eleitoral permitido e o proibido?
- Como a vedação de propaganda negativa impulsionada se articula com a liberdade de expressão?
- Que responsabilidades recaem sobre o provedor quanto à identificação, desligamento e rastreabilidade da publicidade?
- Como o blackout eleitoral brasileiro dialoga com experiências estrangeiras?
- Que métricas, transparência e mecanismos de governança se esperam das plataformas?

2.8.2 BASE NORMATIVA (BRASIL)

O Art. 28 da Res. 23.610/2019 delimita as modalidades possíveis de propaganda eleitoral na internet, conforme o art. 57-B da Lei 9.504/1997. A inclusão do § 7º-A pela Res. 23.732/2024 estabelece uma regra central: o impulsionamento somente pode ser contratado para promover ou beneficiar a própria candidatura/partido/federação, sendo vedado o seu uso para propaganda negativa. Isso cria uma distinção jurídica entre:

- crítica política orgânica (expressão protegida); e
- publicidade negativa paga (vedada como desproporção na disputa eleitoral).

O Art. 29 consolida a cláusula geral de proibição: toda propaganda eleitoral paga na internet é proibida, exceto o impulsionamento regularmente contratado e identificado de forma inequívoca. A regra visa impedir financiamento oculto, propaganda paralela e interferência econômica assimétrica. O novo § 11 (Res. 23.732/2024) cria o blackout de impulsionamento: entre 48h antes e 24h após a votação, é proibida qualquer circulação paga, mesmo que contratada anteriormente, impondo ao provedor o dever de desligamento automático.

Contexto regulatório adjacente: Decisões recentes do STF sobre o art. 19 do Marco Civil da Internet reforçam que provedores podem ser responsabilizados quando deixam de agir diante de notificações idôneas sobre conteúdos manifestamente ilícitos. No contexto da propaganda eleitoral, isso amplia o dever de diligência das plataformas na identificação e suspensão de impulsionamentos irregulares, sobretudo durante o período vedado.

2.8.3 METODOLOGIA DE *BENCHMARKING*

A metodologia de comparação internacional utilizada neste estudo parte de três eixos regulatórios consolidados - União Europeia (DSA e Regulamento 2024/900), Reino Unido (*Online Safety Act*) e Índia (*IT Rules* 2021 + *Election Commission*) - que representam modelos distintos de governança da publicidade política digital.

O objetivo é identificar padrões normativos convergentes e divergentes em relação ao regime brasileiro dos arts. 28 e 29 da Resolução TSE n.º 23.610/2019 (com alterações da Res. 23.732/2024), especialmente no tocante ao impulsionamento, transparência, proibições e deveres de plataformas. Para isso, adota-se um recorte analítico ampliado, composto pelos seguintes eixos de comparação:

- Transparência e rotulagem de anúncios;
- Repositórios públicos e relatórios de transparência;
- Limites de segmentação e microtargeting político;
- Janelas de blackout ou restrições temporais;
- Deveres de rastreabilidade, documentação e auditoria;
- Responsabilidade do provedor na interrupção de veiculações ilegais;
- Governança interna e *accountability*;
- Pré-aprovação e certificação de anúncios políticos;
- Regulação específica de lives e conteúdo audiovisual político;
- Regime de rotulagem reforçada (digital imprint);
- Due diligence eleitoral e avaliação de risco sistêmico;
- Transparência financeira e identificação do responsável econômico;
- Critérios de entrega e explicação algorítmica;
- Distinção (ou não) entre conteúdo orgânico e impulsionado.

Eixo analítico	União Europeia (DSA + Regulamento 2024/900)	Reino Unido (OSA + Electoral Commission)	Índia (*IT Rules* 2021 + ECI)
A) Transparência e rotulagem	Rotulagem obrigatória; indicação de patrocinador, valor, período e segmentação (Arts. 26, 39).	Rotulagem obrigatória; digital imprint (nome, endereço, responsável financeiro).	Identificação obrigatória do partido/candidato; pré-aprovação pela ECI.
B) Repositórios públicos / relatórios	Relatórios semestrais (Arts. 15 e 42); repositório de anúncios políticos.	Transparency reports (Sec. 64-66).	Relatórios mensais de conformidade (Rule 4(1)(d)).
C) Limites de segmentação	Restrição a dados sensíveis; limites ao microtargeting; obrigação de explicar targeting.	Sem proibição ampla, mas regulado por riscos eleitorais.	Segmentação controlada; exigências ligadas ao registro prévio e autorização.
D) Blackout	Não há blackout unificado na UE; alguns países têm.	Silence day (dia da eleição) restringe anúncios pagos.	Blackout de 48h antes da votação (Model Code + *IT Rules*).
E) Rastreabilidade e auditoria	Auditorias obrigatórias para VLOPs; logs e documentação; acesso de pesquisadores.	Registros obrigatórios de moderação; exigências de record keeping.	Logs obrigatórios; documentação de decisões; pré-aprovação gera trilhas verificáveis.
F) Interrupção de veiculações ilegais	Notificação e ação (Arts. 16 e 17); mitigação de riscos sistêmicos.	Mecanismos de denúncia (Sec. 69) e mitigação de harmful misinformation.	Remoção obrigatória mediante ordem; prazos rígidos (36h/15 dias).
G) Governança interna e accountability	Avaliação de risco (Arts. 34-37); medidas proporcionais.	Interferência eleitoral como priority harm; safety by design.	Intermediários significativos devem manter compliance contínuo.
H) Pré-aprovação	Não há pré-aprovação; há conformidade prévia.	Não há pré-aprovação institucional.	Pré-aprovação obrigatória pela ECI.
I) Lives / audiovisuais	Seguem as mesmas regras dos anúncios políticos.	Lives promovidas são campanha eleitoral.	Lives tratadas como campanha digital e exigem pré-aprovação.
J) Digital imprint	Conteúdo deve revelar patrocinador e critérios de segmentação.	Obrigatória (PPERA 143A).	Identificação obrigatória de partido/candidato.
K) Due diligence eleitoral	Forte: avaliações de risco e auditorias.	Forte: priority harm + mitigação obrigatória.	Moderada: foco em aprovação e remoção.
L) Transparência financeira	Indicação de valor pago no anúncio.	Registro de gastos e responsável financeiro.	Autorização formal e identificação do financiador.
M) Explicação algorítmica	Art. 26(2): usuário deve saber por que recebeu o anúncio.	Não há equivalente direto.	Não há equivalente direto.
N) Conteúdo orgânico vs. pago	Não há distinção normativa rígida.	Distinção clara: conteúdo pago é regulado; orgânico, não.	Campanha digital (incluindo orgânicos relevantes) pode exigir pré-aprovação.

2.8.4 *BENCHMARK* INTERNACIONAL (SÍNTESE COMPARATIVA)

União Europeia - DSA (*Digital Services Act*) + Regulamento (UE) 2024/900 sobre publicidade política

O DSA não regula eleições de forma direta, mas estabelece padrões essenciais que impactam a publicidade política; o Regulamento 2024/900 complementa com regras específicas para publicidade política.

Transparência de anúncios (Art. 26 do DSA):

- anúncios devem ser claramente identificados;
- deve constar o contratante/patrocinador, parâmetros de segmentação e período de veiculação;
- obrigação de repositório público de anúncios políticos;
- explicação algorítmica: o usuário deve poder saber por que recebeu aquele anúncio (Art. 26(2)).

Segmentação e impulsionamento (DSA + Reg. 2024/900):

- restrições ao uso de dados sensíveis para segmentação;
- limites ao *microtargeting* político e obrigação de explicitar a base de segmentação;
- modelo fortemente voltado a transparência técnica da entrega (além da mera identificação).
- Interrupção de veiculações ilegais (Arts. 16-17 DSA):
- provedores devem agir prontamente diante de notificações idôneas (*notice & action*), inclusive em contexto eleitoral - paralelo funcional com o desligamento brasileiro no período de blackout.

Avaliação de risco e auditorias (Arts. 34–37 DSA):

- VLOPs (plataformas de muito grande porte) devem avaliar riscos sistêmicos (incluindo desinformação e impacto eleitoral) e adotar medidas de mitigação proporcionais;
- sujeição a auditorias independentes periódicas;
- acesso de pesquisadores (Art. 40) para escrutínio acadêmico dos riscos eleitorais.

Regras específicas do Regulamento 2024/900:

- definição ampla de “publicidade política”;
- identificação granular: patrocinador, valor, período e base de segmentação;
- não há proibição expressa a “anúncios negativos”, mas há deveres indiretos que coíbem práticas abusivas;
- lives são tratadas pelas mesmas regras de transparência aplicáveis à publicidade política;
- não há blackout uniforme no nível da UE (alguns Estados-Membros adotam vedações próprias).

Reino Unido - *Online Safety Act* (OSA) + *Electoral Commission*

Embora não trate de impulsionamento eleitoral de forma específica, o OSA estabelece um guarda-chuva regulatório de segurança por design e de mitigação de danos que se projeta sobre a publicidade política; a Electoral Commission e a legislação eleitoral complementam com regras próprias.

Transparência e rotulagem de conteúdos patrocinados:

- obrigações de rotulagem clara;
- mecanismos de denúncia "*easy to access and easy to use*" (Sec. 69 OSA) para reportar publicidade irregular;
- relatórios de transparência e códigos de prática supervisionados pela Ofcom (Secs. 64-66).

Dever de minimizar exposição a conteúdos ilegais (ss. 9, 16, 67 OSA):

- resposta célere e proporcional;
- interferência eleitoral tratada como *priority harm*, exigindo *logs* e mitigação reforçada.

Complementos eleitorais (Electoral Commission):

- registro de gastos com anúncios políticos e disclaimers padronizados;
- *digital imprint* obrigatório (PPERA 2000, Sec. 143A): identificação do promotor, responsável financeiro e contato;
- *lives* com promoção eleitoral são campanha e seguem as mesmas exigências de gasto e *imprint.*

Blackout/silence day:

- vedação de anúncios pagos no dia da eleição (*silence day*), aplicável também a posts patrocinados e *lives* impulsionadas.

Supervisão e *enforcement:*

- a Ofcom pode exigir auditorias, *record keeping* ampliado e editar códigos vinculantes;
- diretrizes recentes preveem rotulagem e moderação reforçada de *deepfakes* políticos.

Índia - *IT Rules 2021* + *Election Commission of India* (ECI)

O modelo indiano é o mais rígido em termos operacionais e de controle prévio.

Identificação e pré-aprovação (Rule 4(8) + ECI):

- pré-aprovação obrigatória de publicidade política pela ECI;
- identificação clara do anunciante e da natureza paga do conteúdo;
- lives tratadas como digital campaigning e sujeitas à pré-aprovação.

Remoção e prazos (governança responsiva):

- 36 horas para cumprir ordens de remoção governamentais/judiciais;
- relatórios mensais de conformidade por intermediários significativos (Rule 4(1)(d));
- rastreabilidade de denúncias e *ticketing*;
- canal de queixas com prazo de 15 dias para resposta (Rule 3(2)(a)).

Blackout eleitoral:

- proibição de campanhas digitais nas 48h que antecedem o pleito (*Model Code of Conduct + IT Rules*), convergente com o § 11 do art. 29 brasileiros.

Conteúdos enganosos:

- Rule 3(1)(b)(v) veda conteúdo que engane ou desinforme o público e autoriza a autoridade competente a ordenar remoção.

Transparência e cadeia financeira:

- exigência de identificação do partido/candidato responsável e autorização prévia (ECI), o que cria trilha verificável da cadeia de financiamento/contratação.

2.8.5 INTERPRETAÇÃO DOS ARTS. 28 E 29 À LUZ DA LEGISLAÇÃO COMPARADA

A análise comparativa permite interpretar os arts. 28 e 29 da Resolução TSE n.º 23.610/2019 (com alterações da Res. 23.732/2024) em um contexto global de regulação da publicidade política digital. Ao confrontar o modelo brasileiro com o da União Europeia (DSA e Regulamento 2024/900), do Reino Unido (*OSA e Electoral Commission*) e da Índia (*IT Rules* 2021), observa-se que o Brasil adota um modelo híbrido, combinando clareza procedimental e restrição temporal com menor densidade em transparência algorítmica e governança de risco. A seguir, apresentam-se as respostas aos eixos interpretativos centrais, isto é, as perguntas delimitadoras apresentadas no tópico I da presente pesquisa.

2.8.5.1 O que caracteriza o impulsionamento eleitoral permitido e o proibido

O impulsionamento eleitoral permitido é aquele contratado exclusivamente por partidos políticos, federações, coligações, candidatos ou seus representantes (§ 1º do art. 29), identificado de forma inequívoca, e destinado à promoção positiva de candidaturas, programas ou ideias políticas. Impulsionamento proibido, por sua vez, decorre de duas hipóteses: (i) quando não há identificação clara do contratante, violando o dever de transparência; (ii) quando o conteúdo tem natureza negativa, isto é, destinado a prejudicar adversários políticos (§ 7º-A do art. 28).

Comparativamente:

Na União Europeia, o DSA não distingue entre “anúncios positivos” e “negativos”, mas exige transparência total e rastreabilidade do conteúdo político, o que, na prática, inibe campanhas negativas ocultas.

No Reino Unido, anúncios negativos são admitidos, porém sujeitos à mitigação de *misinformation* e à identificação do patrocinador.

Na Índia, não há vedação de conteúdo negativo em si, mas todo material político deve ser pré-aprovado pela *Election Commission*, o que funciona como filtro prévio.

Assim, o modelo brasileiro é único ao proibir expressamente o impulsionamento negativo, traduzindo uma opção normativa de proteção da integridade do debate eleitoral, ainda que à custa de uma limitação mais ampla ao conteúdo político pago.

2.8.5.2 A articulação entre a vedação de propaganda negativa e a liberdade de expressão

A proibição de propaganda negativa impulsionada não elimina a liberdade de expressão política individual, mas regula a utilização de meios pagos que distorcem a paridade de armas informacional. A comparação internacional revela que:

- a UE evita restringir conteúdo político, optando por responsabilizar plataformas por falta de transparência e risco sistêmico;
- o Reino Unido protege a liberdade de expressão, mas impõe obrigações de moderação quando há dano político mensurável (*harmful misinformation*);
- a Índia exerce controle administrativo prévio, subordinando a expressão política à autorização eleitoral.

Nesse espectro, o Brasil se aproxima do modelo europeu quanto à liberdade substantiva, mas adota limitação formal quanto ao uso do impulsionamento pago para fins negativos.

A proibição não censura o conteúdo em si - apenas impede o financiamento direcionado de campanhas de ataque. Trata-se, portanto, de restrição de meio, não de ideia, compatível com o princípio da liberdade de expressão responsável.

2.8.5.3 Responsabilidades do provedor: identificação, desligamento e rastreabilidade

Os arts. 28 e 29 impõem ao provedor três deveres centrais:

- Identificação - assegurar que o impulsionamento seja inequivocamente identificado como propaganda eleitoral, com indicação do contratante e do beneficiário;
- Desligamento - interromper automaticamente a veiculação de anúncios no período de blackout (48h antes até 24h após o pleito);
- Rastreabilidade - manter registros que permitam a verificação de autenticidade, origem e tempo de exibição do anúncio.

No plano internacional:

- o DSA e o Regulamento 2024/900 exigem repositórios públicos, identificação de patrocinador e valor, e sistemas de notificação e ação;
- o OSA britânico impõe mecanismos internos de denúncia, *record keeping* e auditorias da Ofcom;
- o modelo indiano obriga resposta em até 36 horas e relatórios mensais de conformidade.

Assim, o dever brasileiro de desligamento automático corresponde a um modelo proativo de diligência temporal, mais rígido do que o europeu ou o britânico, que dependem de denúncia ou

notificação. A rastreabilidade, contudo, é menos desenvolvida, já que o TSE não exige logs públicos ou relatórios periódicos das plataformas.

2.8.5.4 O blackout eleitoral e as experiências estrangeiras

O blackout brasileiro é de 48 horas antes até 24 horas após o pleito (§ 11 do art. 29). Trata-se de janela de silêncio digital, com efeito automático e objetivo, cuja execução cabe ao provedor de aplicação que comercializa o impulsionamento. Esse modelo encontra paralelos com:

- o silence day do Reino Unido, que proíbe anúncios pagos no dia da eleição;
- o blackout indiano, que proíbe toda campanha digital nas 48 horas anteriores;
- e difere da UE, onde não há regra uniforme, mas Estados-Membros podem adotar períodos nacionais de restrição.

Diferentemente do padrão europeu - voltado à governança e mitigação de risco - o Brasil e a Índia optam por bloqueios automáticos, buscando previsibilidade e equidade informacional. A eficácia brasileira depende, contudo, de cooperação técnica entre Justiça Eleitoral e plataformas, à semelhança dos *compliance channels* previstos no DSA.

2.8.5.5 Métricas, transparência e mecanismos de governança esperados das plataformas

A legislação comparada mostra que a integridade eleitoral digital depende de transparência contínua e governança de risco. O Brasil ainda não exige relatórios periódicos, mas os padrões internacionais apontam expectativas claras:

Aspecto	Referência comparada	Tendência esperada no Brasil
Repositórios de anúncios	UE - DSA (Art. 39)	Criação de banco público de impulsionamentos eleitorais.
Relatórios de moderação e transparência	UE (Arts. 15 e 42), UK (Secs. 64-66)	Publicação de relatórios agregados pós-eleição.
Avaliação de risco e auditorias	UE (Arts. 34-37), UK (Ofcom)	Cooperação com TSE para auditorias técnicas.
Governança e safety by design	UE e UK	Protocolos preventivos de integridade eleitoral.
Rotulagem e digital imprint	UK (PPERA 143A), UE (Art. 26)	Inclusão de parâmetros de rastreabilidade visíveis.
Acesso de pesquisadores	UE (Art. 40 DSA)	Mecanismos de compartilhamento de dados agregados com o TSE e academia.

Portanto, espera-se que as plataformas adotem métricas de transparência compatíveis com padrões internacionais, com registros verificáveis de anúncios, relatórios de conformidade, sistemas internos de denúncia e avaliações de risco eleitoral.

Esses elementos são indispensáveis para consolidar a responsabilidade digital compartilhada entre plataformas e Justiça Eleitoral.

2.8.6 RISCOS, SALVAGUARDAS E DIREITOS

A regulação do impulsionamento eleitoral digital apresenta riscos inerentes de desequilíbrio informacional, restrição indevida da liberdade de expressão e insuficiência de governança tecnológica. O primeiro risco é o da assimetria de poder comunicacional, que decorre da capacidade financeira e técnica de atores políticos ampliarem artificialmente o alcance de mensagens, o que justifica a limitação do impulsionamento a candidatos e partidos oficialmente registrados. O segundo risco é o da instrumentalização da vedação de propaganda negativa como mecanismo de censura indireta, sobretudo quando a distinção entre crítica política legítima e ataque pessoal é tênue. Por isso, a aplicação dos arts. 28 e 29 deve respeitar o núcleo essencial da liberdade de expressão e o debate público robusto, restringindo apenas o uso de recursos pagos com finalidade de desinformação ou difamação.

Outro risco decorre da falta de transparência algorítmica e da opacidade na segmentação das mensagens. Sem mecanismos de auditoria e rastreabilidade, torna-se difícil verificar se o impulsionamento está sendo utilizado dentro dos limites legais. Nesse ponto, o modelo brasileiro carece das salvaguardas institucionais presentes no DSA e na regulação britânica, como relatórios periódicos de moderação, acesso de pesquisadores e sistemas de due diligence eleitoral. A ausência desses instrumentos limita a capacidade de fiscalização e reduz a confiança pública na integridade informacional.

As salvaguardas normativas brasileiras concentram-se em três dimensões: (i) o controle temporal rigoroso (blackout de 48h antes e 24h depois), que impede manipulações de última hora; (ii) a identificação inequívoca do impulsionamento e do contratante, que reforça a *accountability* eleitoral; e (iii) a responsabilização direta das plataformas, obrigadas a desligar anúncios ilegais ou fora do período permitido. Ainda assim, a ausência de um regime de transparência ativa - com publicação de relatórios e dados agregados - fragiliza o exercício de direitos de controle social e de acesso à informação.

Do ponto de vista dos direitos fundamentais, a regulação brasileira deve equilibrar três valores: liberdade de expressão política, integridade eleitoral e transparência digital. A compatibilização desses princípios exige interpretação sistemática que preserve a livre manifestação do pensamento e o pluralismo político, mas impeça a interferência indevida de práticas econômicas e tecnológicas sobre o processo democrático. O impulsionamento deve permanecer como instrumento legítimo de visibilidade, mas sujeito a limites claros de autenticidade, proporcionalidade e rastreabilidade.

2.8.7 RECOMENDAÇÕES (NORMATIVAS E OPERACIONAIS)

À luz da comparação internacional e dos riscos identificados, podem ser propostas recomendações voltadas ao aperfeiçoamento normativo e à melhoria operacional da governança digital eleitoral.

Do ponto de vista normativo, recomenda-se que o TSE avance na transparência estrutural do impulsionamento, criando um repositório público de anúncios eleitorais, à semelhança do previsto

no DSA e nas normas da Ofcom. Esse repositório permitiria acesso a dados agregados sobre valores pagos, público-alvo, duração e contratantes, fortalecendo a confiança pública. Outra medida normativa seria incluir a obrigação de relatórios de conformidade por parte das plataformas, contendo dados sobre desligamentos, denúncias, decisões de moderação e volume de impulsionamentos. Também seria pertinente prever a explicação algorítmica mínima, permitindo que o usuário saiba por que recebeu determinado anúncio político. Tais aprimoramentos aproximariam o modelo brasileiro das boas práticas internacionais sem comprometer a segurança jurídica já consolidada.

No campo operacional, recomenda-se o fortalecimento de canais técnicos entre o TSE e provedores de aplicação, por meio de fluxos automatizados de verificação e desligamento de anúncios em período de blackout, e a criação de protocolos de auditoria cooperativa, permitindo que o tribunal e as plataformas avaliem conjuntamente riscos de desinformação e manipulação algorítmica. É desejável ainda fomentar programas de integridade eleitoral digital, que envolvam universidades, entidades civis e pesquisadores independentes, para produzir dados públicos sobre impulsionamento e seus efeitos sociais.

Finalmente, recomenda-se a atualização contínua das resoluções eleitorais para incluir novos fenômenos (como *deepfakes, microtargeting* e campanhas automatizadas), consolidando um sistema que preserve a liberdade de expressão, mas imponha transparência e responsabilidade técnica aos intermediários digitais. Assim, o Brasil poderá evoluir de um modelo predominantemente restritivo para um regime de governança democrática da publicidade política, alinhado às tendências regulatórias globais e aos princípios constitucionais da informação e da cidadania.

2.8.8 RISCOS, SALVAGUARDAS E DIREITOS

A comparação internacional evidencia que o modelo brasileiro de impulsionamento eleitoral ocupa uma posição intermediária entre o rigor preventivo da Índia, a governança de risco da União Europeia e a transparência procedimental do Reino Unido. Os arts. 28 e 29 da Resolução TSE n.º 23.610/2019 revelam uma arquitetura normativa voltada à proteção da integridade eleitoral, mediante o controle do impulsionamento pago e a proibição da propaganda negativa, equilibrando liberdade de expressão e equidade informacional. O Brasil se destaca pela clareza temporal do blackout e pela responsabilização direta dos provedores, mas ainda carece de mecanismos robustos de transparência, auditoria e rastreabilidade algorítmica.

A evolução do regime jurídico da propaganda eleitoral digital exige, portanto, a incorporação de práticas de governança comparadas, capazes de aliar transparência ativa, cooperação institucional e responsabilidade tecnológica. O futuro da regulação eleitoral brasileira passa por consolidar um modelo de *accountability digital*, em que plataformas, candidatos e Justiça Eleitoral compartilhem deveres de prevenção, documentação e mitigação de riscos informacionais. Assim, o país poderá preservar o pluralismo político e a autenticidade do processo eleitoral sem comprometer o núcleo essencial da liberdade de expressão.

REFERÊNCIAS

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei nº 9.504, de 30 de setembro de 1997. Dispõe sobre normas para as eleições. Brasília, DF: Presidência da República, 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 11 dez. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 dez. 2025.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 2019. Dispõe sobre propaganda eleitoral. Brasília, DF, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 10 dez. 2025

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 2024. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Brasília, DF, 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 10 dez. 2025.

BRASIL. Supremo Tribunal Federal. Informação à sociedade: RE 1.037.396 (Tema 987) e 1.057.258 (Tema 533) responsabilidade de plataformas digitais por conteúdo de terceiros. Brasília: STF, 2025. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/Informac807a771oa768SociedadeArt19MCI_vRev.pdf. Acesso em: 10 dez. 2025.

DATAPRIVACY BR RESEARCH. AI in the 2024 Brazilian elections. 2024. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2024/11/AI-in-the-2024-brazilian-elections.pdf. Acesso em: 11 dez. 2025.

ÍNDIA. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Índia: Ministry of Electronics and Information Technology, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Acesso em: 10 dez. 2025.

OFCOM. Protecting people from illegal harms online: statement & codes. Londres: Ofcom, 2024. Disponível em: https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/statement-protecting-people-from-illegal-harms-online. Acesso em: 10 dez. 2025.

OFCOM. Transparency reporting: consultation (2024-2025) e Final Transparency Guidance (21 jul. 2025). Londres: Ofcom, 2025. Disponível em: https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/transparency-reporting. Acesso em: 10 dez. 2025.

REINO UNIDO. Online Safety Act (OSA). Londres, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Bruxelas, 2022. Dispo-

nível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2024/900 do Parlamento Europeu e do Conselho de 13 de março de 2024 sobre a transparência e o direcionamento da propaganda política. União Europeia, 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202400900. Acesso em: 11 dez.. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial e altera diversos atos legislativos (Artificial Intelligence Act). Official Journal of the European Union, [S. l.], L 277, 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32024R1689. Acesso em: 11 dez. 2025.

2.9 PRESTAÇÃO DE CONTAS, RELATÓRIOS DE IMPACTO E ADEQUAÇÃO DE TECNOLOGIA (ART. 9º-D, *CAPUT*; ART. 9º-G, § 2º; ART. 36, § 2º)

Lucia Maria Teixeira Ferreira

Art. 9º-D. É dever do provedor de aplicação de internet, que permita a veiculação de conteúdo político-eleitoral, a adoção e a publicização de medidas para impedir ou diminuir a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam atingir a integridade do processo eleitoral, incluindo:

I - a elaboração e a aplicação de termos de uso e de políticas de conteúdo compatíveis com esse objetivo;

II - a implementação de instrumentos eficazes de notificação e de canais de denúncia, acessíveis às pessoas usuárias e a instituições e entidades públicas e privadas;

III – o planejamento e a execução de ações corretivas e preventivas, incluindo o aprimoramento de seus sistemas de recomendação de conteúdo;

IV - a transparência dos resultados alcançados pelas ações mencionadas no inciso III do caput deste artigo;

V – a elaboração, em ano eleitoral, de avaliação de impacto de seus serviços sobre a integridade do processo eleitoral, a fim de implementar medidas eficazes e proporcionais para mitigar os riscos identificados, incluindo quanto à violência política de gênero, e a implementação das medidas previstas neste artigo.

VI – o aprimoramento de suas capacidades tecnológicas e operacionais, com priorização de ferramentas e funcionalidades que contribuam para o alcance do objetivo previsto no caput deste artigo.

Art. 9º-G. As decisões do Tribunal Superior Eleitoral que determinem a remoção de conteúdos que veiculem fatos notoriamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral serão incluídas em repositório disponibilizado para consulta pública.

[...]

§ 2º As ordens de remoção de que trata este artigo serão dirigidas aos provedores de aplicação, que, no prazo designado para cumprimento, deverão, por meio de acesso identificado no sistema, informar o cumprimento da ordem e, desde que determinado, alimentar o repositório com:

I - o arquivo de texto, imagem, áudio ou vídeo objeto da ordem de remoção;

II – capturas de tela contendo todos os comentários disponíveis no local de hospedagem do conteúdo, se existentes;

III – os metadados relativos ao acesso, como IP, porta, data e horário da publicação;

IV – os metadados relativos ao engajamento da publicação no momento de sua remoção.

Art. 36, § 2º No período de suspensão a que se refere este artigo, a empresa informará a todas as usuárias e todos os usuários que tentarem acessar o conteúdo que ele está temporariamente indisponível por desobediência à legislação eleitoral, nos termos do art. 57-I, § 2º, da Lei n.º 9.504/1997, no âmbito e nos limites técnicos de cada provedor de aplicação de internet.

29.1 VISÃO GERAL E OBJETIVOS

Objetivo: interpretar os limites e possiblidades dos deveres de prestação de contas dos provedores de aplicação de internet, de modo a assegurar que essas obrigações não se reduzam a uma exposição meramente descritiva, mas impliquem a demonstração substantiva de que os mecanismos adotados são efetivos, proporcionais e compatíveis com a proteção da integridade do debate público no ambiente político-eleitoral. A análise deve identificar requisitos mínimos de cumprimento, comparar com boas práticas internacionais do *benchmarking* selecionado e avaliar os impactos para fiscalização eleitoral, liberdade de expressão e *accountability* das plataformas.

Guia de perguntas:

- Quem são os destinatários do dever de prestação de contas?
- Sobre qual dimensão da atuação das plataformas digitais incide o dever de prestação de contas, e quais aspectos materiais e procedimentais devem ser objeto dessa obrigação?
- Quem são os titulares ou entes legitimados a receber as informações decorrentes do dever de prestação de contas, considerando as esferas institucional e social de *accountability?*
- Em que momento se concretiza o dever de prestação de contas por parte do provedor de aplicação de internet, e qual deve ser a periodicidade ou continuidade dessa obrigação para garantir transparência e controle efetivo?
- Quais parâmetros mínimos devem orientar a elaboração de uma avaliação de impacto sobre a integridade informacional no contexto eleitoral, e em que momento do ano eleitoral essa avaliação deve ser produzida para assegurar a efetividade preventiva das medidas adotadas?
- É possível identificar diferentes graus de exigência no cumprimento do dever de prestação de contas, a depender da natureza e da dimensão dos provedores - especialmente no caso das plataformas e mecanismos de busca de grande dimensão ?
- Quais parâmetros mínimos devem orientar o conteúdo e o formato das informações apresentadas no cumprimento do dever de prestação de contas, de modo a assegurar sua utilidade, verificabilidade e compreensão pública?
- Quais métricas e indicadores de desempenho podem ser requeridos para aferir a efetividade substantiva das medidas de governança, transparência e mitigação de riscos informacionais adotadas pelas plataformas digitais?
- No contexto da corregulação, há espaço para a adoção de medidas complementares de governança e transparência por parte dos provedores de aplicação, destinadas a reforçar a efetividade material dos deveres de prestação de contas e de mitigação de riscos informacionais?

29.2 BASE NORMATIVA (BRASIL)

Res. TSE 23.610/2019, Art. 9º-D: O dever de transparência e prestação de contas, previsto no art. 9º-D, *caput*, da Resolução TSE n.º 23.610/2019, exige que provedores de aplicação de internet que veiculem conteúdo político-eleitoral demonstrem a adoção de medidas para impedir ou

mitigar a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados, preservando a integridade do processo eleitoral. O dispositivo não se limita à formalidade das medidas, mas exige eficácia concreta, de modo que a obrigação se traduza em resultados efetivos na contenção de conteúdos ilícitos e desinformativos. Em outras palavras, não basta apenas declarar conformidade; é necessário que as medidas adotadas sejam comprovadamente eficazes. Essa interpretação deve orientar a leitura do art. 9º-D e de todos os deveres previstos na Resolução TSE n.º 23.610/2019.

Res. TSE 23.610/2019, Art. 9º-G, § 2º: O dispositivo institui obrigações procedimentais aos provedores de aplicação de internet diante de ordens judiciais de remoção de conteúdo, visando assegurar que a retirada de material ilícito ou desinformativo seja realizada de forma transparente, auditável e tecnicamente documentada. Busca-se, assim, preservar evidências relevantes para eventual revisão judicial, responsabilização ou avaliação de impacto informacional. O conjunto dessas obrigações evidencia que a norma não se restringe ao cumprimento material da ordem, mas estrutura um verdadeiro mecanismo de prestação de contas.

Res. TSE 23.610/2019, Art. 36, § 2º: "O art. 36, §2º, da Res. TSE n.º 23.610/2019 impõe aos provedores o dever de informar claramente o motivo da indisponibilidade sempre que um conteúdo for temporariamente suspenso por violação à legislação eleitoral. A medida reforça a transparência, previne bloqueios opacos e legitima a atuação estatal e das plataformas na regulação eleitoral digital. Durante a suspensão, deve ser exibida mensagem indicando a violação ao art. 57-I, §2º, da Lei n.º 9.504/1997, assegurando o direito à informação e prevenindo alegações de censura. O dispositivo ainda admite variação na forma de exibição - tela de alerta, sobreposição ou banner - desde que visível, compreensível e tecnicamente adequada ao provedor.

Contexto regulatório adjacente: Tese do Supremo Tribunal Federal - na ocasião do julgamento dos Temas 987 (RE n.º 1.037.396/SP) e 533 (RE n.º 1.057.258/MG), ambos submetidos ao regime da Repercussão Geral - que, apesar da ressalva expressa de não se aplicar diretamente ao contexto eleitoral (n. 1), reconheceu a existência do dever de cuidado das plataformas digitais em situações de circulação massiva de conteúdos ilícitos graves, incluindo a prática de atos antidemocráticos, atos de terrorismo e incitação à discriminação (n. 5).

29.3 METODOLOGIA DO *BENCHMARKING*

Seleção de jurisdições: UE (DSA), Reino Unido (OSA), Índia (*IT Rules*).

Unidades de comparação:

Plataformas Sujeitas e Obrigações Agravadas: Identificar plataformas cujo alcance ou impacto sistêmico justifique a imposição de deveres de prestação de contas mais rigorosos e complementares em relação a provedores de menor porte.

Medidas e Relatórios de Transparência: Determinar a frequência e o conteúdo mínimo das informações que as plataformas digitais devem publicizar acerca de suas de moderação e mitigação de risco.

Avalições e Relatórios de Impacto: Garantir que as plataformas analisem os efeitos ne-

gativos de seu serviço em áreas críticas, como direitos fundamentais, discurso cívico e processos eleitorais.

Verificação Externa (Auditoria e Controle Regulatório): Garantir a veracidade e o cumprimento efetivo das obrigações da plataforma por meio de fiscalização independente.

Governança Interna (Função de Compliance): Institucionalizar o cumprimento regulatório, criando uma estrutura de gestão que garanta a prioridade da conformidade sobre os objetivos operacionais ou comerciais.

Acesso a Dados (Pesquisadores/Verificadores de Fatos): Empoderar o ecossistema democrático e a supervisão externa, assegurando o acesso a dados relevantes das plataformas para estudos independentes de riscos sistêmicos e desinformação.

Linguagem Clara e Compreensível: Assegurar que as informações de transparência sejam claras, compreensíveis e acessíveis a usuários, pesquisadores e reguladores, indo além da mera publicação formal.

Códigos de Conduta: Identificar o grau de relevância e incentivo à criação códigos de conduta para a densificação, verificação e adaptação de obrigações regulatórias por meio de instrumentos de corregulação e autorregulação voluntária.

Prestação de contas por parte das autoridades regulatórias: Avaliar o grau de *accountability* institucional das autoridades regulatórias em suas funções normativas, fiscalizatórias e decisórias, examinando se fornecem informações claras, tempestivas e acessíveis, justificam suas decisões e se submetem a mecanismos de controle interno e externo.

Adequação tecnológica e operacional: Identificar medidas de aprimoramento de capacidades tecnológicas e operacionais, com priorização de ferramentas e funcionalidades que contribuam adoção e a publicização de medidas para impedir ou diminuir a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam atingir a integridade do processo eleitoral.

Unidades de Comparação	União Europeia - *Digital Service Act* (DSA)	Reino Unido - *Online Safety Act* (OSA)	Índia – *IT Rules*
Plataformas Sujeitas e Obrigações Agravada	O DSA impõe diferentes níveis de obrigações para plataformas e motores de busca de grande dimensão (VLOPs e VLOSEs)	O OSA adota uma lógica de regulação diferenciada, estabelecendo deveres graduados de acordo com a classificação dos provedores de aplicação em categorias.	Intermediários de mídia social significativos estão sujeitos a obrigações de prestação de contas mais rigorosas, distinguindo-se de provedores comuns pelo número de usuários registrados na Índia, que deve exceder o limite definido pelo Governo Central.

Medidas e Relatórios de Transparência	Considerando 151: A Comissão é competente para estabelecer modelos relativos ao formato, ao conteúdo e a outros pormenores dos relatórios sobre moderação de conteúdos. Art. 15.º, n.º 1: Exige que a maioria dos intermediários de serviços - exceto micro e pequenas empresas - publique relatórios anuais de transparência, contendo: (a) decisões recebidas de autoridades dos Estados-Membros, por tipo de conteúdo ilegal; (b) notificações de entidades e indivíduos, categorizadas por tipo de conteúdo alegadamente ilegal e sinalizadores de confiança, com a medida adotada; (c) moderação proativa de conteúdos, incluindo ferramentas automatizadas e medidas aplicadas; (d) reclamações recebidas e decisões tomadas; e (e) uso de moderação automatizada, com indicadores de precisão e taxas de erro. Art. 15.º, n.º 3 A Comissão pode adotar atos de execução para estabelecer modelos relativos ao formato, ao conteúdo e a outros pormenores dos relatórios de transparência. Art. 24.º, n.º 1: Elenca uma lista de elementos adicionais que devem constar no relatório de transparência. São eles: (a) o número de litígios submetidos a organismos de resolução extrajudicial e os seus resultados; (b) o número de suspensões impostas por utilização abusiva do serviço. Art. 24.º, n.º 2: As plataformas devem publicar semestralmente o número médio mensal de destinatários ativos na União (DSA, Art. 24.º, n.º 2) e submeter à Comissão decisões e exposições de motivos de remoção de conteúdo para inclusão em base de dados pública (DSA, Art. 24.º, n.º 2). Art. 24.º, n.º 6: A Comissão pode adotar atos de execução para estabelecer modelos relativos ao formato, ao conteúdo e a outros pormenores dos relatórios. Art. 42.º: Impõe uma periodicidade mais curta (seis em seis meses) e um conteúdo mais detalhado para os relatórios elaborados por as grandes plataformas (VLOPs e VLOSEs).	Seções 17 e 19: Provedores de Categoria 1 devem explicitar, de forma clara e acessível em seus termos de serviço, suas políticas e processos de proteção de conteúdos de relevância democrática e jornalística, incluindo critérios de identificação e procedimentos para tratar reclamações sobre moderação desses conteúdos. Seção 23, (3)(a) e (10): Dever de fornecimento à OFCOM de uma cópia integral dos registros de avaliações de risco, assim que forem criados ou revisados, garantindo uma supervisão direta e contínua. Seção 77 e Anexo 8: A OFCOM deve exigir anualmente que provedores das Categorias 1, 2A e 2B publiquem relatório de transparência detalhando a incidência de conteúdos prejudiciais e as medidas adotadas para mitigá-los, assegurando completude, precisão e acessibilidade. Seção 94(4)(4A)(f): Estabelece que a OFCOM, ao proteger cidadãos contra danos associados ao conteúdo dos serviços regulados, deve avaliar, entre outros aspectos, o grau de transparência e responsabilidade dos provedores na utilização de sistemas e processos de mitigação desses riscos. Seção 23 (9): Provedores de Categoria 1 devem elaborar e manter registro escrito, claro e acessível, das avaliações de risco relacionadas ao dever de empoderamento do usuário adulto, conforme Seção 14 (5).	Seção 3(1)(j): Todos os intermediários, sejam ou não plataformas de mídia social, devem fornecer informações ou prestar assistência a agências governamentais legalmente autorizadas para investigação, prevenção, detecção ou persecução de infrações, no prazo máximo de 72 horas, reduzido para 24 horas quando se tratar de intermediários de jogos online. Seção 4(1)(d): Os intermediários de mídia social considerados significativos têm o dever de publicar relatórios de conformidade mensais, detalhando as reclamações recebidas e as ações tomadas em resposta a elas. Intermediários de mídia social significativos também devem incluir o número de links ou informações removidos proativamente através de ferramentas automatizadas. Seção 4(6): Dever de fornecimento de razões para ações tomadas. a uma reclamação apresentada, o intermediário deve, de modo razoável, fornecer ao usuário reclamante as razões que justificam a ação tomada - ou a ausência de ação - em relação ao conteúdo ou conduta questionada. Seção 4(8): dever de notificação em casos de remoção de conteúdo criado por usuário, informando a medida adotada e seus fundamentos, assegurada a oportunidade razoável de contestar a decisão, como forma de garantir transparência e contraditório no processo de moderação.

Avalições e Relatórios de Impacto	Considerando 85: Conservação de todos os documentos comprovativos relacionados às avaliações dos riscos realizados por VLOPs e VLOSEs e VLOPs. Art. 34.º, n.º 1: Exige que provedores de aplicação de grande dimensão (VLOPs e VLOSEs) realizem, ao menos anualmente, avaliação dos riscos sistêmicos de seu serviço, abrangendo: (i) difusão de conteúdos ilegais; (ii) efeitos negativos reais ou previsíveis sobre direitos fundamentais; (iii) impactos sobre discurso cívico, processos eleitorais e segurança pública; e (iv) efeitos sobre violência de gênero, saúde pública, proteção de menores e bem-estar físico e mental. Art. 36.º, n.º 1 e 2: Exige que VLOPs e VLOSEs apresentem à Comissão relatório de impacto detalhando como seus serviços podem contribuir para ameaças graves à segurança ou à saúde pública na União, incluindo medidas específicas, eficazes e proporcionais para prevenir, eliminar ou limitar tais impactos.	Seção 23(2): Todos os provedores estão obrigados a elaborar e conservar, em linguagem clara e acessível, registros escritos de todas as avaliações de riscos. Seção 23(10): Obrigação de fornecer à OFCOM cópia integral dos registros de avaliações de risco assim que criados ou revisados, garantindo supervisão direta e contínua, abrangendo os diferentes níveis de risco detalhados na Seção 9(5). Seção 22: Obrigação de elaborar e publicar avaliação de impacto das medidas ou políticas de segurança em fase de decisão, considerando seus efeitos sobre a liberdade de expressão legalmente garantida e a privacidade dos usuários. Seção 9(4) e Seção 26(4): Exigem a realização de nova avaliação de risco de conteúdo ilegal, adequada e suficiente, antes de mudanças significativas no design ou operação do serviço, considerando: (i) o risco de dano a indivíduos por diferentes tipos de conteúdo ilegal ou facilitação de priority offences; e (ii) a natureza e gravidade do dano potencial aos indivíduos.	Não informado.
Verificação Externa (Auditoria e Controle Regulatório)	Considerando 92: VLOPs e VLOSEs serão responsabilizadas, por meio de auditorias independentes, pelo cumprimento das obrigações do regulamento e, quando aplicável, de compromissos adicionais previstos em códigos de conduta e protocolos de crise. Considerando 93: O relatório de auditoria deverá ser fundamentado, a fim de descrever eficazmente as atividades empreendidas e as conclusões alcançadas. Art. 37.º: Exige que VLOPs e VLOSEs se submetam, ao menos anualmente e a suas custas, a auditorias independentes, cujo relatório fundamentado deve apresentar recomendações operacionais caso não seja 'positivo' (DSA, Art. 37.º, n.º 6). Art. 49.º, n.º 1 e 2: Os Coordenadores dos Serviços Digitais são autoridades competentes designadas por cada Estado-Membro da União Europeia para supervisionar os prestadores de serviços intermediários e aplicar o DAS.	Seção 104: A OFCOM pode nomear, ou exigir que o provedor nomeie, pessoa qualificada para elaborar relatório destinado a auxiliar a identificação e avaliação de falhas ou potenciais falhas do provedor no cumprimento de requisitos relevantes. Seção 178(3)(a)(iii): O Secretário de Estado deve revisar o funcionamento do quadro regulatório, avaliando se os serviços regulados operam com sistemas e processos que garantam, na medida do pertinente, transparência e accountability aos usuários, especialmente em relação às medidas adotadas para cumprimento dos deveres normativos. Schedule 12, Paragragh 4: A OFCOM pode emitir notificação de auditoria exigindo que o provedor permita avaliação do cumprimento dos requisitos aplicáveis ou da existência de riscos e das medidas para mitigá-los.	Seção 4(9): O Ministério pode solicitar informações adicionais a qualquer intermediário de mídia social significativo, conforme considere necessário.

Governança Interna (Função de Compliance)	Art. 41.º, n.º 1: Estabelece que os VLOPs e VLOSEs deverão criar uma "função de conformidade" destacada e independente de outras funções operacionais. Art. 41.º, n.º 2: O chefe de conformidade deve prestar contas diretamente ao órgão de administração do fornecedor e pode alertar sobre riscos ou incumprimentos do DSA. Para assegurar independência, não pode ser destituído sem aprovação prévia do órgão de administração.	Seção 103: A OFCOM pode emitir uma notificação dirigida a um provedor, exigindo a nomeação de um gerente sênior, que assumirá um papel significativo na tomada de decisões relacionadas à conformidade regulatória imposta pelo OSA. Seção 23: Os provedores devem manter trilhas de auditoria detalhadas sobre suas decisões e sistemas de segurança. Seção 23(2): Todos os provedores estão obrigados a elaborar e conservar, em linguagem clara e acessível, registros escritos de todas as avaliações de riscos. Seção 23(3)(a)(b): Os provedores devem elaborar e manter registro escrito das medidas adotadas ou vigentes para cumprir deveres relevantes, especialmente quando previstas em código de conduta e recomendadas como meios adequados de observância do regulamento.	Não informado.
Acesso a Dados (Pesquisadores e Verificadores de Fatos):	Art. 40.º: VLOPs e VLOSEs devem fornecer acesso a seus dados ao coordenador dos serviços digitais e à Comissão Europeia para monitorar o cumprimento do regulamento (n.º 1), bem como a pesquisadores habilitados para investigações sobre riscos sistêmicos (n.º 4).	Seção 154A: O Secretário de Estado pode, via regulamentos, exigir que provedores de serviços regulados forneçam informações para pesquisa independente sobre segurança online, sem exigir: (i) processamento de dados em violação à proteção de dados pessoais; ou (ii) fornecimento de informações protegidas por segredo empresarial. Seção 162: Exige que a OFCOM elabore relatório avaliando o acesso atual de pesquisadores independentes a dados de provedores de serviços regulados, detalhando como e em que medida essas informações podem ser obtidas para subsidiar pesquisas em segurança online.	Não informado.

Linguagem Clara e Compreensíve	Art. 14.º, n.º 1: Exige que VLOPs e VLOSEs forneçam aos destinatários uma síntese clara, concisa, acessível e legível por máquina dos termos e condições, incluindo os mecanismos de ressarcimento e reparação disponíveis. Art. 17.º, n.º 1: Impõe a exposição de motivos, de forma clara e específica, a todos os destinatários do serviço em relação à moderação de conteúdo. Art. 27.º, n.º 1: Exige que os termos e condições de serviço indiquem, de forma clara e inteligível, os principais parâmetros dos sistemas de recomendação e as opções disponíveis aos destinatários para alterá-los ou influenciá-los.	Secções 10(9), 12(14): Plataformas digitais user-to-user e motores de busca devem publicar, em termos de serviço ou declaração pública equivalente, resumo acessível dos resultados de suas avaliações de risco mais recentes sobre veiculação de conteúdo ilegal. Seção 72(7): Provedores devem incluir em seus termos de serviço, de forma acessível inclusive a crianças, disposições sobre políticas e procedimentos para tratar e resolver reclamações relacionadas à moderação de conteúdos gerados por usuários.	Não informado.
Códigos de Conduta	Arts. 45.º, 46 e 47: Incentivo e facilitação, por parte da Comissão Europeia, de elaboração de códigos conduta facultativos a nível da União. O Código de Conduta sobre Desinformação oferece um conjunto de “compromissos” para enfrentar os danos da desinformação. No âmbito do Código, o dever de prestar contas está associado a uma vasta gama de compromissos que visam garantir a transparência, a supervisão e a responsabilidade dos signatários.	Seção 41: A OFCOM é obrigada a preparar e emitir códigos de prática para provedores de serviços regulados. O dever se divide em códigos específicos para certos tipos de conteúdo e códigos gerais para outros deveres. Seção 41 (4): A OFCOM deve preparar e emitir um código de prática para provedores de Serviços Categoria 1 e Serviços Categoria 2a descrevendo medidas recomendadas para o cumprimento dos deveres estabelecidos no Capítulo 5 (publicidade fraudulenta). Seção 41 (5): A OFCOM pode emendar, emitir uma substituição ou retirar um código de prática em vigor. Schedule 4, Paragraphs 1 e 2: Ao elaborar um código, a OFCOM deve avaliar a adequação das disposições a diferentes tipos e tamanhos de serviços, bem como a provedores de variadas capacidades, assegurando que as medidas sejam claras, proporcionais e tecnicamente viáveis.	Seção 13 (1)(a): Ministério deverá coordenar e facilitar a adesão ao Código de Ética por parte dos editores e dos organismos de autorregulação, desenvolver um Mecanismo de Supervisão e desempenhar as seguintes funções: publicar uma carta de diretrizes destinada aos organismos autorreguladores, incluindo Códigos de Prática aplicáveis a esses órgãos.

Prestação de contas por parte das autoridades regulatórias	Considerando 122: O coordenador dos serviços digitais deverá publicar regularmente, nomeadamente no seu sítio web, um relatório sobre as atividades realizadas ao abrigo do regulamento. Art. 35.º, n.º 2: A Comissão e o Comitê devem publicar anualmente relatórios abrangentes sobre mitigação de riscos sistêmicos, incluindo: (a) identificação e avaliação dos riscos mais significativos e recorrentes reportados por VLOPs e VLOSEs; e (b) boas práticas de mitigação adotadas por essas plataformas, discriminando os riscos por Estado-Membro e pela União, quando aplicável. Art. 36.º, n.º 7 e 11: A Comissão deve emitir um relatório sobre o acompanhamento das medidas de mitigação de riscos sistêmicos indicadas nos relatórios de impacto publicados por VLOPs e VLOSEs. Art. 55.º, n.º 1 e 2: Os coordenadores dos serviços digitais devem elaborar relatório anual sobre suas atividades, incluindo número de reclamações e resumo do acompanhamento, bem como quantidade e objeto das decisões sobre conteúdos ilegais, decisões de prestação de informações e seus efeitos.	Seção 92: A OFCOM deve demonstrar como suas ações estão alinhadas com as prioridades governamentais e deve prestar contas publicamente sobre suas estratégias. Seção 149: A OFCOM deve ser transparente sobre como e contra quem exerce seus poderes de aplicação da lei. Seções 159: A OFCOM deve elaborar e publicar relatórios de transparência com base nas informações dos provedores, incluindo resumo de conclusões, padrões ou tendências identificadas e medidas consideradas 'boas práticas da indústria', excluindo informações confidenciais ou prejudiciais a indivíduos ou entidades.	Seção 19(1)(2): O dever de prestação de contas também é estendido aos Órgãos de Autorregulação (Self-Regulating Bodies), que devem fazer uma divulgação pública, verdadeira e completa de todas as reclamações recebidas e de como foram tratadas, com atualizações mensais.
Adequação tecnológica e operacional	Art. 35.º, n.º 1, alínea "a": VLOPs e VLOSEs devem efetuar adaptação do Serviço, incluindo conceção, elementos ou funcionamento das interfaces online. Art. 35.º, n.º 1", alínea "d": VLOPs e VLOSEs devem realizar teste e adaptação de sistemas algorítmicos (incluindo sistemas de recomendação e correção de critérios). Art. 35.º, n.º 1, alínea "f": VLOPs e VLOSEs devem reforçar processos ou supervisionar atividades, detecção de riscos). Art. 36.º, n.º 1, alínea "b": VLOPs e VLOSEs devem adaptar processos de moderação de conteúdos e aumento de recursos em caso de crise.	Seção 121(2)(3): Os provedores de serviços podem ser especificamente obrigados a aprimorar suas capacidades tecnológicas no contexto de lidar com conteúdo terrorista (terrorism content) e abuso e exploração sexual infantil (CSEA content).	Seção 4: Os intermediários de mídias sociais significativos devem se esforçar para implantar medidas baseadas em tecnologia, incluindo ferramentas automatizadas ou outros mecanismos para identificar proativamente conteúdos relacionados a abuso sexual.

Análise adicional do REGULAMENTO UE 2024/900:

Unidades de Comparação	União Europeia - *Digital Service Act* (DSA)
Plataformas Sujeitas e Obrigações Agravadas	O Regulamento UE 2024/900 impõe diferentes níveis de obrigações para plataformas e motores de busca de grande dimensão (VLOPs e VLOSEs).
Medidas e Relatórios de Transparência	Artigo 6.º, n.º 1 e 2: A prestação de serviços de propaganda política deve ser transparente, assegurando que as disposições contratuais permitam o cumprimento do Regulamento. Art. 9.º, n.º 1, 2 e 3: Prestadores de serviços devem conservar, por sete anos em formato eletrônico legível por máquina, registros sobre montantes faturados ou benefícios recebidos, origem dos fundos (pública/privada, UE/fora da UE) e identidade do patrocinador e da entidade controladora. Art. 11.º, n.º 1: Editores devem assegurar que cada anúncio seja identificado de forma clara e inequívoca como político, indicando a identidade do patrocinador e se houve uso de técnicas de direcionamento. Art. 12.º, n.º 1, 3 e 4: Editores devem fornecer Aviso de Transparência contendo: identidade do patrocinador/entidade controladora, período de divulgação, montantes agregados, origem dos fundos, eleição ou referendo associado, links para o Repositório Europeu e, se possível, dados de alcance/interações, devendo conservar o aviso por sete anos. Art. 13.º, n.º 2: Editores que são VLOPs/VLOSEs devem garantir que cada anúncio de cariz político e as informações de transparência (Artigo 12.º, n.º 1) sejam disponibilizados no seu repositório de anúncios (Art. 39.º do Regulamento (UE) 2022/2065), a partir do momento da publicação e durante todo o período de veiculação, e acessíveis através do Repositório Europeu durante sete anos após o anúncio ser veiculado pela primeira vez. Artigo 14.º, n.º 1: Editores de propaganda política devem incluir informações sobre os montantes recebidos, incluindo a utilização de técnicas de direcionamento, agregadas por campanha, num anexo ao seu relatório de gestão anual. Art. 19.º, n.º 1, alíneas “a” e “b”: Responsáveis pelo tratamento que usam técnicas de direcionamento devem adotar e disponibilizar publicamente uma política interna que descreva o seu uso, e manter registros sobre essas técnicas. Art. 19.º, n.º 1, alínea “c”: Responsáveis pelo tratamento que usam técnicas de direcionamento devem facultar, juntamente com a indicação de que se trata de um anúncio de cariz político, informações adicionais necessárias para permitir que a pessoa em causa compreenda a lógica subjacente e os principais parâmetros das técnicas utilizadas, nomeadamente se foi utilizado um sistema de inteligência artificial para o direcionamento ou a distribuição do anúncio de cariz político.
Avaliações e Relatórios de Impacto	Considerando 46: Editores que são VLOPs/VLOSEs devem identificar, analisar e avaliar diligentemente os riscos sistémicos que os serviços de propaganda política colocam, em conformidade com o Regulamento (UE) 2022/2065. Art. 19.º, n.º 1, alínea “d”: Os responsáveis pelo tratamento que usam técnicas de direcionamento devem preparar uma avaliação anual interna dos riscos para os direitos e liberdades fundamentais, cujos resultados devem ser disponibilizados ao público.
Verificação Externa (Auditoria e Controle Regulatório)	Artigo 16.º, n.º 1: Autoridades nacionais competentes têm poderes para solicitar todas as informações necessárias aos prestadores de serviços de propaganda política para verificar o cumprimento dos deveres de transparência. Art. 22.º, n.º 5, alínea “a”: As autoridades competentes têm poderes para solicitar acesso a dados e documentos, emitir advertências, ordenar a cessação de infrações, e aplicar sanções financeiras/medidas de correção.

Governança Interna (Função de Compliance)	Art. 6.º, n.º 2: Prestadores de serviços devem garantir que os acordos contratuais permitem o cumprimento do Regulamento. Art. 7.º, n.º 5: Prestadores de serviços que utilizem interfaces online devem concebê-las para facilitar o cumprimento das obrigações pelos patrocinadores. Art. 16.º, n.º 5: Prestadores de serviços de propaganda política devem designar um ponto de contacto para a interação com as autoridades nacionais competentes.
Acesso a Dados (Pesquisadores/ Verificadores de Fatos)	Art. 17.º, n.º 1 e 2 : A pedido de entidades interessadas (incluindo investigadores, jornalistas, organizações da sociedade civil e observadores eleitorais), os prestadores de serviços devem transmitir gratuitamente e rapidamente as informações de transparência (Artigos 9.º, 11.º e 12.º), num formato legível por máquina, se possível. Art. 20.º: Os responsáveis pelo tratamento devem transmitir às entidades interessadas as informações sobre o uso de técnicas de direcionamento (Artigo 19.º).
Linguagem Clara e Compreensível	Artigo 12.º, n.º 3: Os Avisos de Transparência devem ser claramente visíveis e de fácil utilização, nomeadamente através da utilização de linguagem simples, e devem cumprir os requisitos de acessibilidade aplicáveis (atendendo às necessidades de pessoas com deficiência). Art. 19.º, n.º 1, alínea “a”, e 4: A política interna sobre técnicas de direcionamento deve ser redigida em linguagem clara e simples. As informações adicionais sobre direcionamento devem ser apresentadas de forma facilmente acessível e de fácil utilização.
Códigos de Conduta	Art. 11.º, n.º 5: Os Estados-Membros e a Comissão devem incentivar a elaboração de códigos de conduta voluntários para apoiar a correta aplicação dos requisitos de rotulagem (Artigo 11.º), tendo em conta as características específicas dos prestadores de serviços pertinentes e as necessidades específicas das micro, pequenas e médias empresas.
Prestação de contas por parte das autoridades regulatórias	Artigo 13.º, n.º 1: A Comissão deve estabelecer e gerir o Repositório Europeu de Anúncios de Cariz Político Online, que deve ser público e fornecer acesso a todos os anúncios online e respetivas informações de transparência num formato legível por máquina e através de um portal único. Art. 21.º, n.º 4: Os Estados-Membros devem manter registros públicos e legíveis por máquina dos representantes legais de prestadores não estabelecidos na União. Art. 25.º, n.º 8: Os Estados-Membros devem apresentar relatórios anuais à Comissão sobre as sanções impostas. Art. 26.º: Os Estados-Membros devem publicar as datas das eleições e referendos em local facilmente acessível, e a Comissão disponibiliza um portal para essas informações. Art. 27.º: A Comissão deve apresentar um relatório público de avaliação e revisão sobre a aplicação e eficácia do Regulamento ao Parlamento Europeu e ao Conselho, no prazo de dois anos após cada eleição europeia.

2.9.4 *BENCHMARK* INTERNACIONAL (SÍNTESE COMPARATIVA)

União Europeia (UE) – DAS

Relatórios de Transparência Gerais e Detalhados: A maioria dos prestadores de serviços intermediários, exceto micro e pequenas empresas, deve publicar relatórios de transparência anuais (Art. 15º, n.º 1), detalhando: decisões recebidas de autoridades; notificações de conteúdos alegadamente ilegais, incluindo de sinalizadores de confiança e medidas adotadas; moderação proativa, com uso de ferramentas automatizadas e tipos de medidas; número de reclamações e decisões tomadas; e indicadores de precisão e taxas de erro das ferramentas automatizadas.

Relatórios Aumentados para VLOPs e VLOSEs: VLOPs e VLOSEs devem apresentar relatórios semestrais mais detalhados (Art. 42º), incluindo número e resultados de litígios submetidos à resolução extrajudicial e número de suspensões por uso abusivo do serviço (Art. 24º, n.º 1).

Avaliação e Documentação de Riscos Sistêmicos: Impõe-se às VLOPs e VLOSEs o dever de realizar, pelo menos anualmente, uma avaliação dos riscos sistêmicos decorrentes do seu serviço, que incluem a difusão de conteúdos ilegais e os efeitos negativos em direitos fundamentais ou processos eleitorais (Art. 34.º, n.º 1). Além disso, devem conservar todos os documentos comprovativos relacionados a essas avaliações (Considerando 85).

Relatórios de Impacto e Mitigação: VLOPs e VLOSEs devem apresentar à Comissão Europeia relatórios de impacto contendo informações sobre como seus serviços podem contribuir para uma ameaça grave à segurança pública ou à saúde pública, devendo incluir medidas específicas para prevenir ou limitar essa contribuição.

Auditorias Independentes: As VLOPs e VLOSEs são obrigadas a submeter-se, pelo menos uma vez por ano e a expensas próprias, a auditorias independentes (Art. 37º). O relatório de auditoria deve ser fundamentado e, em caso de resultado não "positivo", deve incluir recomendações operacionais (Art. 37.º, n.º 6; Considerando 93).

Função de Conformidade Independente: VLOPs e VLOSEs devem criar uma "função de conformidade" destacada e independente de outras funções operacionais. O chefe dessa função deve prestar contas diretamente ao órgão de administração e pode manifestar preocupações ou advertir sobre riscos ou incumprimentos do DSA (Art. 41º, n.º 1 e 2).

Acesso a Dados para Supervisão e Pesquisa: VLOPs e VLOSEs devem conceder acesso aos seus dados ao Coordenador dos Serviços Digitais e à Comissão Europeia para que estes possam controlar o cumprimento do regulamento (Art. 40º, n.º 1). O acesso a dados também deve ser facultado a investigadores habilitados para investigações sobre riscos sistêmicos (Art. 40º, n.º 4).

Transparência ao Usuário na Moderação: Há a obrigação de fornecer, em linguagem clara e inequívoca, uma síntese concisa dos termos e condições, incluindo mecanismos de ressarcimento (Art. 14, n.º 1). Em relação à moderação, impõe-se a exposição de motivos de forma clara e específica a todos os destinatários do serviço (Art. 17, n.º 1).

Relatório Regulatório: Os Coordenadores dos Serviços Digitais devem elaborar um relató-

rio anual sobre suas atividades, incluindo o número de reclamações, a síntese do seguimento dado e o objeto das decisões de atuação contra conteúdos ilegais (Art. 55, n.º 1 e 2).

Adequação Tecnológica: VLOPs e VLOSEs devem efetuar adaptação do de seus serviço, com a realização de testes e adaptação de sistemas algorítmicos (incluindo sistemas de recomendação e correção de critérios), bem como reforçar processos internos de supervisão, detecção de riscos (Art. 35.º). Além disso, as VLOPs e VLOSEs devem adaptar processos de moderação de conteúdos e aumento de recursos em caso de crise (Art. 36.º).

Reino Unido – OSA

Relatórios de Transparência Anuais: Provedores das Categorias 1, 2A e 2B devem elaborar e publicar relatórios de transparência anuais a pedido da OFCOM, detalhando a incidência de conteúdos prejudiciais e as medidas de mitigação adotadas. Os relatórios devem ser completos, precisos e acessíveis (Seção 77 e Anexo 8).

Avaliações de Risco e Registros Escritos: Todos os provedores estão obrigados a elaborar e conservar registros escritos de todas as avaliações de riscos em linguagem clara e acessível (Seção 23(2); Seção 17). Provedores de Categoria 1 devem manter um registro escrito das avaliações de risco relacionadas ao empoderamento do usuário adulto (Seção 23 (9)).

Registro de Medidas de Cumprimento: Os provedores devem manter um registro escrito das medidas adotadas ou em vigor para o cumprimento de deveres relevantes, especialmente aquelas descritas em códigos de conduta (Seção 23(3)(a)(b)).

Fornecimento de Registros à OFCOM: Há o dever de fornecer à OFCOM uma cópia integral dos registros de avaliações de risco assim que forem criados ou revisados, garantindo supervisão direta e contínua (Seção 23, (3)(a) e (10); Seção 17).

Avaliação de Impacto e Liberdade de Expressão: Os provedores devem elaborar e publicar uma avaliação do impacto que as medidas ou políticas de segurança, em fase de decisão, teriam sobre o direito dos usuários à liberdade de expressão dentro da lei e sobre a privacidade (Seção 22). Uma nova avaliação de risco deve ser feita antes de qualquer mudança significativa no design ou operação do serviço (Seção 9(4) e Seção 26(4)).

Trilhas de Auditoria e Supervisão: Os provedores devem manter trilhas de auditoria detalhadas sobre suas decisões e sistemas de segurança (Seção 23). A OFCOM pode emitir uma notificação de auditoria para avaliar o cumprimento dos requisitos (Schedule 12, Paragragh 4), ou exigir a nomeação de um gerente sênior para a conformidade regulatória (Seção 103).

Transparência Específica para Conteúdos Sensíveis: Provedores de Categoria 1 devem explicitar em termos de serviço suas políticas e processos de proteção de conteúdos de relevância democrática e jornalísticos (Seções 17 e 19). Plataformas *user-to-user* e motores de busca devem publicar resumo acessível de suas avaliações de risco mais recentes sobre conteúdo ilegal (Seções 10(9), 12(14)).

Reclamações e Resolução: Os termos de serviço devem incluir disposições de fácil acesso que especifiquem as políticas e procedimentos aplicáveis ao tratamento e à resolução de reclamações relacionadas à moderação de conteúdos gerados por usuários, inclusive para crianças (Seção 72(7)).

Acesso a Dados para Pesquisa Independente: O Secretário de Estado pode exigir, via regulamentos, que os provedores forneçam informações para pesquisa independente sobre segurança online, respeitando a legislação de proteção de dados e segredos de negócio (Seção 154A).

Prestação de Contas da OFCOM: A OFCOM deve produzir e publicar seus próprios relatórios de transparência com base nas informações recebidas dos provedores, incluindo um resumo das conclusões, tendências identificadas e sugestões de "boa prática da indústria" (Seções 159). A OFCOM também é obrigada a ser transparente sobre como e contra quem exerce seus poderes de aplicação da lei (Seção 149).

Índia – *IT Rules*

Relatórios de Conformidade Mensais: Os intermediários de mídia social significativos têm o dever de publicar relatórios de conformidade mensais. Esses relatórios devem detalhar as reclamações recebidas e as ações tomadas em resposta a elas, além de incluir o número de links ou informações removidos proativamente por meio de ferramentas automatizadas (Seção 4(1)(d)).

Fornecimento de Razões e Contraditório: Os intermediários devem fornecer ao usuário reclamante as razões que justificam a ação tomada (ou a ausência de ação) em relação ao conteúdo questionado (Seção 4(6)). Em casos de remoção de conteúdo, o intermediário deve notificar o usuário da medida e seus fundamentos, garantindo uma oportunidade razoável de contestar a decisão (Seção 4(9)).

Assistência Rápida a Agências Governamentais: Todos os intermediários são obrigados a fornecer informações ou assistência a agências governamentais legalmente autorizadas para fins de investigação, prevenção ou persecução de infrações. Essa obrigação deve ser cumprida no prazo máximo de 72 horas, reduzido para 24 horas no caso de intermediários que operam com jogos online (Seção 3(1)(j)).

Prestação de Contas da Autorregulação: Os Órgãos de Autorregulação também têm o dever de prestação de contas, devendo fazer uma divulgação pública, verdadeira e completa de todas as reclamações recebidas e de como foram tratadas, com atualizações mensais (Seção 19(1)(2)).

Solicitação Ministerial: O Ministério pode solicitar informações adicionais a qualquer intermediário de mídia social significativo, conforme considere necessário para a supervisão (Seção 4(9)).

29.5 INTERPRETAÇÃO DO ART. 9º-D À LUZ DO *BENCHMARKING* INTERNACIONAL

O *caput* do art. 9º-D da Res. TSE 23.610/2019 estabelece o dever de transparência e prestação de contas para provedores de aplicação de internet, exigindo a demonstração de medidas para impedir ou mitigar a circulação de desinformação que ameace a integridade do processo eleitoral. Uma interpretação adequada deve considerar três dimensões fundamentais:

Eficiência: A obrigação vai além da adoção formal de políticas, centrando-se na eficácia concreta das medidas, com resultados efetivos na contenção de conteúdos ilícitos ou desinformativos.

A prestação de contas deve demonstrar o impacto real das ações implementadas, superando meros procedimentos formais.
Intensidade proporcional: Embora a Resolução não estabeleça níveis diferenciados de exigência, a experiência internacional indica que a prestação de contas deve ser proporcional ao alcance e influência da plataforma. VLOPs e VLOSEs devem cumprir obrigações acrescidas de transparência e *accountability* devido ao seu impacto sistêmico sobre a integridade informacional e o debate público democrático.

Vigência contínua: O dever de prestação de contas não se limita ao período oficial de campanha. Para períodos fora da pré-campanha ou campanha eleitoral, aplica-se a tese do STF nos Temas 987 e 533 da Repercussão Geral, determinando que provedores de aplicação de internet atuantes no Brasil devem fornecer às autoridades informações sobre funcionamento do provedor, regras e procedimentos de moderação, gestão de reclamações, relatórios de transparência e medidas de monitoramento e mitigação de riscos sistêmicos.

A análise comparada com marcos regulatórios internacionais oferece um roteiro para transformar esses princípios em mecanismos concretos e verificáveis. O objetivo central do dispositivo é assegurar a eficácia concreta das ações, exigindo que os provedores demonstrem resultados efetivos na contenção de conteúdos notoriamente inverídicos ou gravemente descontextualizados que possam comprometer a integridade do processo eleitoral.

Em Síntese:

Destinatários do dever de prestação de contas:

A obrigação de prestação de contas prevista no art. 9º-D da Res. TSE n.º 23.610/2019 incide sobre todos os provedores de aplicação que possibilitem a veiculação de conteúdo político-eleitoral, ainda que não ofertem serviços de impulsionamento.

Ainda que o art. 9º-D da Res. TSE n.º 23.610/2019 se dirija apenas aos provedores de aplicação que veiculem conteúdo político-eleitoral, mesmo sem ofertar impulsionamento, o art. 9º-G expressa o compromisso da Justiça Eleitoral com os princípios da publicidade e da *accountability*. O caput impõe ao TSE um dever de transparência institucional, determinando que todas as decisões de remoção de conteúdos - quando relacionados a fatos notoriamente inverídicos ou gravemente descontextualizados que afetem a integridade do processo eleitoral - sejam disponibilizadas em repositório público. Já o §2º do mesmo artigo institui obrigações procedimentais aos provedores de aplicação no cumprimento das ordens judiciais de retirada, configurando não apenas a execução material da decisão, mas um mecanismo de efetiva prestação de contas.

No modelo europeu instituído pelo DSA, o dever de prestação de contas aplica-se a todos os provedores de aplicação, com encargos acrescidos para VLOPs e VLOSEs. A prestação de contas é estendida para outros atores, como os Coordenadores de Serviços Digitais, a Comissão Europeia e o Comitê, que também devem divulgar relatórios periódicos e anuais sobre suas atividades, notadamente quanto à mitigação de riscos sistêmicos, cabendo à Comissão acompanhar as medidas de mitigação indicadas nos relatórios de impacto das VLOPs e VLOSEs.

No âmbito do OSA, o dever de prestação de contas abrange todos os provedores de serviço, que devem elaborar e manter registros escritos de suas avaliações de risco em linguagem clara. Os

provedores das categorias 1, 2A e 2B têm ainda a obrigação de publicar relatórios anuais de transparência, detalhando a incidência de conteúdos prejudiciais e as medidas de mitigação adotadas. O dever também alcança o Secretário de Estado, responsável por revisar o funcionamento do regime regulatório, e a OFCOM, encarregada de elaborar e divulgar relatórios de transparência baseados nas informações prestadas pelos provedores.

Na Índia, as obrigações mais rigorosas são impostas aos intermediários de mídia social considerados significativos (com base no número de usuários), que devem publicar relatórios de conformidade mensais detalhando reclamações e ações tomadas. Aqui, o dever de prestação de contas também se estende aos Órgãos de Autorregulação (*Self-Regulating Bodies*), que devem divulgar publicamente todas as reclamações recebidas e o seu tratamento, com atualizações mensais.

À luz do *benchmarking* internacional, percebe-se que o modelo regulatório brasileiro instituído pela Res. TSE 23.610/2019 se distancia dos diplomas analisados, na medida em que não estabelece um padrão robusto de *accountability* multinível, que alcance não apenas os provedores, mas também o próprio Tribunal Superior Eleitoral, na qualidade de órgão regulador.

Aspectos materiais e procedimentais que devem ser objeto de prestação de contas:

No que tange ao seu objeto, não se limita à comprovação formal de medidas contra a desinformação, mas assegurar eficácia concreta, de modo que mecanismos protocolares se traduzam em resultados efetivos na contenção de conteúdos ilícitos e desinformativos. É dizer: não basta apenas pretender cumprir a Resolução; é necessário que as medidas adotadas para tal finalidade sejam comprovadamente eficazes.

Na União Europeia, a prestação de contas das plataformas é escalonada, mais rigorosa para VLOPs e VLOSEs. O DSA exige relatórios anuais (ou semestrais para grandes plataformas) sobre notificações de conteúdos ilegais, medidas adotadas, moderação própria - incluindo ferramentas automatizadas -, indicadores de precisão e decisões sobre reclamações. Para VLOPs/VLOSEs, o foco central é a avaliação anual de riscos sistêmicos, abrangendo difusão de conteúdos ilegais, impactos no discurso cívico, processos eleitorais e segurança pública. Procedimentalmente, essas plataformas devem submeter-se a auditorias independentes, manter documentação das avaliações de risco, criar função de conformidade independente, justificar decisões de moderação e garantir acesso a dados a reguladores e pesquisadores.

No Reino Unido, a prestação de contas incide sobre gestão de riscos e integridade dos processos de segurança, escalonada por categoria de provedor. Exige-se elaboração e manutenção de registros de todas as avaliações de risco, compatíveis com o nível de dano de diferentes conteúdos ilegais; provedores de Categoria 1 devem registrar também avaliações voltadas ao empoderamento do usuário adulto. É obrigatória avaliação de impacto antes da implementação de políticas de segurança, considerando liberdade de expressão e privacidade. Procedimentalmente, os provedores devem fornecer à OFCOM cópia integral dos registros, publicar relatórios anuais sobre conteúdos prejudiciais e medidas de mitigação e, quando exigido, nomear gerente sênior de conformidade e submeter-se a auditorias.

Na Índia, o dever de prestação de contas recai sobre transparência operacional e conformidade legal, especialmente para intermediários de mídia social significativos. O aspecto material central da obrigação recai sobre a publicação de relatórios mensais, contendo detalhes sobre as reclamações recebidas, as ações adotadas e os conteúdos removidos proativamente por ferramentas auto-

matizadas. Procedimentalmente, os intermediários devem cooperar com agências governamentais legalmente autorizadas, fornecendo informações em prazos curto, notificar usuários sobre remoções de conteúdo, explicando fundamentos e garantindo oportunidade de contestação, e atender a solicitações adicionais do Ministério quando necessário.

Titulares ou entes legitimados a receber as informações decorrentes do dever de prestação de contas, considerando as esferas institucional e social de *accountability*:

Embora o Art. 9º-D estabeleça o dever de transparência e prestação de contas para os provedores de aplicação de internet que permitam a veiculação de conteúdo político-eleitoral, a Resolução TSE 23.610/2019 não define claramente quem são os destinatários institucionais ou públicos desses relatórios. De modo diverso, a experiência regulatória internacional estabelece ecossistema complexo e multinível de *accountability*, abrangendo tanto a esfera institucional (reguladores e governo) quanto a esfera social (público, usuários e pesquisadores).

Diante de uma interpretação sistemática do art. 9º-D, e que leve em conta os padrões atuais de *accountability* tanto no setor público quanto privado, bem como a lógica do microssistema de normas do Direito Eleitoral, parece seguro afirmar que os principais legitimados a receber as informações decorrentes do dever de prestação de contas são: (i) a Justiça Eleitoral, dada sua função regulatória no tocante à veiculação da propaganda eleitoral; (ii) os próprios partidos, federações, coligações ou candidatos na qualidade de titulares do direito subjetivo à propaganda eleitoral; (iii) a sociedade, incluindo eleitores, usuários das plataformas e serviços de controle da sociedade civil, como institutos de pesquisa, jornalistas e verificadores de fatos.

O art. 36, §2º, da Res. TSE n.º 23.610/2019 exemplifica a prestação de contas voltada aos usuários. O dispositivo exige que, em caso de suspensão temporária de conteúdo por violação à legislação eleitoral, o provedor informe de forma clara o motivo da indisponibilidade. A exigência promove transparência, coíbe remoções arbitrárias e reforça a legitimidade da atuação estatal e das plataformas na regulação eleitoral digital. Durante a suspensão, deve ser exibida mensagem indicando que o conteúdo está temporariamente indisponível por infringir normas eleitorais, com referência ao art. 57-I, §2º, da Lei n.º 9.504/1997.

O dever de prestação de contas não é uniforme, devendo variar em intensidade, escopo e nível de detalhamento conforme o perfil institucional e a função democrática do destinatário. Impõe-se, assim, uma abordagem granular e proporcional, capaz de assegurar à Justiça Eleitoral o acesso a informações técnicas, auditáveis e verificáveis, indispensáveis à fiscalização e à efetividade da regulação. Ao mesmo tempo, deve-se garantir a inteligibilidade e a acessibilidade dos dados destinados ao público em geral, preservando-se, de modo equilibrado, a proteção dos segredos de negócio e das estratégias comerciais das plataformas digitais frente a seus concorrentes, em consonância com o princípio da proporcionalidade e com o dever de transparência responsável.

Momento e periodicidade do cumprimento do dever de prestar contas:

Uma leitura menos atenta da Resolução n.º 23.610/2019 poderia levar a crer que o art. 9º-D se aplica apenas durante o período de campanha eleitoral. Isso decorre do art. 3º-C, que estende fora de campanha apenas as regras de transparência (art. 27-A) e de uso adequado de tecnologias digitais na veiculação de conteúdo político-eleitoral (arts. 9º-B e 9º-C). Contudo, o art. 9º-D deve ser interpretado considerando o princípio da função social, o dever de cuidado e - nos períodos não

abrangidos pela pré-campanha ou pela campanha eleitoral - a tese fixada pelo STF no julgamento dos Temas 987 e 533 Repercussão Geral.

O princípio da função social e o dever de cuidado impõem um dever contínuo de proteção, de modo que instrumentos de notificação, canais de denúncia, ações corretivas e preventivas, e aprimoramento tecnológico não podem se limitar ao período eleitoral. Por sua natureza, os deveres elencados nos incisos do art. 9º-D demandam uma série de providências que antecedem o período eleitoral. Mesmo o dever de elaboração de avaliação de impacto de seus serviços sobre a integridade do processo eleitoral, previsto apenas para o ano eleitoral, requer certa anterioridade, a fim de cumpra sua função de implementar medidas eficazes e proporcionais para mitigar os riscos identificados.

Nos períodos não abrangidos pela pré-campanha ou pela campanha eleitoral, aplica-se a tese fixada pelo STF nos Temas 987 e 533 da Repercussão Geral, que reconheceu a inconstitucionalidade progressiva do art. 19 do MCI. Conforme o item 11(b) do julgado, os provedores de aplicação com atuação no Brasil devem manter sede e representante no país, incumbidos de prestar às autoridades competentes informações relativas ao funcionamento do provedor, às regras e aos procedimentos utilizados para moderação de conteúdo e para gestão das reclamações pelos sistemas internos; aos relatórios de transparência, monitoramento e gestão dos riscos sistêmicos (Brasil, 2025).

Por essas razões, o dever de prestação de contas, assim como os de transparência e de uso adequado de tecnologias digitais na veiculação de conteúdo político-eleitoral, deve vigorar de forma contínua, inclusive fora do período de campanha. Assim, esses deveres devem ser gradativamente implementados nos períodos que antecedem ou sucedem o período oficial de campanha.

Na UE, a prestação de contas ocorre via relatórios periódicos, mais rigorosos para grandes plataformas. Intermediários, exceto micro e pequenas empresas, publicam relatórios anuais (Art. 15º, n.º 1). VLOPs e VLOSEs apresentam relatórios semestrais detalhados (Art. 42º), informam destinatários ativos (Art. 24, n.º 2), realizam avaliação anual de riscos sistêmicos sobre processos eleitorais e discurso cívico (Art. 34º, n.º 1), submetem-se a auditorias independentes (Art. 37º) e conservam continuamente todos os documentos das avaliações, garantindo transparência nos relatórios dos Coordenadores dos Serviços Digitais.

No Reino Unido, a prestação de contas é contínua e vinculada à gestão de riscos. Provedores devem elaborar e conservar registros de todas as avaliações de risco e medidas adotadas (Seção 23(2), (3)(a)), fornecendo cópia integral à OFCOM assim que criados ou revisados (Seção 23(3)(a) e (10)). Alterações significativas no serviço exigem nova avaliação prévia. Provedores das Categorias 1, 2A e 2B devem publicar relatórios de transparência anuais sobre conteúdos prejudiciais e medidas de mitigação (Seção 77 e Anexo 8). O controle é reforçado pela possibilidade de auditorias exigidas pela OFCOM (Schedule 12, Paragraph 4).

Na Índia, a prestação de contas é contínua, focada em transparência operacional e resposta a reclamações. Intermediários significativos devem publicar relatórios mensais detalhando reclamações recebidas, ações adotadas e conteúdos removidos proativamente por ferramentas automatizadas (Seção 4(1)(d)). O controle é reforçado pela obrigação de cooperar com agências governamentais, fornecendo informações ou assistência para investigações em até 72 horas. Órgãos de autorregulação devem divulgar publicamente todas as reclamações e medidas adotadas, com atualizações mensais.

Parâmetros mínimos que devem orientar a elaboração de uma avaliação de impacto sobre a integridade informacional no contexto eleitoral:

O art. 9º-D da Res. TSE 23.610/2019 impõe aos provedores de aplicação de internet, em ano eleitoral, a elaboração de avaliação de impacto sobre a integridade do processo eleitoral, visando implementar medidas eficazes e proporcionais para mitigar riscos (inciso V). Apesar de sua relevância, a Resolução não estabelece parâmetros mínimos nem define o período exato do ano eleitoral em que a avaliação deve ser realizada. Considerando a necessidade de execução prévia para que a avaliação cumpra sua função de implementar medidas eficazes e proporcionais para mitigar os riscos identificados, recomenda-se detalhar o dispositivo quanto ao momento específico de cumprimento desse dever.

Na UE, o DSA estabelece parâmetros rigorosos para avaliação de impacto, focados na identificação e mitigação de riscos sistêmicos. VLOPs e VLOSEs devem realizar avaliação anual abrangente, incluindo efeitos sobre discurso cívico, processos eleitorais, direitos fundamentais, segurança pública e difusão de conteúdos ilegais. O relatório deve detalhar como o serviço pode contribuir para ameaças graves e as medidas proporcionais para mitigá-las, incluindo informações sobre moderação automatizada, indicadores de precisão e taxas de erro. A prestação de contas e o número médio mensal de destinatários ativos devem ser publicados semestralmente, garantindo fiscalização periódica mais frequente.

No Reino Unido, o OSA adota avaliação de impacto dinâmica e preventiva. O parâmetro mínimo exige elaboração e conservação de registros escritos de todas as avaliações de risco, abordando níveis de risco e severidade de dano. É obrigatório elaborar e publicar avaliação de impacto das políticas de segurança sobre liberdade de expressão e privacidade dos usuários. A prestação de contas é contínua e proativa: registros devem ser mantidos e revisados constantemente, nova avaliação é exigida antes de alterações significativas no serviço, e cópias integrais devem ser fornecidas à OFCOM assim que criadas ou revisadas.

Na Índia, as *IT Rules* 2021 adotam prestação de contas retrospectiva e responsiva, em contraste com a avaliação anual de riscos sistêmicos na UE ou no Reino Unido. Intermediários de mídia social significativos (definidos pelo número de usuários registrados) devem publicar relatórios mensais detalhando reclamações recebidas, ações adotadas e conteúdos removidos proativamente por ferramentas automatizadas. A avaliação se concretiza na demonstração da eficácia dessas respostas, garantindo fiscalização de curto prazo.

Diferentes graus de exigência no cumprimento do dever de prestação de contas:

A análise comparada confirma que a intensidade proporcional é um princípio fundamental na regulação internacional. Embora a Resolução TSE n.º 23.610/2019 não discipline de forma clara a gradação de obrigações baseada em parâmetros objetivos, a experiência internacional e a própria racionalidade regulatória indicam que a carga de prestação de contas deve ser proporcional ao poder de influência e ao alcance social da plataforma.

O DSA na União Europeia estabelece níveis diferenciados de obrigação para plataformas e motores de busca de grande dimensão (VLOPs e VLOSEs), refletindo seu impacto sistêmico. Enquanto a maioria dos intermediários publica relatórios anuais, VLOPs e VLOSEs devem apresentar relatórios semestrais mais detalhados e realizar avaliação anual de riscos sistêmicos, incluindo efei-

tos sobre discurso cívico e processos eleitorais. A maior carga de responsabilidade é reforçada por auditorias independentes anuais, criação de função de conformidade destacada e independente, e dever de fornecer acesso a dados a reguladores e pesquisadores habilitados para investigações sobre riscos sistêmicos.

O OSA no Reino Unido adota regulação diferenciada, graduando deveres conforme a categoria do provedor. Provedores das Categorias 1, 2A e 2B, de maior alcance e risco, estão sujeitos a obrigações intensificadas: elaboração e publicação de relatórios de transparência anuais sobre conteúdos prejudiciais e medidas de mitigação; manutenção e revisão contínua de registros de avaliações de risco, fornecendo cópia integral à OFCOM; e, para Categorias 1 e 2A, detalhamento em termos de serviço das políticas de proteção de conteúdos de relevância democrática e jornalística. Essa estrutura assegura supervisão direta e contínua, além da prestação de contas periódica *ex post.*

As *IT Rules* na Índia também estabelecem diferentes escalonamentos de obrigações conforme o porte do provedor, impondo maior rigor a intermediários significativos, definidos pelo número de usuários registrados. Esses provedores devem publicar relatórios mensais detalhando reclamações recebidas, ações adotadas e conteúdos removidos proativamente por ferramentas automatizadas. A periodicidade e o detalhamento das métricas proativas refletem maior exigência de monitoramento e *accountability* em comparação com intermediários menores.

Portanto, propõe-se que o art. 9º-D seja interpretado à luz do princípio da proporcionalidade regulatória, de modo que as plataformas de grande dimensão e elevado alcance - em razão de seu impacto sistêmico sobre a integridade dos processos eleitorais - assumam deveres mais rigorosos de prestação de contas (Bioni, 2022). Tais deveres devem compreender, entre outros, a demonstração da eficácia concreta das medidas adotadas, a submissão a auditorias independentes e a apresentação periódica de relatórios detalhados, em conformidade com o padrão regulatório analisado no *benchmarking.*

Parâmetros mínimos devem orientar o conteúdo e o formato das informações apresentadas no cumprimento do dever de prestação de contas, para assegurar sua utilidade, verificabilidade e compreensão pública:

O Art. 9º-D da Res. TSE n.º 23.610/2019 impõe o dever de prestação de contas, visando garantir a eficácia concreta das medidas adotadas pelas plataformas contra a desinformação. Para que essa prestação de contas seja útil, verificável e compreensível ao público, é necessário que o conteúdo e o formato garantam transparência e precisão. Apesar disso, a Resolução não oferece parâmentos mínimos sobre o conteúdo de relatórios de transparência e de impacto, tampouco dispõe sobre o formato desses documentos.

Na União Europeia, os parâmetros mínimos de conteúdo e formato são densificados para garantir a utilidade e a verificabilidade. Nesse sentido, VLOPs e VLOSEs devem fornecer aos destinatários termos e condições claros, concisos, acessíveis e compatíveis com leitura por máquina, incluindo mecanismos de ressarcimento e reparação. Quanto à moderação de conteúdo, o DSA exige exposição de motivos clara e específica a todos os destinatários. Além disso, é obrigatória a divulgação, em linguagem inteligível, dos principais parâmetros dos sistemas de recomendação e das opções de personalização disponíveis. Por sua vez, VLOPs e VLOSEs estão sujeitos a auditorias independentes, cujos relatórios devem ser fundamentados e, em caso de resultado não positivo, incluir recomendações operacionais.

No Reino Unido, o OSA determina que plataformas user-to-user e motores de busca publiquem, em termos de serviço ou declaração equivalente, resumo acessível das avaliações de risco mais recentes sobre conteúdo ilegal. Os termos devem incluir disposições de fácil acesso, inclusive para crianças, detalhando políticas e procedimentos de tratamento e resolução de reclamações relacionadas à moderação de conteúdo. No tocante à verificação externa, a OFCOM e o Secretário de Estado fiscalizam o cumprimento do regulamento, podendo OFCOM notificar o provedor para permitir auditoria.

Na Índia, as *Information Technology Rules (IT Rules)* não contemplam disposições específicas voltadas à padronização dos relatórios de transparência, tampouco trata de aspectos relacionados à utilidade pública, verificabilidade das informações ou inteligibilidade dos dados divulgados.

Métricas e indicadores de desempenho para aferir a efetividade substantiva das medidas de governança, transparência e mitigação de riscos informacionais adotadas pelas plataformas digitais:

O dever de prestação de contas previsto no art. 9º-D da Resolução TSE n.º 23.610/2019 exige das plataformas digitais que veiculem conteúdo político-eleitoral a demonstração da eficácia concreta das medidas de mitigação de riscos informacionais. Contudo, a Resolução não oferece parâmetros objetivos nem estabelece indicadores específicos que possam ser utilizados para aferir a efetividade substantiva das medidas de governança, transparência e mitigação de riscos informacionais implementadas por essas plataformas.

No DSA, a efetividade das plataformas de grande dimensão (VLOPs e VLOSEs) é aferida por métricas detalhadas sobre seus sistemas de controle. Indicadores incluem moderação própria, uso de ferramentas automatizadas, precisão e taxas de erro dessas ferramentas. A transparência procedimental considera número de reclamações, decisões adotadas, notificações categorizadas e medidas subsequentes. A governança de riscos é avaliada por meio de avaliações anuais de riscos sistêmicos, incluindo efeitos sobre discurso cívico e processos eleitorais. Auditorias independentes anuais validam a eficácia das medidas, devendo relatórios negativos apresentar recomendações operacionais.

No Reino Unido, o OSA exige métricas que demonstrem gestão de riscos contínua, transformando a prestação de contas em processo ativo de supervisão. Indicador central é o registro escrito e contínuo de todas as avaliações de risco, mantido em linguagem clara e acessível. A efetividade é aferida pelo fornecimento desses registros e dos relatórios de medidas de segurança à OFCOM assim que criados ou revisados, garantindo supervisão em tempo real. Os indicadores incluem não apenas a incidência de conteúdos prejudiciais, mas também o impacto das medidas de segurança sobre liberdade de expressão e privacidade, demonstrando proporcionalidade. Para verificação, as plataformas devem manter trilhas de auditoria detalhadas, e o regulador pode exigir auditorias ou nomeação de especialistas para avaliar cumprimento das regras.

No modelo indiano, as *IT Rules* não exigem métricas complexas de mitigação de riscos, focando na aferição de conformidade por meio de relatórios mensais, especialmente para intermediários significativos. O indicador central é a periodicidade e detalhamento desses relatórios, que devem descrever reclamações recebidas e ações adotadas. A atuação proativa é medida pelo número de links ou informações removidos por ferramentas automatizadas.

Corregulação e adoção de medidas complementares de governança e transparência:

Embora a Res. TSE 23.610/2019 preveja dever de cooperação entre plataformas e Justiça Eleitoral, não estabelece mecanismos formais de corregulação. Ainda assim, foram celebrados memorandos de entendimento com provedores, orientando ações de enfrentamento à desinformação eleitoral nas Eleições de 2024. Por esses instrumentos, as plataformas comprometeram-se a adotar medidas céleres para conter informações falsas e cooperar com o TSE no âmbito do âmbito do Centro Integrado de Enfrentamento à Desinformação e Defesa da Democracia (CIEDDE).

Na União Europeia, o DSA estabelece um ecossistema de transparência complementado por corregulação, reforçando a efetividade das obrigações estatutárias. A Comissão Europeia incentiva códigos de conduta facultativos, como o Código de Conduta sobre Desinformação, que definem compromissos adicionais para enfrentar danos da desinformação, garantindo maior transparência, supervisão e responsabilidade. Para VLOPs e VLOSEs, a prestação de contas abrange não apenas as obrigações do regulamento, mas também compromissos assumidos em códigos de conduta e protocolos de crise.

No Reino Unido, o OSA integra medidas complementares diretamente ao cumprimento dos deveres estatutários. A OFCOM emite códigos de prática recomendando ações para observância dos deveres. Os provedores devem manter registros escritos das medidas adotadas, especialmente quando alinhadas a códigos de conduta considerados adequados. A OFCOM publica relatórios de transparência com resumos de conclusões, padrões, tendências e boas práticas da indústria, promovendo evolução contínua das medidas de governança e transparência para reforçar a efetividade.

Nas *IT Rules*, o Ministério coordena e incentiva a adesão ao Código de Ética por editores e organismos de autorregulação, além de desenvolver um Mecanismo de Supervisão. Entre suas atribuições está a publicação de uma carta de diretrizes aos organismos autorreguladores, acompanhada de códigos de prática aplicáveis à sua atuação.

29.6 EVIDÊNCIAS E ESTUDOS DE CASO

Structural indicators of the Code of Practice on Disinformation: the 2nd EDMO report: O relatório elaborado pelo Centro para o Pluralismo e a Liberdade da Mídia (CMPF) para o EDMO apresenta uma síntese do processo iterativo de desenvolvimento dos indicadores estruturais relativos ao Código de Práticas sobre Desinformação. O documento traz uma proposta aperfeiçoada desses indicadores, abordando, ainda, os desafios práticos relacionados à sua implementação (Nenadić et al., 2024).

Implementing the EU Code of Practice on Disinformation: an evaluation of VLOPSE compliance and effectiveness (jan-jun 2024): O relatório avalia a implementação do Código de Práticas sobre Desinformação (CoPD) no período de janeiro a junho de 2024, com foco nas ações reportadas pelas plataformas Meta (Facebook e Instagram), Google (Pesquisa e YouTube), Microsoft (Bing e LinkedIn) e TikTok (Botan; Meyer, 2025).

29.7 RECOMENDAÇÕES (NORMATIVAS E OPERACIONAIS)

Recomendações normativas:

Estabelecimento de *accountability* multinível e granular (intensidade proporcional):

Formalizar o princípio da proporcionalidade, estabelecendo obrigações escalonadas. Plataformas de grande porte devem estar sujeitas a exigências mais rigorosas, como a realização de avaliações de risco sistêmico focadas no processo eleitoral e a submissão a auditorias externas independentes.

Disciplinar a granularidade das obrigações de prestação de contas com base em parâmetros objetivos, como o número de usuários ativos no Brasil. As plataformas e mecanismos de busca de grande dimensão devem suportar deveres mais rigorosos, incluindo a submissão a auditorias independentes anuais e relatórios mais frequentes. Neste ponto, reconhece-se que a definição de parâmetros objetivos para a aplicação da referida granularidade requer amplo debate e discussão no âmbito da esfera normativa do Tribunal Superior Eleitoral.

Exigir que plataformas e mecanismos de busca de grande dimensão criem uma "função de conformidade" (compliance) destacada e independente internamente, cujo chefe preste contas diretamente ao órgão de administração, conforme o modelo do DAS.

Definição de conteúdo mínimo para avaliações de risco e relatórios de transparência:

O TSE, em diálogo com os provedores e a sociedade civil, poderia coordenar o desenvolvimento de modelos harmonizados para os relatórios de transparência, facilitando a análise comparativa e a supervisão, como previsto na estrutura de governança do Código de Conduta europeu.

A Resolução TSE n.º 23.610/2019 deve ser aprimorada para especificar o conteúdo, a periodicidade e o formato dos relatórios de transparência, inspirando-se no detalhamento do DSA e do Código de Conduta da UE. Deveria ser explicitada a exigência de dados quantitativos e qualitativos sobre moderação, precisão de sistemas automatizados, recursos humanos alocados e métricas de impacto das políticas.

Detalhamento dos parâmetros mínimos para a Avaliação de Impacto sobre a Integridade Eleitoral (Art. 9º-D, V), exigindo que cubram explicitamente a identificação e mitigação de riscos sistêmicos decorrentes dos serviços, incluindo os efeitos negativos reais ou previsíveis no discurso cívico e nos processos eleitorais.

Obrigação de que os relatórios incluam métricas específicas sobre o uso de ferramentas automatizadas para moderação, detalhando seus indicadores de precisão e taxas de erro.

Inclusão da exigência de avaliação do impacto das medidas de segurança sobre o direito à liberdade de expressão e a privacidade dos usuários antes da implementação de políticas de segurança, em linha com o OSA.

Vigência e Periodicidade Contínua das Obrigações:

A redação da Resolução deve deixar claro que o dever de prestação de contas do art. 9º-D, assim como outras obrigações de cuidado, se aplica de forma contínua.

Especificar o período de exigência, em ano eleitoral, da avaliação de impacto dos serviços dos provedores de aplicação de internet sobre a integridade do processo eleitoral, a fim de implementar medidas eficazes e proporcionais para mitigar os riscos identificados.

Estabelecer a obrigatoriedade de apresentação de relatórios de transparência anuais para todos os provedores e semestrais (ou mensais) para as plataformas de grande dimensão, garantindo fiscalização mais frequente e efetiva.

Ampliação do Dever de Transparência Institucional:

Obrigação de que o próprio Tribunal Superior Eleitoral (ou o órgão regulador responsável) publique relatórios de transparência anuais com base nas informações recebidas dos provedores. Esses relatórios devem incluir um resumo das conclusões, padrões, tendências identificadas e quaisquer medidas consideradas “boa prática da indústria”.

Empoderamento da comunidade de pesquisa e da sociedade civil:

Estabelecer um arcabouço normativo que garanta o acesso de pesquisadores e da sociedade civil a dados das plataformas para o estudo independente da desinformação, em linha com o DSA e o Código de Conduta.

Recomendações operacionais (mecanismos de execução e fiscalização)

Fortalecimento dos mecanismos de verificação externa:

Exigir a submissão a auditorias independentes anuais para as VLOPs e VLOSEs, a expensas próprias, como mecanismo de validação da efetividade substantiva das medidas de mitigação de riscos. Os relatórios de auditoria devem ser fundamentados e, em caso de não conformidade, incluir recomendações operacionais.

Implementar a supervisão direta e contínua, exigindo que as plataformas forneçam ao regulador (Justiça Eleitoral) cópias integrais dos registros de avaliações de risco assim que forem criados ou revisados.

Acesso a dados para pesquisadores e sociedade civil:

Estabelecer o dever de conceder acesso aos dados das plataformas (VLOPs/VLOSEs) a pesquisadores habilitados para investigações sobre riscos sistêmicos, sob condições que protejam a privacidade e os segredos de negócio.

Exigir a publicação de sínteses concisas, facilmente acessíveis e legíveis por máquina dos termos e condições.

Garantir a transparência direcionada ao usuário, impondo que, em caso de remoção de conteúdo, o provedor notifique o usuário com a exposição de motivos clara e específica e assegure a oportunidade razoável de contestar a decisão.

Formalização da corregulação e de códigos de prática:

Formalizar o incentivo à elaboração de códigos de conduta facultativos (corregulação), seguindo o modelo do DSA, onde a prestação de contas abrange o cumprimento de quaisquer compromissos complementares assumidos voluntariamente.

Exigir que os provedores mantenham registros escritos das medidas adotadas que estejam em consonância com os códigos de conduta ou códigos de prática regulatórios, demonstrando a incorporação de boas práticas da indústria.

Obrigar as plataformas a manterem trilhas de auditoria detalhadas sobre suas decisões e sistemas de segurança, facilitando a fiscalização ex post.

O TSE, em parceria com as plataformas digitais, deve viabilizar a criação de portais de transparência para solicitações de acesso a dados e detalhar nos relatórios como os resultados de pesquisas são incorporados em suas políticas.

Adoção de prestação de contas dinâmica:

As plataformas devem implementar sistemas de manutenção e atualização contínua de registros sobre avaliações de risco e medidas de mitigação, como no modelo do OSA. Esses registros devem estar à disposição da Justiça Eleitoral para permitir um acompanhamento tempestivo e efetivo, não apenas reativo.

Capacitação de verificadores de fatos:

Formalizar parcerias institucionais com entidades especializadas, assegurar acesso estruturado a ferramentas, bases de dados e mecanismos de checagem, bem como publicar métricas periódicas sobre o alcance, a eficácia e o impacto das verificações no ecossistema informacional.

Adequação Tecnológica e Algorítmica:

Efetuar a adaptação do serviço, incluindo a conceção (design), elementos ou funcionamento das interfaces online.

Realizar o teste e adaptação de sistemas algorítmicos (incluindo sistemas de recomendação) e correção de critérios, a fim de mitigar a difusão de conteúdos desinformativos.

Plataformas de grande alcance ou dimensão devem se esforçar para implantar medidas baseadas em tecnologia, incluindo ferramentas automatizadas ou outros mecanismos, para identificar proativamente conteúdos relacionados à integridade eleitoral.

29.8 RISCOS, SALVAGUARDAS E DIREITOS

Riscos: Embora os deveres de prestação de contas se concentrem em medidas de mitigação de riscos, como os que afetam a segurança pública ou os processos eleitorais, a própria exigência de *accountability* evidencia riscos internos das plataformas, especialmente relacionados à parcialidade ou a práticas de *"washing"* que mascaram o cumprimento das obrigações regulatórias. Assim, a prestação de contas monitora a atuação das plataformas e atua como instrumento de detecção e prevenção de falhas estruturais e comportamentais no ambiente digital.

Salvaguardas: Nesse contexto, plataformas de grande dimensão devem submeter-se a auditorias independentes, cujos relatórios fundamentem eventuais não conformidades e incluam recomendações operacionais precisas. Para garantir a veracidade das informações, os auditores devem ter acesso pleno a serviços e dados relevantes. Plataformas de grande dimensão devem instituir função de conformidade destacada e independente, com o chefe de conformidade reportando diretamente ao órgão de administração, podendo alertar sobre riscos ou descumprimentos, sem possibilidade de remoção sem aprovação do órgão.

Direitos: Os provedores devem assegurar que verificadores de fatos tenham acesso rápido e, quando possível, automatizado às informações relevantes, formalizar parcerias estruturadas com canais de comunicação estáveis e garantir remuneração justa, promovendo transparência, responsabilização e eficácia na mitigação de conteúdos desinformativos.

REFERÊNCIAS

BIONI, Bruno Ricardo. Regulação e proteção de dados pessoais: o princípio da *accountability*. Rio de Janeiro: Forense, 2022.

BOTAN, Madalina; MEYER, Trisha (Coords.). Implementing the EU Code of Practice on Disinformation: an evaluation of VLOPSE compliance and effectiveness (jan-jun 2024). European Digital Media Observatory, 2025. Disponível em: https://edmo.eu/wp-content/uploads/2025/06/EDMO-Report-%E2%80%93-Implementing-the-EU-Code-of-Practice-on-Disinformation.pdf. Acesso em: 12 dez. 2025.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei nº 9.504, de 30 de setembro de 1997. Dispõe sobre normas para as eleições. Brasília, DF: Presidência da República, 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 11 dez. 2025.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 2019. Dispõe sobre propaganda eleitoral. Brasília, DF, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 10 dez. 2025

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 2024. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Brasília, DF, 2024. Disponível

em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 10 dez. 2025.

BRASIL. Supremo Tribunal Federal. Informação à sociedade: RE 1.037.396 (Tema 987) e 1.057.258 (Tema 533) responsabilidade de plataformas digitais por conteúdo de terceiros. Brasília: STF, 2025. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/Informac807a771oa768SociedadeArt19MCI_vRev.pdf. Acesso em: 10 dez. 2025.

COMISSÃO EUROPEIA. The strengthened code of practice on disinformation 2022. [S. l.]: Comissão Europeia, 2022. Disponível em: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation. Acesso em: 10 dez. 2025.

COMISSÃO EUROPEIA. Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065. Official Journal of the European Union, [S. l.], 2024. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403014. Acesso em: 10 dez. 2025.

ÍNDIA. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Índia: Ministry of Electronics and Information Technology, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Acesso em: 10 dez. 2025.

LABORATÓRIO de Estudos de Internet e Redes Sociais (NetLab). Faturar um milhão é fácil: publicidade política no TikTok e o desequilíbrio da disputa eleitoral em 2024. Rio de Janeiro, 2025. Disponível em: https://netlab.eco.ufrj.br/post/faturar-um-milhao. Acesso em: 12 dez. 2025.

NENADIĆ, Iva; BROGI, Elda; BLEYERSIMON, Konrad; REVIGLIO, Urbano. Structural indicators of the Code of Practice on Disinformation: the 2nd EDMO report. European Digital Media Observatory, 2024. Disponível em: https://edmo.eu/wp-content/uploads/2024/03/SIs_-2nd-EDMO-report.pdf. Acesso em: 12 dez. 2025.

REINO UNIDO. Online Safety Act (OSA). Londres, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Bruxelas, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2024/900 do Parlamento Europeu e do Conselho de 13 de março de 2024 sobre a transparência e o direcionamento da propaganda política. União Europeia, 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202400900. Acesso em: 11 dez.

2.10 PROTEÇÃO DE DADOS (ART. 33-A, *CAPUT*; ART. 33-B)

Tayná Frota

Art. 33-A. Os provedores de aplicação deverão informar expressamente às usuárias e aos usuários sobre a possibilidade de tratamento de seus dados pessoais para a veiculação de propaganda eleitoral no âmbito e nos limites técnicos de cada provedor, caso admitam essa forma de propaganda.
[...]
Art. 33-B. Cabe aos provedores de aplicação, aos partidos políticos, às federações, às coligações, às candidatas ou aos candidatos, quando realizarem tratamento de dados pessoais para fins de propaganda eleitoral:
I - garantir o acesso facilitado às informações sobre o tratamento de dados, previsto no art. 9º da Lei n.º 13.709/2018, em especial quanto aos dados utilizados para realizar perfilamento de usuárias e usuários com vistas ao microdirecionamento da propaganda eleitoral;
II - garantir o cumprimento dos direitos previstos nos arts. 17 a 20 da Lei n.º 13.709/2018;
III - adotar as medidas necessárias para a proteção contra a discriminação ilícita e abusiva, nos termos do inciso IX do art. 6º da Lei n.º 13.709/2018;
IV - usar os dados exclusivamente para as finalidades explicitadas e consentidas pela pessoa titular, respeitando os princípios da finalidade, da necessidade e da adequação;
V - implementar medidas de segurança técnica e administrativa para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas que possam levar à destruição, perda, alteração, comunicação ou difusão dos dados, nos termos do art. 46 da Lei n.º 13.709/2018;
VI - notificar, em caso de incidentes de segurança que possam acarretar riscos ou danos relevantes às(aos) titulares dos dados, a autoridade nacional e às(aos) titulares afetadas(os), nos termos do art. 48 da Lei n.º 13.709/2018.
§ 1º Na propaganda eleitoral, o tratamento de dados pessoais sensíveis ou de dados pessoais que possam revelar dados pessoais sensíveis exige, além do disposto nos incisos do caput deste artigo, o consentimento específico, expresso e destacado do titular.
§ 2º No caso de dados pessoais sensíveis a que a candidata ou o candidato tenha acesso pessoalmente em decorrência de seu núcleo familiar, de suas relações sociais e de seus vínculos comunitários, como a participação em grupos religiosos, associações e movimentos, o consentimento específico, expresso e destacado de que trata o § 1º deste artigo somente será exigido para a transferência a terceiros, respondendo o cedente por divulgação ou vazamento.
§ 3º É dever de partidos políticos, federações, coligações, candidatas e candidatos exigir e fiscalizar o cumprimento do disposto neste artigo pelas pessoas e empresas contratadas por suas campanhas.
§ 4º O descumprimento do disposto neste artigo e no § 1º do art. 31 desta Resolução acarretará a remoção do conteúdo veiculado e a comunicação do fato à Autoridade Nacional da Proteção de Dados, a quem compete avaliar a aplicação das sanções previstas no art. 52 da Lei n.º 13.702/2018, sem prejuízo da eventual apuração de ilícitos eleitorais ou crimes.

2.10.1 VISÃO GERAL E OBJETIVOS

Objetivo: os arts. 33-A, *caput* e 33-B, introduzidos na Resolução TSE n. 23.732/2024, estabelecem obrigações específicas à proteção de dados pessoais direcionados aos atores político-partidários. Os artigos estabelecem deveres específicos de transparência, segurança e governança de dados pessoais aplicáveis a plataformas digitais, partidos políticos, federações, coligações e candidaturas que realizem tratamento de dados para fins de propaganda eleitoral (Brasil, 2024).

Esses dispositivos visam alinhar a prática de microdirecionamento político e o uso de dados em campanhas às garantias constitucionais de privacidade, autodeterminação informativa e igualdade de tratamento, harmonizando a legislação eleitoral com a Lei Geral de Proteção de Dados (Brasil, 2018).

Em síntese, os artigos buscam evitar o uso abusivo de dados pessoais e sensíveis na propaganda eleitoral, assegurar consentimento livre e informado e prevenir discriminação ou manipulação informacional de eleitores.

Guia de perguntas:

- O ordenamento jurídico exige que plataformas informem claramente aos usuários sobre o tratamento de dados pessoais para fins de propaganda eleitoral ou política?
- Em caso de notificação, esta deve ser prévia (antes da coleta/tratamento) ou pode ocorrer no momento da exibição da propaganda?
- Há exigência de repositório público de anúncios políticos?
- Há indicação de quais bases legais (ou demais requisitos legais) são aplicáveis para o tratamento de dados para este objetivo?
- Há obrigação de informar o uso de perfilamento e microdirecionamento (targeted ads) com base em dados pessoais?

2.10.2 BASE NORMATIVA (BRASIL)

TSE Res. n. 23.732/2024 (art. 33-A, *caput*; art. 33-B): A notificação quanto à possibilidade de tratamento de dados para fins de propaganda deve ser prévia – antes da coleta/tratamento, conforme princípios (art. 6º) e direitos da LGPD, como o direito ao acesso facilitado às informações sobre o tratamento de seus dados (art. 9º). O Brasil não possui previsão expressa para repositório público de anúncios políticos, e a efetivação da transparência depende de fiscalização eleitoral e identificação na postagem. Além da aplicação das disposições da LGPD, exige-se o consentimento específico e destacado para o tratamento de dados pessoais sensíveis (art. 33-B, §1º). O art. 33-B, I impõe dever de informar sobre dados usados em perfilamento, mas não há especificação sobre os dados que devem ser utilizados.

2.10.3 METODOLOGIA DE *BENCHMARKING*

Seleção de jurisdições: UE (GDPR, DSA, Regulamento 2024/900), Reino Unido (UK GDPR, ICO Guidance, OSA) e Índia (*IT Rules*/2021 e alterações)

Unidades de comparação: os critérios derivam dos artigos ora analisados e estão organizados em quatro eixos:

Transparência e informação prévia ao usuário: identificar se dever de aviso prévio e destacado nas políticas de privacidade ou nos próprios anúncios e se há sanções para a ausência dessa transparência.

Identificação pública e rastreabilidade de propagandas políticas: analisar se há obrigação legal de manter um repositório público ou biblioteca de anúncios políticos, identificando quem financiou, os critérios de segmentação e os dados pessoais usados.

Base legal e limites para o tratamento de dados pessoais: avaliar se há definição de bases legais válidas para o tratamento de dados destinados à propaganda eleitoral e se há vedações expressas ao uso de dados pessoais sensíveis.

Perfilamento e microdirecionamento: verificar se há obrigação de informar e permitir controle sobre o uso de perfilamento e microdirecionamento de anúncios com base em dados pessoais.

Critério	União Europeia (GDPR, DSA, Regulamento 2024/900)	Reino Unido (UK GDPR, ICO Guidance, OSA	Índia (*IT Rules* 2021)
Transparência e informação prévia ao usuário	A UE exige que anúncios políticos sejam claramente identificados como tais e que contenham "transparency notice" com patrocinador, eleição, montante, uso de técnicas de segmentação.	A ICO indica que, para propaganda política, o uso de dados pessoais para segmentação exige cumprimento dos princípios do UK GDPR.	As *IT Rules* exigem que "significant social media intermediaries" publiquem relatórios mensais incluindo detalhes das reclamações e ações tomadas ("compliance reports"), o que implica em obrigação de transparência sobre operações da plataforma.
Identificação pública e rastreabilidade de propagandas políticas	A regulamentação 2024/900 estipula que os anúncios políticos "must be clearly labelled as such" e que todos os anúncios online estarão "available in an online European repository".	No Reino Unido, embora exista orientação da ICO, não há atualmente obrigação geral de repositório público específico para todos anúncios políticos sob o UK GDPR nesta guia. A orientação trata de processamento de dados de campanha política.	As *IT Rules* 2021 exigem relatórios mensais de intermediários, e mecanismos de rastreio do "first originator" da informação em mensagens, mas não especificam claramente um "repositório público de anúncios políticos".

Base legal e limites para o tratamento de dados pessoais	A regulamentação 2024/900 exige que o uso de dados para anúncios políticos só seja possível após o dado ter sido recolhido junto ao titular e com seu consentimento separado; e que categorias especiais de dados (opinião política, origem étnica) não possam ser usadas para perfilamento.	A ICO destaca que o direito de objeção sob o UK GDPR (art. 21) aplica-se ao perfilamento para marketing e que decisões exclusivamente automatizadas com efeitos legais ou semelhantes (art. 22) requerem consentimiento explícito.	As *IT Rules* não contêm um arcabouço tão detalhado quanto a UE para tratamento de dados especificamente para propaganda política (em especial no que toca bases legais e perfilamento).
Perfilamento e microdirecionamento	A regulamentação proíbe perfilamento para anúncios políticos com base em categorias de dados sensíveis (como opinião política, origem étnica) ou menores de idade.	A ICO orienta que "profiling and micro-targeting" podem ocorrer, mas se forem "solely automated decisions" com efeitos legais ou semelhantes, estão sujeitas ao art. 22 e requerem consentimento explícito.	As *IT Rules* não contêm disposições específicas de perfilamento político ou microdirecionamento com dados pessoais no nível de detalhe da UE/UK para propaganda eleitoral. A ênfase está mais em intermediários, rastreamento da origem da informação, e relatórios de conformidade.

2.10.4 *BENCHMARK* INTERNACIONAL (SÍNTESE COMPARATIVA)

União Europeia:

O DSA (Art. 26 e 39) exige transparência de anúncios políticos e identificação da base de dados utilizada, mas não traz obrigação específica para o contexto eleitoral.

O GDPR (Arts. 13–14) exige transparência antes ou durante a exibição, com ênfase em clareza e contexto de uso das informações. Além disso, há obrigação de informação prévia e clara sobre o tratamento de dados pessoais.

O DSA (Art. 39) exige repositório público obrigatório de anúncios políticos.

GDPR (Art. 6 e 9): base legal pode ser consentimento explícito ou interesse público legítimo, conforme o caso.

O DSA (Art. 26) exige transparência em anúncios baseados em targeting; GDPR também regula decisões automatizadas (Art. 22).

GDPR (Arts. 12–22) assegura todos esses direitos, incluindo oposição ao profiling político. O art. 18º do Regulamento UE 2024/900, indica a proibição, em geral, do uso de dados sensíveis para perfilamento e microdirecionamento de propaganda política, mesmo se há consentimento explícito dos titulares.

Reino Unido:

Há dever de transparência e aviso claro sobre uso de dados para publicidade política. *ICO Guidance* reforça necessidade de informar finalidade e base legal.

***Data Protection Act* e UK GDPR** seguem modelo idêntico ao europeu, exigindo informação prévia e clara sobre o tratamento de dados.

A *Electoral Commission* orienta que plataformas mantenham bibliotecas de anúncios políticos (ex.: *Meta Ad Library*).

UK GDPR segue o mesmo regime de bases legais; uso para propaganda política normalmente exige consentimento explícito. ICO exige transparência em profiling e advertência clara sobre uso de dados pessoais em segmentação.

Índia:

IT Rules impõem dever de informação genérica; o DPDP Act exige aviso e consentimento para coleta e uso de dados pessoais, mas não há regra específica eleitoral.

A informação sobre o tratamento de dados deve ser prévia - DPDP Act Sec. 5(1).
Não há exigência legal de repositório público. A *Election Comission of India* (ECI) tem papel para fiscalizar a transparência.

DPDP *Act* exige consentimento prévio e informado (Sec. 6), com base no princípio da finalidade.

DPDP *Act* reconhece o direito à informação, mas não define obrigações específicas sobre microtargeting eleitoral.

2.10.5 INTERPRETAÇÃO DOS ARTS. 33-A E 33-B

A comunicação sobre o tratamento de seus dados pessoais para veiculação de propaganda eleitoral, que deve ser prévia, não pode ocorrer apenas no momento da exibição do anúncio, mas deve constar das políticas e telas de consentimento do serviço.

O dever de identificação não é apenas gráfico (rótulo “propaganda eleitoral”), mas também informacional, de modo que as plataformas devem manter rastreabilidade e dados de transparência ativa. Quando tecnicamente possível, registrada em repositório público de anúncios com informações sobre patrocinador, valores e critérios de exibição. A respeito, entende-se como pertinente a realização de consultas pública e outros meios para subsidiar a atuação do TSE e definição de limites técnicos objetivos.

É válido ao TSE interpretar o art. 33-B com exigência de consentimento expresso obrigatório, além da vedação de uso de dados sensíveis para segmentação política? Como conciliar com a hipótese do art. 33-B, §2º da Resolução? Como a ANPD pode atuar neste caso? Existem exceções legalmente justificadas?

A respeito do perfilamento e microdirecionamento, o usuário deve saber por que recebe determinado conteúdo político e poder optar por não participar de segmentações automatizadas. Existem circunstâncias em que o microdirecionamento deve ser vedado?

2.10.6 EVIDÊNCIAS E ESTUDOS DE CASOS

O Guia Orientativo da ANPD-TSE, referente à aplicação da LGPD por agentes de tratamento no contexto eleitoral, e anterior à Resolução, apresenta exemplos que podem orientar a utilização de dados pessoais, inclusive para perfilamento. No exemplo de impulsionamento de conteúdo, destaca-se a necessidade de: identificar a base legal aplicável, garantir transparência do tratamento, e cautela quanto ao uso de perfil comportamental (como em casos em que é exigível o direito de revisão).

2.10.7 RECOMENDAÇÕES (NORMATIVAS E OPERACIONAIS)

- Necessária articulação com ANPD para revisão, no que couber, das normas e condições para o tratamento de dados pessoais no contexto eleitoral.
- Exigência de aviso de transparência eleitoral, com seção específica e em destaque nas políticas.
- Exigência de relatórios públicos de anúncios, conforme o modelo europeu (DSA Art. 39), e adaptáveis conforme o tamanho dos agentes que realizam tratamento no contexto eleitoral.

2.10.8 RISCOS, SALVAGUARDAS E DIREITOS

Riscos	Descrição	Exemplos	Consequências
Risco de tratamento indevido de dados pessoais	Coleta, uso ou compartilhamento de dados no contexto eleitoral sem base legal válida ou sem consentimento livre e informado.	Captação de preferências políticas a partir de interações em redes sociais para microdirecionamento.	Violação de direitos fundamentais à privacidade e à autodeterminação informativa; sanções da LGPD e do TSE.
Risco de discriminação e manipulação informacional	Segmentação de eleitores com base em dados sensíveis (opinião política, origem étnica, religião) para influenciar comportamento eleitoral.	Campanhas direcionadas a grupos específicos por crença ou condição socioeconômica.	Manipulação de eleitores, desigualdade de tratamento e violação da isonomia eleitoral.
Risco de falta de transparência	Ausência de informações claras sobre quem trata os dados, para quais finalidades e com quais critérios de perfilamento.	Propagandas sem rótulo "anúncio político" ou sem indicação do patrocinador e da base de dados utilizada.	Redução da confiança pública e comprometimento da integridade eleitoral.

Risco de decisões automatizadas sem revisão humana	Uso de algoritmos de segmentação ou impulsionamento que afetam direitos dos titulares sem possibilidade de revisão.	Sistemas que selecionam automaticamente quem verá determinado conteúdo político.	Violação à LGPD (art. 20).
Risco de vazamento ou reidentificação	Falhas de segurança ou compartilhamento indevido com terceiros, inclusive fora do país.	Exposição de bases de dados de apoiadores ou de perfis de engajamento.	Responsabilização administrativa e judicial.
Risco de insegurança jurídica	Falta de coordenação entre TSE, ANPD e plataformas quanto aos limites e exceções aplicáveis.	Divergência de interpretações sobre consentimento obrigatório ou condições legítimas para o uso de dados.	Incerteza regulatória e aumento de litígios.

Salvaguardas

Consentimento informado e destacado

O titular deve compreender claramente a finalidade, os tipos de dados tratados e a possibilidade de revogar o consentimento a qualquer momento. Base normativa: LGPD (arts. 7º e 9º); Res. TSE 23.732/2024, art. 33-B, §1º.

Transparência ativa e acesso público

As plataformas e candidaturas devem disponibilizar repositórios públicos de anúncios políticos com informações sobre patrocinador, valores, critérios de segmentação e dados utilizados. A notificação sobre o tratamento de dados deve ocorrer antes da coleta e constar das políticas de privacidade. Base normativa: GDPR (arts. 13-14); Regulamento (UE) 2024/900, art. 18; Res. TSE 23.732/2024, art. 33-A.

Limitação de finalidade e uso proporcional

Os dados coletados para fins eleitorais não podem ser reutilizados para outros propósitos, como marketing comercial ou segmentação permanente de eleitores. O uso deve restringir-se ao período e à finalidade eleitoral declarada. Base normativa: LGPD (art. 6º, I e II); Regulamento (UE) 2024/900, art. 18.

Revisão humana e direito de oposição

Os eleitores têm direito de se opor ao uso de seus dados para perfilamento político e de exigir revisão de decisões automatizadas. As plataformas devem assegurar canais simples para revisão humana e correção de possíveis vieses algorítmicos. Base normativa: LGPD (arts. 18, §1º e 20); UK GDPR, art. 22.

Segurança da informação e retenção limitada

TSE e ANPD devem atuar quanto à definição de período de retenção dos dados após o término da finalidade eleitoral. Base normativa: LGPD (arts. 46-48); DSA, art. 35(3).

Cooperação institucional e fiscalização integrada

É necessária coordenação contínua entre o TSE, a ANPD e os agentes de tratamento para monitorar e corrigir eventuais abusos no uso de dados eleitorais. Devem ser instituídos protocolos de resposta rápida e relatórios conjuntos de conformidade. Base normativa: Res. TSE 23.732/2024, art. 33-B, §2º; Guia ANPD-TSE (2024).

Direitos

Transparência e acesso à informação

O titular possui direito de ser informado, de forma clara e prévia, sobre o tratamento de seus dados pessoais para fins de propaganda política ou eleitoral; saber quem é o controlador, quais dados são utilizados, para qual finalidade e com base em qual fundamento legal; acessar repositórios públicos de anúncios políticos e relatórios de transparência que indiquem patrocinadores, valores e critérios de segmentação.

Objetivo: garantir que o eleitor compreenda como e por que está sendo impactado por determinada comunicação política, fortalecendo a confiança no processo democrático.

Controle e autodeterminação informativa

O titular possui o direito de consentir ou se opor ao uso de seus dados, podendo revogar o consentimento a qualquer momento; solicitar correção, atualização, anonimização ou eliminação de informações pessoais utilizadas em campanhas.

Objetivo: assegurar que o titular mantenha controle efetivo sobre seus próprios dados e sobre o modo como eles influenciam sua experiência digital durante o pleito.

Proteção contra decisões automatizadas e abusos

O titular possui o direito de não ser submetido a decisões automatizadas (como perfilamento ou microdirecionamento) que afetem seus direitos políticos sem revisão humana; solicitar explicações sobre a lógica envolvida em sistemas de recomendação ou segmentação de anúncios eleitorais; e à intervenção humana e à revisão de resultados decorrentes de processamento automatizado.

Objetivo: evitar discriminação algorítmica, manipulação informacional e usos abusivos de dados sensíveis (como opinião política ou religião).

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 dez. 2025.

BRASIL. Tribunal Superior Eleitoral. Autoridade Nacional de Proteção de Dados. Guia orientativo: apli-

cação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral. Brasília, DF, 2021. Disponível em: https://www.tse.jus.br/institucional/catalogo-de-publicacoes/arquivos/guia-orientativo-aplicacao-da-lgpd/@@display-file/file/guia-orientativo-aplicacao-da-lgpd.pdf. Acesso em: 12 dez. 2025.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 2019. Dispõe sobre propaganda eleitoral. Brasília, DF, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 10 dez. 2025

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 2024. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Brasília, DF, 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 10 dez. 2025.

ÍNDIA. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Índia: Ministry of Electronics and Information Technology, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Acesso em: 10 dez. 2025.

MANORAMA YEARBOOK. Govt seeks compliance report from large social media companies. 2025. Disponível em: https://www.manoramayearbook.in/current-affairs/india/2021/05/27/govt-seeks-compliance-report-from-large-social-media-companies.html. Acesso em: 12 dez. 2025.

REINO UNIDO. Online Safety Act (OSA). Londres, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 10 dez. 2025.

REINO UNIDO. Online Safety Act: explainer. Londres: Gov.uk, [2025?]. Disponível em: https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer. Acesso em: 10 dez. 2025.

REINO UNIDO. Information Commissioner's Office. Guidance for the use of personal data in political campaigning. [Londres]: Information Commissioner's Office, [202-?]. Disponível em: https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-for-the-use-of-personal-data-in-political-campaigning-1/. Acesso em: 12 dez. 2025.

UNIÃO EUROPEIA. Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Bruxelas, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIRA. Conselho da União Europeia. EU introduces new rules on transparency and targeting of political advertising. União Europeia, 2024. Disponível em: https://www.consilium.europa.eu/en/press/press-releases/2024/03/11/eu-introduces-new-rules-on-transparency-and-targeting-of-political-advertising/pdf. Acesso em: 12 dez. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2024/900 do Parlamento Europeu e do Conselho de 13 de março de 2024 sobre a transparência e o direcionamento da propaganda política. União Europeia, 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202400900. Acesso em: 11 dez. 2025.

2.11 REMOÇÃO DE CONTEÚDO (ART. 9º-B, § 4º)

Bárbara Pontalti e Marina Lucena

Art. 9º-B. A utilização na propaganda eleitoral, em qualquer modalidade, de conteúdo sintético multimídia gerado por meio de inteligência artificial para criar, substituir, omitir, mesclar ou alterar a velocidade ou sobrepor imagens ou sons impõe ao responsável pela propaganda o dever de informar, de modo explícito, destacado e acessível que o conteúdo foi fabricado ou manipulado e a tecnologia utilizada.
[...]
§ 4º O descumprimento das regras previstas no caput e no § 3º deste artigo impõe a imediata remoção do conteúdo ou indisponibilidade do serviço de comunicação, por iniciativa do provedor de aplicação ou determinação judicial, sem prejuízo de apuração nos termos do § 2º do art. 9º-C desta Resolução.

21.1.1 VISÃO GERAL E OBJETIVOS

Objetivo: analisar o alcance e os efeitos do art. 9º-B, §4º, da Resolução TSE n.º 23.732/2024, que prevê a remoção imediata de conteúdos eleitorais sintéticos multimídia manipulados por inteligência artificial quando não houver a devida informação ao eleitor sobre sua natureza artificial. Busca-se compreender em que medida o dispositivo representa uma mudança de paradigma na responsabilidade das plataformas, ao romper com a lógica de neutralidade do art. 19 do Marco Civil da Internet e adotar um modelo de atuação proativa e resposta célere a riscos eleitorais (Brasil 2014, 2024).

Guia de Perguntas:

- Qual é o conteúdo e alcance normativo do §4º do art. 9º-B da Resolução TSE n.º 23.732/2024?
- Como esse dispositivo se insere no contexto jurídico brasileiro e no marco regulatório da internet?
- O que caracteriza, juridicamente, uma "remoção imediata"?
- Quais aprimoramentos poderiam ser sugeridos à norma brasileira, com base no direito comparado e nas boas práticas internacionais?
- Como tem sido a aplicação prática da norma pelo TSE e pelos tribunais regionais eleitorais?

21.1.2 BASE NORMATIVA (BRASIL)

TSE Res. 23.610, Art. 9º-B, §4º – O § 4º do art. 9º-B da Resolução TSE n.º 23.610/2019 estabelece que a veiculação de propaganda eleitoral contendo conteúdo sintético multimídia gerado por inteligência artificial (IA), sem a devida informação explícita ao eleitor de que se trata de conteúdo manipulado, bem como da tecnologia utilizada, ou que simule interlocução com pessoa candidata, enseja a remoção imediata do conteúdo. Essa remoção pode ocorrer de duas formas: por iniciativa do próprio provedor de aplicação ou mediante determinação judicial, conforme previsto na norma.

Contexto regulatório adjacente:

O contexto normativo brasileiro já fornece bases sólidas para a compreensão do dever de remoção imediata e para a consolidação de uma responsabilidade ativa das plataformas digitais em contextos eleitorais.

O ponto de partida é o art. 170 da Constituição Federal, que consagra a função social da atividade econômica. A atuação das plataformas digitais, como agentes que mediam fluxos informacionais e participam diretamente da formação da opinião pública, deve observar essa função social e não pode ser dissociada da proteção da coletividade.

O regime de responsabilidade civil dos provedores de aplicação na internet, tal como previsto no art. 19 do Marco Civil da Internet (MCI), foi substancialmente alterado pelo julgamento conjunto dos Recursos Extraordinários n.º 1.037.396 e n.º 1.057.258 pelo Supremo Tribunal Federal (STF), que declarou a inconstitucionalidade parcial do dispositivo.

O art. 19 do Marco Civil da Internet originalmente previa a responsabilização dos provedores apenas mediante ordem judicial, configurando um modelo de neutralidade passiva. Contudo, o STF entendeu que essa limitação não garante a proteção adequada dos direitos fundamentais nem da ordem democrática em casos de conteúdos manifestamente ilícitos. Assim, reconheceu-se a legitimidade de exigir um dever de cuidado reforçado das plataformas, incluindo a remoção imediata de conteúdos sem decisão judicial e a responsabilização pela inércia diante da ilicitude conhecida. Dessa forma, o art. 19 é hoje considerado parcialmente inconstitucional e deve ser interpretado conforme os parâmetros definidos pelo STF.

Além disso, o art. 11 do Marco Civil da Internet assegura a aplicação da legislação brasileira a serviços estrangeiros, conferindo alcance transfronteiriço às ordens de remoção - entendimento consolidado pelo STJ no REsp n.º 2.147.711, relatado pela Ministra Nancy Andrighi, que reconheceu a eficácia global das decisões judiciais de indisponibilidade de conteúdo, dada a natureza descentralizada e o alcance transnacional da internet.

Retornando ao texto da Resolução n.º 23.732/2024, o §4º do art. 9º-B remete ao §2º do art. 9º-C, estabelecendo que a apuração das responsabilidades pelo descumprimento será conduzida conforme os parâmetros da legislação eleitoral, inclusive com a possibilidade de cassação de registro ou de mandato quando configurado abuso de poder político ou uso indevido dos meios de comunicação.

Entretanto, sua eficácia prática depende de uma leitura integrada ao sistema mais amplo de responsabilidade das plataformas, que envolve o debate sobre a responsabilização dos intermediários e os desafios técnicos da moderação automatizada.

2.11.3 METODOLOGIA DE *BENCHMARKING*

Seleção de jurisdições: UE (DSA), Reino Unido (OSA), Índia (*IT Rules*).

Unidades de comparação (possíveis critérios):

Dever de diligência e atuação proativa: medidas exigidas das plataformas para identificar e suprimir conteúdos ilícitos ou manipulados, inclusive antes de ordem judicial, e desenvolver padrões de prevenção de danos informacionais.

Fundamentação e transparência das decisões de remoção: dever de justificar e comunicar de forma clara os motivos da exclusão ou bloqueio de conteúdo, assegurando previsibilidade, direito de defesa e equilíbrio entre integridade informacional e liberdade de expressão.

Mitigação de riscos sistêmicos: dever de identificar, avaliar e reduzir riscos relacionados à desinformação, manipulação de conteúdo e interferência nos processos democráticos.

Prazos e procedimentos de remoção: existência de prazos máximos, etapas procedimentais e requisitos de eficácia e proporcionalidade na execução das medidas de *takedown e notice and action.*

Governança e fiscalização: mecanismos institucionais de supervisão e auditoria sobre as práticas de moderação de conteúdo, incluindo obrigações de transparência, relatórios públicos, auditorias independentes e monitoramento por autoridades competentes. Avalia também o grau de *accountability* das plataformas e a existência de sanções ou incentivos regulatórios para assegurar o cumprimento efetivo dos deveres de remoção.

Critério	União Europeia - *Digital Service Act* (DSA)	Reino Unido - *Online Safety Act* (OSA)	Índia – *IT Rules*
Dever de diligência e atuação proativa	Considerando 2: explicita sobre os requisitos de atuação diligente dos prestadores de serviços intermediários sobre conteúdos ilegais, desinformação e outros riscos sociais. Considerando 22: estabelece que, para que o prestador mantenha a isenção de responsabilidade, deve atuar com diligência na remoção ou bloqueio de conteúdos ilegais, seja a partir de notificação de terceiros ou por iniciativa própria, quando tiver conhecimento da ilicitude. Nesse mesmo sentido, o artigo 6º consagra que a responsabilidade do prestador quanto às informações armazenadas a pedido do usuário somente se configura após o conhecimento efetivo da ilegalidade. A partir desse momento, impõe-se o dever de agir de forma célere e diligente para suprimir ou restringir o acesso ao conteúdo ilícito, tornando a isenção de responsabilidade condicional ao cumprimento desse dever de atuação imediata. Considerando 40: menciona que um ambiente em linha seguro e transparente necessita de um conjunto claro, eficaz, previsível e equilibrado de obrigações de devida diligência dos prestadores. Art. 7: Autoriza medidas proativas de moderação sem perda da isenção de responsabilidade. Reforça o dever de prevenção e atuação de boa-fé, inclusive com o uso de ferramentas automatizadas. Art. 9: operacionaliza o dever de agir quando houver decisão judicial ou administrativa, mas, interpretado em conjunto com os considerandos anteriores, reforça o caráter de resposta célere e responsável.	Já na introdução, o OSA adota o princípio do safe by design, exigindo que os serviços sejam projetados e operados de modo a reduzir riscos antes que ocorram. Também nessa parte inicial, são impostas avaliações periódicas de risco sobre conteúdos ilegais, levando em conta a probabilidade de exposição, o impacto do modelo de negócio e a estrutura de governança interna. A Seção 1 estabelece deveres de transparência e accountability, impondo que provedores ajam de modo aberto, responsável e mensurável. É a base normativa do dever de diligência. A Seção 2 impõe obrigações específicas às plataformas que permitem interação entre usuários, prevenindo a circulação de conteúdos ilegais. Expressa a exigência de atuação proativa. A Seção 10 concretiza o dever de diligência ao exigir medidas proporcionais para evitar que usuários encontrem conteúdo ilegal, representando o núcleo do proactive duty.	A Parte 2 define informações sobre a diligência devida dos intermediários e reparação das reclamações Rule 3: consolida o núcleo do dever de diligência, ao exigir que intermediários cumpram padrões de transparência, informem usuários suas regras de uso e utilizem-se de esforços razoáveis para que estes não publiquem informações de diversos tipos, incluindo: (v) desinformação ou conteúdo incorreto, inverídico ou falso, ou verificada como falsa pelo Governo; (vii) ameaças à integridade da segurança e soberania da Índia ou, de modo geral; (xi) que violem a lei. Rule 4: determina que os intermediários devem empregar ferramentas tecnológicas para identificar proativamente conteúdo de estupro, abuso sexual infantil ou idêntico a material previamente removido.

Fundamentação e transparência das decisões de remoção	Art. 17: Os prestadores de serviços devem apresentar uma exposição de motivos clara e específica a todos os destinatários do serviço afetados relativamente a qualquer restrição imposta. Essas restrições incluem: supressão de conteúdos, desativação do acesso a conteúdos ou despromoção de conteúdos. Ainda, deve-se incluir, se alegadamente ilegal, uma referência ao fundamento jurídico invocado.	Seção 71: estabelece que a moderação de conteúdo deve ocorrer nos limites dos termos de serviço previamente definidos pelas plataformas. Excepcionalmente, admite-se a remoção ou restrição de conteúdo fora desses termos quando tal medida for necessária para: (i) cumprir deveres legais de proteção contra conteúdos ilícitos ou prejudiciais a crianças; ou (ii) evitar responsabilidade criminal ou civil previsível, caso nenhuma ação seja adotada. Seção 17: os provedores devem operar seus serviços com sistemas e processos proporcionais concebidos para assegurar que a importância da livre expressão seja efetivamente considerada ao tomar decisões sobre: (i) como tratar o conteúdo, especialmente quanto à remoção (take down) ou restrição de acesso; e (ii) se devem adotar medidas contra o usuário que tenha gerado, carregado ou compartilhado esse conteúdo - o que inclui advertências, suspensões, banimentos ou restrições de uso.	Rule 4(8): Prevê expressamente que o intermediário, ao remover conteúdo, deve: (a) notificar previamente o usuário, explicando as razões e fundamentos da decisão de remoção; (b) garantir ao usuário uma oportunidade adequada de contestação e pedido de restabelecimento do conteúdo, a ser decidido em prazo razoável; e (c) o Resident Grievance Officer deve supervisionar todo o processo de resolução dessas disputas. Rule 3(1)(m)-(n): Determina que os intermediários devem atuar de forma proporcional, diligente e transparente, assegurando a acessibilidade dos serviços e o respeito aos direitos fundamentais previstos nos artigos 14, 19 e 21 da Constituição Indiana - igualdade, liberdade de expressão e proteção da vida e da liberdade pessoal. Essa previsão busca conciliar a liberdade de expressão com o dever de proteção do interesse público.
Mitigação de riscos sistêmicos	Art. 34, 1, c + Considerando 82: um dos riscos sistêmicos previstos no DSA é sobre os efeitos negativos reais ou previsíveis no discurso cívico e nos processos eleitorais. Essas previsões consagram a ideia de dever de cuidado institucional, impondo às grandes plataformas a obrigação de mitigar riscos aos processos democráticos e à segurança pública. Art. 35: prevê a necessidade de atenuação dos riscos sistêmicos identificados pelas plataformas, com medidas proporcionais, razoáveis e eficazes. Essa é uma previsão que demonstra a operatividade do dever de cuidado. A alínea "k" exige que as VLOPs marquem ou rotulem (através de marcações visíveis) o conteúdo gerado ou manipulado (como deepfakes) que possa parecer falso. Art. 45: valoriza os códigos de conduta como instrumentos que auxiliam na correta aplicação do regulamento, considerando os desafios de resposta aos diferentes tipos de conteúdos ilegais. Art. 48: prevê protocolos de crise, reforçando o dever de cuidado em situações excepcionais (como eleições).	Seção 9: impõe às plataformas o dever de realizar avaliações de risco, base para o exercício responsável do duty of care. Seção 10: complementa a anterior, detalhando o dever de implementar medidas de mitigação proporcionais. Seção 17: Estabelece deveres de proteger conteúdos de importância democrática. É esclarecida a necessidade de sistemas e processos proporcionais, designados para assegurar a liberdade de expressão de conteúdos democráticos. Esses sistemas e processos devem ser aplicados de maneira semelhante para opiniões políticas diversas. Seção 41: reconhece os códigos de conduta como instrumentos para estabelecer balizas e critérios de aplicação dos deveres de cuidado.	Rule 3(1)(b)(vii): Proíbe a hospedagem ou circulação de conteúdos que ameacem a unidade, integridade, defesa, segurança ou soberania da Índia, bem como suas relações exteriores ou a ordem pública, incluindo incitação à prática de crimes cognoscíveis ou ofensas contra outras nações. Rule 3(1)(b)(v): Determina que os intermediários devem impedir a disseminação de informações falsas, enganosas ou desinformativas, incluindo aquelas que induzam o destinatário a erro quanto à origem da mensagem ou que sejam patentemente inverídicas. Após a emenda de 06.04.2023, o dispositivo passou a exigir a remoção obrigatória de informações classificadas como falsas ou enganosas por uma unidade de verificação de fatos designada pelo Governo Central. A Rule 4 estabelece obrigações mais rigorosas para os significant social media intermediaries, exigindo a nomeação de três agentes responsáveis pelo cumprimento das normas: - um Chief Compliance Officer, residente na Índia e encarregado de assegurar a conformidade legal, respondendo pessoalmente em caso de descumprimento (Rule 4(1)(a)); - um Nodal Officer, disponível 24 horas por dia para comunicação direta com autoridades públicas (Rule 4(1)(b)); e - um Resident Grievance Officer, responsável pela gestão do sistema interno de reclamações (Rule 4(1)(c)).

Prazos e procedimentos de remoção	Art. 6º: Implica o dever de agi com diligência após o conhecimento do conteúdo ilegal. Art. 16º: Os prestadores de serviços de alojamento virtual são obrigados a criar mecanismos de notificação e ação que permitam a qualquer pessoa ou entidade notificar a presença de elementos específicos de conteúdo alegadamente ilegal no seu serviço. É exigido que a pessoa ou entidade que apresentar a notificação forneça uma justificativa clara e suficientemente fundamentada, indicando as razões pelas quais considera que as informações em questão configuram conteúdo ilegal. Quando a notificação contiver os dados de contato da pessoa ou entidade que a apresentou, o provedor de serviços de hospedagem deve enviar, sem demora injustificada, um aviso de recebimento da notificação. O provedor deve também informar a pessoa ou entidade notificante, sem demora injustificada, sobre a decisão adotada em relação ao conteúdo indicado, fornecendo orientações sobre as possibilidades de recurso ou reparação disponíveis em face dessa decisão.	Seção 10: Estabelece que os provedores de serviços devem minimizar o tempo de permanência online de conteúdos ilegais e removê-los rapidamente assim que forem detectados. Seção 38: Prevê um dever específico para os Serviços de Categoria 1 quanto à remoção de anúncios fraudulentos. O provedor deve operar o serviço com sistemas e processos proporcionais concebidos para: (i) minimizar o tempo de permanência de anúncios fraudulentos; e (ii) removê-los prontamente após ser alertado ou tomar conhecimento de sua existência. Define-se "anúncio fraudulento" como aquele pago (paid-for advertisement) que configura ofensa penal prevista na Section 40, como fraude por falsa representação, e que não é conteúdo gerado por usuário regulamentado.	Rules (2)(a)(i) e 3(1)(g): O sistema de reclamações instituído pelas *IT Rules* deve reconhecer as queixas em até vinte e quatro horas e solucioná-las no prazo máximo de quinze dias, com redução para setenta e duas horas em casos envolvendo conteúdo ilícito sensível, como materiais de nudez ou abuso sexual. Além disso, os intermediários têm o dever de preservar os registros por cento e oitenta dias após a remoção do conteúdo, conforme a Rule 3(1)(g), garantindo rastreabilidade, transparência e possibilidade de auditoria sobre as decisões de moderação tomadas.
Governança e fiscalização	Art. 37: realização de auditorias independentes, que também auxiliam na identificação e mitigação dos riscos sistêmicos e na concretização do dever de cuidado das plataformas digitais. Art. 40: assegura acesso a dados por autoridades e pesquisadores, permitindo controle social e institucional da diligência das plataformas.	Seções 104-105: tratam da possibilidade de a Ofcom determinar auditorias independentes (reports by skilled persons), o que reforça o eixo de governança.	Não há previsão de de auditorias independentes periódicas sobre bibliotecas de anúncios ou conformidade eleitoral.

2.11.4 *BENCHMARK* INTERNACIONAL (SÍNTESE COMPARATIVA)

União Europeia – DSA

Considerando 22: a isenção de responsabilidade depende da atuação diligente do prestador na supressão de conteúdos ilegais, seja por notificação de terceiros ou iniciativa própria.

- Art. 6º: define que o prestador só se exime de responsabilidade quando, após adquirir conhecimento efetivo da ilegalidade, agir prontamente para remover ou bloquear o acesso ao conteúdo.
- Art. 7º: autoriza investigações e medidas proativas de moderação, inclusive automatiza-

das, sem perda da proteção jurídica, desde que conduzidas de boa-fé e com diligência.

- Art. 16º: institui os mecanismos de notificação e ação (notice and action), exigindo que a pessoa notificante apresente fundamentação suficiente da alegação de ilegalidade. O provedor deve enviar aviso de recebimento e, posteriormente, comunicar a decisão tomada, informando as possibilidades de recurso.
- Art. 17º: impõe o dever de exposição clara de motivos em toda decisão de moderação (remoção, bloqueio ou despromoção), indicando o fundamento jurídico ou a cláusula contratual aplicada.
- Art. 18º: prevê comunicação obrigatória às autoridades competentes quando houver suspeita de crime.
- Art. 20º: determina a criação de sistema interno de gestão de reclamações, garantindo canal acessível e célere para contestação das decisões.
- Art. 34º, 1, c + Considerando 82: inclui, entre os riscos sistêmicos, os efeitos negativos sobre processos democráticos e eleitorais, exigindo monitoramento contínuo das plataformas.
- Art. 35º: obriga as VLOPs e VLOSEs a atenuar riscos sistêmicos mediante medidas proporcionais e eficazes, como rotulagem e despromoção de conteúdos manipulados.
- Art. 37º: estabelece a auditoria independente periódica, verificando a adequação das medidas de moderação e mitigação adotadas.
- Art. 48.º: determina protocolos de crise para situações que representem risco à segurança pública, inclusive períodos eleitorais.

O *DSA Elections Toolkit for Digital Services Coordinators* foi elaborado como documento de referência que consolida instrumentos, boas práticas e lições regulatórias voltadas à proteção da integridade dos processos eleitorais no ambiente digital.

Embora não trate especificamente da remoção de conteúdo, o material recomenda que os fornecedores de serviços adaptem seus termos e condições para reduzir o alcance e o impacto de conteúdos gerados por inteligência artificial generativa que possam disseminar desinformação eleitoral.

Entre as medidas sugeridas estão a rotulagem, marcação, despromoção ou supressão de conteúdos falsos ou manipulados, bem como a cooperação com verificadores de fatos e o compartilhamento de informações entre plataformas, a fim de evitar a amplificação de desinformação.

Além disso, o art. 27 institui um mecanismo de governança periódica, ao exigir que, a cada dois anos, a Comissão apresente um relatório público de avaliação e revisão do regulamento. Além de promover transparência e *accountability*, o dispositivo permite revisar continuamente o conceito de propaganda política, o que é relevante diante do surgimento de novas formas de comunicação digital que, embora não sejam propaganda formal, exercem função semelhante.

Reino Unido – *Online Safety Act* (OSA)

Seção 1: consagra os princípios de transparência e *accountability*, vinculando os provedores a padrões verificáveis de segurança.

Seção 9: impõe o dever de realizar avaliações periódicas de risco sobre conteúdos ilegais e seus impactos na arquitetura do serviço.

Seção 10: prevê a obrigação de operar sistemas e processos proporcionais destinados a minimizar o tempo de exposição de conteúdo ilegal e removê-lo rapidamente uma vez identificado (*swift take-down*).

Seção 17: estabelece os deveres de proteger conteúdos de importância democrática, determinando que as decisões de remoção considerem a relevância da livre expressão política e se apliquem de modo imparcial a diferentes opiniões.

Seção 20: prevê mecanismos acessíveis de denúncia, permitindo que qualquer usuário notifique conteúdos ilegais com facilidade.

Seção 71: dispõe que a moderação só pode ocorrer nos termos previstos contratualmente, salvo quando necessária para cumprir dever legal ou evitar responsabilidade penal ou civil.

Seção 38: impõe, aos Serviços de Categoria 1, o dever de agir contra anúncios fraudulentos, removendo-os sem demora injustificada.

Seção 41: reconhece a utilidade dos códigos de conduta emitidos pela autoridade reguladora (Ofcom) como instrumentos de harmonização e boa prática.

Seções 179–180: tipificam o delito de *false communications*, punindo a disseminação intencional de informações falsas capazes de causar dano psicológico ou físico relevante, com exceções legítimas (por exemplo, conteúdo jornalístico).

Índia – *IT Rules* 2021

Rule 3: obriga os intermediários a adotar medidas preventivas para impedir a publicação de conteúdos ilícitos, obscenos ou falsos e enganosos, incluindo aqueles identificados como desinformação por unidades oficiais de *fact-checking*.

Rule 3(1)(d): determina que, mediante ordem judicial ou notificação governamental, o conteúdo ilícito seja removido ou bloqueado em até 36 horas.

Rule 3(2)(b): impõe prazo de 24 horas para retirada de material envolvendo nudez, exposição íntima ou manipulação digital.

Rule 4(1)(a)–(c): exige a nomeação de três responsáveis internos: *Chief Compliance Officer, Nodal Officer* (disponível 24 h) e *Resident Grievance Officer*, com responsabilidade pessoal pelo cumprimento das regras.

Rule 3(2)(a)(i): determina que o sistema de reclamações reconheça as queixas em 24 horas e as resolva em 15 dias, reduzindo o prazo para 72 horas em casos graves. Ainda, os registros das remoções devem ser preservados por 180 dias (Rule 3(1)(g)).

Rule 4(4): impõe aos *Significant Social Media Intermediaries* o uso de tecnologias automatizadas para identificar proativamente conteúdos ilícitos, com supervisão humana periódica para evitar vieses.

Rule 4(8)(a)–(b): garante que, ao remover conteúdo por iniciativa própria, o intermediário notifique previamente o usuário, explique os motivos e permita contestação.

Rule 7: dispõe que o descumprimento das obrigações implica perda do safe harbor previsto na Seção 79 do *IT Act*, sujeitando o provedor a responsabilidade civil e penal direta.

Rule 3(1)(n): reafirma a necessidade de respeito aos direitos fundamentais da Constituição Indiana (arts. 14, 19 e 21), equilibrando diligência com liberdade de expressão.

Rule 4(2): em serviços de mensagens, obriga o SSMI a identificar o primeiro originador de informações em casos de crimes graves, mediante ordem judicial, preservando o conteúdo criptografado.

2.11.5 INTERPRETAÇÃO DO ART. 9º-B, § 4º (PROPOSTAS)

O constitucionalismo digital busca adaptar os princípios constitucionais clássicos - como liberdade de expressão, privacidade e direito à informação - ao ambiente virtual e às novas relações de poder estabelecidas pelas plataformas digitais. Nesse contexto, a Resolução n.º 23.732/2024 do TSE, que introduziu o art. 9º-B na Resolução n.º 23.610/2019, representa um avanço importante ao disciplinar o uso de IA na propaganda eleitoral.

O § 4º do dispositivo assume caráter sancionatório imediato, ao prever que o descumprimento das regras de transparência impõe a remoção imediata do conteúdo ou a indisponibilidade do serviço de comunicação, tanto por iniciativa da própria plataforma quanto por determinação judicial. Embora essa atuação extrajudicial possa parecer incompatível com a redação original do art. 19 do Marco Civil da Internet, o próprio dispositivo admite "disposições legais em contrário". A competência normativa do TSE - reconhecida pelos arts. 118, I, da Constituição Federal, 23, IX, do Código Eleitoral, e 57-J e 105 da Lei n.º 9.504/1997 - legitima a força normativa de suas resoluções, permitindo interpretar o § 4º do art. 9º-B como medida dotada de respaldo legal e constitucional.

Reitera-se também a recente decisão do STF, que reconheceu a possibilidade de responsabilização e dever de cuidado reforçado das plataformas em casos de conteúdos manifestamente ilícitos. Assim, o §4º pode ser considerado constitucionalmente legítimo e compatível com a nova interpretação conferida ao art. 19 do MCI.

Ainda assim, persistem lacunas regulatórias: muitos conteúdos artificiais circulam fora do âmbito da propaganda eleitoral, e a moderação segue sob controle das plataformas, com critérios opacos e decisões de grande impacto público.

Esse dilema é compartilhado por outros ordenamentos. Reconhecendo os limites da autorregulação, a União Europeia aprovou o *Digital Services Act* (DSA), que adota um modelo de corregulação, impondo deveres de diligência, transparência e *accountability* às empresas de serviços digitais. No Brasil, o Comitê Gestor da Internet (CGI.br) reforça essa mesma diretriz, ao defender que a regulação das plataformas de redes sociais assegure transparência, prestação de contas e mecanismos de

verificação das remoções de conteúdo, garantindo o devido processo e a proteção dos direitos dos usuários.

Por fim, um aspecto positivo do § 4º do art. 9º-B é a delimitação precisa do tipo de conteúdo sujeito à remoção imediata: deepfakes eleitorais ou qualquer manipulação multimídia produzida por IA sem a devida informação clara e destacada ao eleitor. Essa delimitação confere maior segurança jurídica, restringindo o alcance da medida e evitando interpretações genéricas que poderiam ampliar indevidamente a atuação das plataformas ou da Justiça Eleitoral. Passa-se, agora, à interpretação sugerida do art. 9º-B, § 4º:

Conteúdo e alcance normativo

O dispositivo possui duplo alcance normativo:

- cria um dever jurídico positivo de atuação das plataformas digitais, que devem reagir prontamente diante de conteúdos ilícitos identificados; e
- reconhece à Justiça Eleitoral competência para determinar coercitivamente a retirada, inclusive mediante sanções.

Sua natureza é preventiva e sancionatória. É preventiva porque visa evitar a disseminação de *deepfakes* e outros conteúdos sintéticos manipulados que possam comprometer a integridade informacional do processo eleitoral. É também sancionatória porque o próprio §4º prevê consequências jurídicas imediatas para o descumprimento do dever de transparência: a remoção compulsória do conteúdo ou a indisponibilidade do serviço, caracterizando uma reação punitiva à conduta ilícita, ainda que sem necessidade de prévia decisão judicial.

Inserção no contexto jurídico brasileiro e no marco regulatório da internet

O dispositivo deve ser interpretado à luz do MCI e da jurisprudência recente do STF, que reformularam o regime de responsabilidade civil dos intermediários digitais.

O art. 19 do MCI condicionava a responsabilização das plataformas à existência de ordem judicial específica, consolidando o modelo da chamada neutralidade passiva. Contudo, o STF, ao julgar os REs 1.037.396 e 1.057.258, declarou a inconstitucionalidade parcial desse artigo, afirmando que a exigência de decisão judicial prévia pode ser afastada em hipóteses excepcionais.

Nesse novo contexto, o §4º do art. 9º-B materializa essa mudança de paradigma, incorporando o entendimento de que as plataformas possuem dever de cuidado reforçado e devem atuar de forma diligente, proporcional e transparente na proteção da integridade democrática.

Conceito jurídico de “remoção imediata”

A expressão “remoção imediata” deve ser compreendida não como ato instantâneo, mas como dever de resposta célere e eficaz, compatível com a natureza dinâmica do ambiente digital.

Juridicamente, caracteriza-se pela obrigação de adotar todas as medidas técnicas e operacionais disponíveis para cessar a exposição de conteúdo ilícito logo após a constatação ou notificação idônea da violação, sem necessidade de decisão judicial prévia.

Essa interpretação é coerente com o que o DSA (art. 16) denomina swift takedown e com o OSA (seção 10), que exige que as plataformas "minimizem o tempo de permanência" de conteúdos ilegais.

A remoção imediata pressupõe, portanto:

- identificação inequívoca do conteúdo manipulado;
- avaliação mínima de verossimilhança da irregularidade; e
- resposta documentada e rastreável, que demonstre a diligência da plataforma.

Trata-se, portanto, de obrigação de meio, sujeita à aferição de boa-fé, proporcionalidade e capacidade técnica.

2.11.6 EVIDÊNCIAS E ESTUDOS DE CASO

Em pesquisa de jurisprudência feita no site do TSE, não foram encontrados resultados significativos. No entanto, na jurisprudência dos TREs há duas decisões relevantes:

TRE-GO: REI n.º 060017366. Acórdão Goiânia – GO. Relator(a): Des. Rodrigo De Melo Brustolin. Julgamento: 30/10/2024 Publicação: 01/11/2024

A decisão menciona que o conteúdo sintético multimídia criou falas não proferidas, violando os artigos 9º-B e 9º-C da Resolução TSE n.º 23.610/2019. No entanto, configurou-se a perda superveniente do interesse de agir quanto ao pedido de direito de resposta, em razão do encerramento do período eleitoral.

TRE-RS: RE n.º 060024522. Acórdão Tapehara – RS. Relator(a): Des. Volnei Dos Santos Coelho. Julgamento: 02/10/2024. Publicação: 03/10/2024

Decisão de manutenção de vídeo, sem remoção do conteúdo, já que não há comprovação de conteúdo sintético, uma vez que o vídeo é simples e caseiro. Assim, não se constitui como propaganda eleitoral irregular, já que é uma manifestação de posições políticas pessoais, merecendo tutela constitucional.

Embora o número de casos judicializados após a entrada em vigor da Resolução n.º 23.732/2024 ainda seja reduzido, alguns episódios de 2024 evidenciam sua aplicação. Um deles ocorreu em Araguaína (TO), na Representação n.º 0600321-84.2024.6.27.0001, em que o juiz determinou a suspensão de trecho de propaganda eleitoral gratuita por uso de inteligência artificial sem identificação para simular a apresentação de um projeto de UPA.

Além da propaganda eleitoral tradicional, observa-se o surgimento de um campo cinzento de práticas comunicacionais que, embora não se enquadrem formalmente como propaganda, cumprem função semelhante. Atualmente, é comum encontrar nas redes sociais vídeos manipulados por IA que mostram candidatos em situações inexistentes, produzidos por meio de estratégias digitais automatizadas, como bots, redes de desinformação e impulsionamento artificial. Essa dinâmica revela a insuficiência dos instrumentos normativos vigentes para lidar com as novas formas de manipulação informacional e propaganda velada.

2.11.7 RECOMENDAÇÕES (NORMATIVAS E OPERACIONAIS)

Estabelecer mecanismos de incentivo regulatório, para que plataformas adotem protocolos de prevenção, auditoria e transparência voluntária.

Favorecer a criação de acordos de corregulação, em que o Estado define parâmetros gerais e as plataformas desenvolvem soluções técnicas próprias, supervisionadas por autoridade pública.

Promover políticas de prevenção, com treinamento constante dos modelos de detecção de desinformação e *deepfakes* eleitorais.

Quando o aspecto preventivo falhar, exigir procedimentos internos padronizados para remoção célere, mas fundamentada.

Garantir comunicação imediata e justificada ao usuário afetado, com indicação clara do motivo da remoção, fundamento normativo e meios de recurso.

Implementar auditorias independentes para avaliar se as decisões de moderação respeitam a normativa.

2.11.8 RISCOS, SALVAGUARDAS E DIREITOS

Riscos

Risco de censura indevida: a ausência de verificação prévia rigorosa pode levar à remoção de conteúdos legítimos que apenas empreguem IA de forma estética, sem intenção manipulativa.

Risco de decisões opacas: a falta de transparência nos critérios de detecção e remoção dificulta o controle social e judicial das medidas.

Risco de desinformação reativa: a remoção sem explicação clara pode ser explorada por atores mal-intencionados como suposta "censura política", minando a confiança no sistema eleitoral.

Para mitigar esses riscos, propõe-se:

- fundamentação obrigatória das decisões de remoção, com indicação clara da violação (ausência de aviso sobre uso de IA);
- notificação imediata ao responsável, assegurando prazo de recurso administrativo junto à própria plataforma;
- revisão humana obrigatória em casos de dúvida, evitando decisões puramente automatizadas;
- supervisão independente, por meio de auditorias externas ou comitê técnico vinculado à Justiça Eleitoral, para avaliar a proporcionalidade e consistência das remoções.

REFERÊNCIAS

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 dez. 2025.

BRASIL. Superior Tribunal de Justiça (STJ). Recurso Especial n. 2.147.711 - SP (2024/0065404-7). Relatora: Ministra Nancy Andrighi. Publicado em: 26 nov. 2024. Disponível em: https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=282072669&registro_numero=202400654047&publicacao_data=20241126&formato=PDF. Acesso em: 12 dez. 2025.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 2019. Dispõe sobre propaganda eleitoral. Brasília, DF, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 10 dez. 2025

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 2024. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Brasília, DF, 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 10 dez. 2025.

COMISSÃO EUROPEIA. Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065. Official Journal of the European Union, [S. l.], 2024. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403014. Acesso em: 10 dez. 2025.

COMITÊ GESTOR DA INTERNET NO BRASIL. Princípios para a regulação de redes sociais. CGI, 2025. Disponível em: https://cgi.br/pagina/principios-cgibr-regulacao-redes-sociais/. Acesso em: 12 dez. 2025.

ÍNDIA. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Índia: Ministry of Electronics and Information Technology, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Acesso em: 10 dez. 2025.

MENDES, Gilmar Ferreira; OLIVEIRA FERNANDES, Victor. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. Revista Brasileira de Direito, Passo Fundo, v. 16, n. 1, p. 1-33, out. 2020. Disponível em: https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4103/2571. Acesso em: 12 dez. 2025.

REINO UNIDO. Online Safety Act (OSA). Londres, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Bruxelas, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2024/900 do Parlamento Europeu e do Conselho de 13 de março de 2024 sobre a transparência e o direcionamento da propaganda política. União Europeia, 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202400900. Acesso em: 11 dez. 2025.

2.12 RESPONSABILIDADE CIVIL E ADMINISTRATIVA DAS PLATAFORMAS NA OBRIGAÇÃO DE INDISPONIBILIZAÇÃO IMEDIATA DOS CONTEÚDOS GRAVES (E CONTAS) NOS CASOS DE RISCO (ART. 9º-E E 28 § 4º)

Elaine Gomes dos Santos

Art. 9º-E. Os provedores de aplicação serão solidariamente responsáveis, civil e administrativamente, quando não promoverem a indisponibilização imediata de conteúdos e contas, durante o período eleitoral, nos seguintes casos de risco:
I – de condutas, informações e atos antidemocráticos caracterizadores de violação aos artigos 296, parágrafo único; 359-L, 359- M, 359-N, 359-P e 359-R do Código Penal;
II – de divulgação ou compartilhamento de fatos notoriamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos;
III – de grave ameaça, direta e imediata, de violência ou incitação à violência contra a integridade física de membros e servidores da Justiça eleitoral e Ministério Público eleitoral ou contra a infraestrutura física do Poder Judiciário para restringir ou impedir o exercício dos poderes constitucionais ou a abolição violenta do Estado Democrático de Direito;
IV – de comportamento ou discurso de ódio, inclusive promoção de racismo, homofobia, ideologias nazistas, fascistas ou odiosas contra uma pessoa ou grupo por preconceito de origem, raça, sexo, cor, idade, religião e quaisquer outras formas de discriminação;
V - de divulgação ou compartilhamento de conteúdo fabricado ou manipulado, parcial ou integralmente, por tecnologias digitais, incluindo inteligência artificial, em desacordo com as formas de rotulagem trazidas na presente Resolução.
Art. 28, § 4º O provedor de aplicação de internet que possibilite o impulsionamento pago de conteúdos deverá contar com canal de comunicação com suas usuárias e seus usuários e somente poderá ser responsabilizado por danos decorrentes do conteúdo impulsionado se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente pela Justiça Eleitoral.

2121 VISÃO GERAL E OBJETIVOS

Res. TSE 23.610/2019, Art. 9º-E: O art. 9º-E inaugura, no ordenamento eleitoral brasileiro, uma cláusula de responsabilidade solidária de plataformas digitais em situações de grave risco à integridade do processo eleitoral, à democracia e aos direitos fundamentais. Ele transforma o dever de cooperação (art. 9º-D) em dever de resultado: a plataforma deve agir de forma imediata e eficaz, sob pena de responder civil e administrativamente junto ao autor do dano. O dispositivo também consolida um modelo preventivo e sancionatório híbrido, combinando o dever de indisponibilização imediata (inspirado no regime europeu de *notice and action*) com o reconhecimento de riscos democráticos específicos (atos antidemocráticos, desinformação eleitoral, violência institucional e discurso de ódio).

Res. TSE 23.610/2019, Art. 28, § 4º: O art. 28, §4º, da Res. TSE n.º 23.610/2019 estabelece que, além de manter canal de comunicação com os usuários, o provedor terá responsabilidade civil e administrativa limitada. Ele só responde por danos decorrentes de conteúdo impul-

sionado se, após ordem judicial específica, não adotar, dentro do prazo e dos limites técnicos de seu serviço, medidas para tornar o conteúdo apontado pela Justiça Eleitoral indisponível.

Objetivo: Garantir resposta rápida, coordenada e verificável de provedores de aplicação em situações de risco informacional e institucional durante o período eleitoral, assegurando:

- a integridade dos processos de votação, apuração e totalização;
- a segurança física e psicológica de membros da Justiça Eleitoral e do Ministério Público;
- a prevenção de violência política, discurso de ódio e incitação;
- a contenção de conteúdos manipulados por Inteligência Artificial (IA) que possam enganar o eleitor; e
- a responsabilização solidária das plataformas que se omitam.

Guia de Perguntas:

- O que significa "indisponibilização imediata"?
- A responsabilidade solidária é objetiva (independente de culpa) ou condicionada à inércia comprovada?
- Como o dever de "indisponibilização imediata" previsto no art. 9º-E se harmoniza com o art. 19 do Marco Civil da Internet, à luz da interpretação do STF nas ADIs 6.449, 6.451, 6.467 e ADPF 403, que reconheceu a possibilidade de responsabilização direta de plataformas em casos de ilicitude manifesta ou descumprimento de dever de cuidado?
- Qual é o limite razoável de "imediato"?
- A plataforma pode invocar excludente de responsabilidade se comprovar ação tempestiva?

2122 BASE NORMATIVA (BRASIL)

TSE Res. 23.610/2019, Art. 9º-E: Os provedores de aplicação serão solidariamente responsáveis, civil e administrativamente, quando não promoverem a indisponibilização imediata de conteúdos e contas, durante o período eleitoral, nos seguintes casos de risco: (Incluído pela Resolução n.º 23.732/2024) de condutas, informações e atos antidemocráticos caracterizadores de violação aos artigos 296, parágrafo único; 359-L, 359- M, 359-N, 359-P e 359-R do Código Penal; (Incluído pela Resolução n.º 23.732/2024)

- de divulgação ou compartilhamento de fatos notoriamente inverídicos ou gravemente descontextualizados que atinjam a integridade do processo eleitoral, inclusive os processos de votação, apuração e totalização de votos; (Incluído pela Resolução n.º 23.732/2024)
- de grave ameaça, direta e imediata, de violência ou incitação à violência contra a integridade física de membros e servidores da Justiça eleitoral e Ministério Público eleitoral ou contra a infraestrutura física do Poder Judiciário para restringir ou impedir o exercício dos poderes constitucionais ou a abolição violenta do Estado Democrático de Direito; (Incluído pela Resolução n.º 23.732/2024)

- de comportamento ou discurso de ódio, inclusive promoção de racismo, homofobia, ideologias nazistas, fascistas ou odiosas contra uma pessoa ou grupo por preconceito de origem, raça, sexo, cor, idade, religião e quaisquer outras formas de discriminação; (Incluído pela Resolução n.º 23.732/2024)
- de divulgação ou compartilhamento de conteúdo fabricado ou manipulado, parcial ou integralmente, por tecnologias digitais, incluindo inteligência artificial, em desacordo com as formas de rotulagem trazidas na presente Resolução. (Incluído pela Resolução n.º 23.732/2024).

Contexto regulatório adjacente:

O Marco Civil da Internet (art. 19) criou regime de imunidade condicional para plataformas, dependendo de ordem judicial específica para responsabilização. A jurisprudência inferior consolidava essa imunidade condicional como regra, com responsabilidade subsidiária apenas quando descumprida ordem judicial.

O STF, em 2025, redefiniu esse paradigma, admitindo responsabilidade direta de plataformas em casos de ilicitude manifesta, relativizando a exigência da ordem judicial quando os fatos são claros e o risco elevado.

Há precedentes judiciais que já operam remoções judiciais e responsabilização de provedores, embora ainda não no contexto eleitoral com atuação do art. 9º-E.

Houve debate legislativo anterior em torno sobre esse ponto no PL 2630 que mostrava que o tema da responsabilidade digital já estava em pauta, embora ainda sem consenso.

O art. 9º-E se insere nesse novo momento, usando base penal-eleitoral e jurisprudencial para justificar que, em casos de risco grave, a plataforma não pode esperar ordem judicial para agir.

Mais recentemente, houve a promulgação da Lei 15.211/2025 (conhecida como ECA Digital): O ECA Digital nos artigos 29 e 30 não condiciona a responsabilidade à existência de ordem judicial, mas à inércia injustificada da plataforma diante de riscos evidentes, uma forma de responsabilidade civil de segunda geração, baseada em deveres de cuidado e segurança. Principais semelhanças:

- Ambos superam a dependência da ordem judicial prevista no art. 19 do Marco Civil da Internet.
- Criam obrigações positivas de prevenção e reação imediata, vinculadas à proteção de direitos fundamentais (democracia e infância).
- Convergem para o mesmo modelo de responsabilidade solidária mitigada, em que a omissão da plataforma é equiparada à coautoria no dano.
- O TSE atua como regulador situacional, ativado em contextos eleitorais;
- O ECA Digital, como regulador estrutural, aplicável permanentemente no ecossistema infantojuvenil.

2123 METODOLOGIA DE *BENCHMARKING*

Seleção de jurisdições: UE (DSA), Reino Unido, Índia (*IT Rules*).

Unidades de comparação:

- Estrutura geral de responsabilidade;
- Tipologia de riscos regulados;
- Prazos e fluxo de resposta (notice and action);
- Salvaguardas e direitos;
- Mecanismos de cooperação institucional;
- Comparativo de proporcionalidade e garantias constitucionais.

Critério	União Europeia - *Digital Service Act* (DSA)	Reino Unido - *Online Safety Act* (OSA)	Índia – *IT Rules*
Estrutura geral de responsabilidade	Art. 14 (1-6): Obriga prestadores a indicar, nos termos e condições, regras claras sobre restrições de conteúdo, com respeito aos direitos fundamentais. Art. 4º e Art. 6º: Define exclusão de responsabilidade apenas se o provedor atuar como intermediário passivo e agir "sem demora injustificada" após ter conhecimento de conteúdo ilegal. Art. 22: Impõe remoção ou bloqueio ao tomar "conhecimento efetivo" de conteúdo ilegal, respeitando direitos fundamentais. Art. 34 e 35: Estabelece avaliação e mitigação de riscos sistêmicos, incluindo integridade eleitoral, segurança pública e desinformação. O DSA funda a responsabilidade na diligência ativa e não na culpa posterior - o mesmo fundamento material que o TSE usa para justificar a responsabilidade solidária por omissão.	Section 9(1)-(3): Provedores de "user-to-user services" devem adotar medidas proporcionais para prevenir e mitigar riscos de conteúdo ilegal. Section 10: extensão aos motores de busca. Section 71(2): Falha em cumprir "safety duties" sujeita a sanções administrativas e criminais impostas pela Ofcom. Section 160-165: dirigentes podem responder por diligência.	Rule 3(1)9a) obrigação de diligência. Rule 7: perda da isenção de responsabilidade. Rule 3(1)(b) e 3(2): responsabilidade por omissão. Rule 4(1): Plataformas com mais de 5 milhões de usuários devem manter mecanismos internos de conformidade, inclusive Chief Compliance Officer. Assim como o TSE, a Índia adota o princípio de responsabilidade por inércia: se a plataforma não age de forma diligente e tempestiva, perde a proteção jurídica. No Brasil (TSE), a consequência é solidariedade direta; na Índia, é perda da imunidade legal e sanções administrativas.
Tipologia de riscos regulados	Art. 34(1)(c): Riscos sistêmicos que afetam "os processos eleitorais e o discurso cívico". Considerandos 90-92: Tratam da propagação de conteúdos que ameacem a ordem pública, integridade democrática e segurança nacional. Art. 16(1)(b) e Considerando 12: Preveem remoção de conteúdos ilegais que violem o direito penal da UE, incluindo incitação ao ódio e terrorismo. Art. 35(1)(d): Determina mitigação de riscos relativos à manipulação algorítmica, desinformação e conteúdos sintéticos. O escopo material do art. 9º-E espelha a matriz de riscos sistêmicos do DSA, mas com ênfase eleitoral e sanção direta (solidariedade).	Section 53(2): Inclui terrorismo, incitação à violência, ódio racial ou religioso, crimes contra o Estado. → Corresponde aos incisos I e III (atos antidemocráticos e ameaças). Schedule 6 + Codes of Practice (Ofcom): Obriga plataformas a avaliar impacto de "false or misleading information likely to influence democratic participation". → Equivalente ao inciso II (fatos notoriamente inverídicos). Section 53(2)(c): discurso de ódio/ discriminação. Section 56 + Schedule 7: Obriga mitigação de conteúdos "generated or materially altered by AI" que induzam engano. → Equivalente ao inciso V (deepfakes). O OSA reproduz quase integralmente as categorias do art. 9º-E, mas em regime permanente e com amplitude temática maior (abrangendo inclusive proteção infantil e autoagressão). Ambos convergem para uma noção de risco democrático e social ampliado.	Rule 3(1)(b)(v): Proíbe conteúdos que ameacem "a unidade, integridade, defesa, segurança ou soberania da Índia". → Equivalente aos incisos I e III. Rule 3(1)(b)(xii) e Rule 4(4): Veda "informações falsas ou enganosas" que causem "perturbação da ordem pública". → Inciso II. Rule 3(1)(b)(ii)-(iv): Proíbe incitação ao ódio com base em religião, casta, sexo ou raça. → Inciso IV. Rule 4(4A) (2023 update): Obriga rotulagem de conteúdo produzido por IA e remoção de material manipulado que possa enganar o público. → Inciso V. O catálogo indiano de riscos cobre todas as hipóteses do art. 9º-E.

Prazos e fluxo de resposta (notice and action)	Art. 16 e 17: Define o mecanismo pelo qual terceiros podem notificar conteúdos ilegais; o provedor deve agir com diligência e informar a decisão ao notificante. Art. 22: "Sem demora injustificada" após conhecimento efetivo ou alerta. Art. 22(6) e Art. 62: Sinalizadores de confiança (trusted flaggers) O DSA disciplina prazos e obrigações procedimentais de remoção (sem demora injustificada), enquanto o TSE exige indisponibilização imediata.	Sections 159-160: Plataformas devem manter mecanismos de denúncia acessíveis e responder "dentro de prazos razoáveis" (reasonable timeframes). Section 77: Ofcom pode exigir informações detalhadas sobre prazos médios de remoção. Section 72(4): oferece critério de celeridade (terrorismo e ódio). Section 115: Poder sancionatório da Ofcom. O OSA não fixa prazos numéricos (como a Índia) nem exige ação instantânea (como o TSE), mas o conceito de "reasonable time" é calibrado por tipo de dano.	Rule 3(1)(d): 36 horas para remover conteúdo ilegal após ordem ou notificação. Rule 3(2)(a): 24 h para reconhecer e 15 dias para resolver ou justificar. Rule 3(2)(b): 72 h para remoção quando houver risco grave à segurança do Estado ou à vida. Rule 4(1)(d): Plataformas devem publicar relatórios mensais com tempo de resposta e volume de remoções. Enquanto o TSE exige "indisponibilização imediata", a Índia quantifica a diligência: 24-72 h para casos graves. O modelo indiano fornece, portanto, um parâmetro temporal mensurável para o conceito de "imediato" do TSE.
Salvaguardas e direitos	Art. 17: Garante ao usuário notificado o direito de contestar decisões de moderação. Art. 17(5) e Art. 24: Exigem explicação clara das razões para remoção e critérios utilizados. Art. 14(4) e Art. 63: Impõem respeito aos direitos fundamentais, especialmente à liberdade de expressão e informação. Art. 63 e Considerando 90: Exige que as medidas de moderação sejam proporcionais e fundamentadas. O DSA formaliza salvaguardas que o TSE ainda aplica implicitamente via princípios constitucionais.	Section 159(4): notificação ao usuário. Section 159(5): motivação da decisão. Section 160(2): direito de recurso interno. Section 72(5): proibição de remoção arbitrária.	Rule 3(2)(a)(v): Direito de resposta / contestação. Rule 3(2)(a)(iv): Notificação de remoção. Rule 3(2)(a)(ivA): Indica se a decisão foi humana ou automatizada. Rule 4(1)(d): Transparência periódica As ***IT Rules*** oferecem salvaguardas expressas (notificação, motivação e recurso) que podem inspirar a regulamentação infralegal do art. 9º-E, especialmente para garantir revisão posterior sem comprometer a urgência.
Mecanismos de cooperação institucional	Art. 49-52: Define os Coordenadores de Serviços Digitais e a Comissão Europeia como autoridades de supervisão. Art. 45 e 46:Prevê códigos de conduta voluntários, inclusive sobre desinformação e integridade eleitoral. Art. 56-59: Coordenação entre Estados-Membros em caso de riscos sistêmicos. O DSA distribui responsabilidades entre autoridades administrativas e a Comissão Europeia, enquanto o TSE centraliza a competência no órgão judicial eleitoral, reforçando a autoridade imediata sobre as plataformas. O DSA torna a proporcionalidade um critério textual e verificável.	Part 7 – Sections 110-126: Ofcom supervisiona, emite Codes of Practice e aplica sanções. Sections 71 e 113: Códigos de conduta (Codes of Practice) Section 112(3): Plataformas devem responder às solicitações da Ofcom e fornecer dados sobre cumprimento. Section 77: Relatórios de transparência. No Reino Unido, a autoridade administrativa (Ofcom) cumpre papel análogo ao do TSE: ambos são reguladores centrais com poder sancionatório direto, mas no Brasil a natureza é jurisdicional-eleitoral; no Reino Unido, regulatória e técnica.	Rule 3(2)(a): Grievance Officer (oficial de reclamações) Rule 4(1)(a): Chief Compliance Officer Rule 4(1)(b): Nodal Contact Person. A Índia institucionaliza a corregulação por meio de uma rede obrigatória de responsáveis locais.

2.12.4 *BENCHMARK* INTERNACIONAL (SÍNTESE COMPARATIVA)

O art. 9º-E coloca o Brasil em um modelo híbrido de responsabilidade democrática, situado entre: o DSA europeu, que privilegia a diligência proporcional e auditável; o OSA britânico, que exige processos internos consistentes e dever de cuidado reforçado; e as *IT Rules* indianas, que impõem resposta imediata e prazos objetivos.

O art. 9º-E da Resolução TSE 23.610/2019 situa o Brasil no grupo das jurisdições que adotam resposta imediata e responsabilidade solidária das plataformas, combinando a lógica preventiva do DSA com a celeridade coercitiva das *IT Rules* indianas, sob a moldura constitucional de proteção democrática.

Ele representa o ponto mais avançado da transição brasileira para um modelo de deveres positivos de proteção informacional, em que a integridade do processo eleitoral é tratada como bem jurídico de máxima prioridade.

O art. 28, § 4º segue a lógica da responsabilidade limitada de provedores (similar ao modelo de *notice-and-take-down* presente em legislações internacionais), conciliando liberdade de expressão e controle judicial de conteúdos ilícitos, ao mesmo tempo em que protege os provedores de serem responsabilizados automaticamente por conteúdos de terceiros.

Mesmo após a ordem judicial, a responsabilização ocorre apenas se o provedor não tomar as providências necessárias para tornar o conteúdo indisponível, considerando: (i) os limites técnicos do serviço: a plataforma só responde dentro daquilo que sua infraestrutura permite; por exemplo, se não for tecnicamente possível remover imediatamente todo o conteúdo, essa limitação deve ser considerada; (ii) o prazo assinalado pela ordem judicial: há um período específico determinado pela Justiça para a remoção; o descumprimento deste prazo caracteriza eventual responsabilidade.

Os "limites técnicos" se referem às restrições práticas e operacionais da própria plataforma digital que podem afetar a capacidade do provedor de cumprir integralmente uma ordem judicial. Em outras palavras, não se espera que o provedor realize algo que seja tecnicamente impossível ou inviável dentro da infraestrutura do serviço que oferece.

Dentre os exemplos de limites técnicos, pode-se citar:

Capacidade de detecção e remoção: (i) Sistemas automatizados podem não identificar imediatamente todo o conteúdo impulsionado que infringe a lei; (ii) Arquivos já replicados em cache, backups ou cópias de terceiros podem não ser acessíveis ao provedor.

Escala do serviço: Plataformas com milhões de conteúdos impulsionados podem ter dificuldade prática de agir instantaneamente sobre cada conteúdo, mesmo com ordens judiciais.

Ferramentas internas da plataforma: Se o sistema da plataforma não permite bloqueio imediato de certos tipos de conteúdo ou links, isso é um limite técnico.

Integração com terceiros: Conteúdos hospedados fora da infraestrutura direta da plataforma (como em redes de CDN ou servidores externos) podem não ser totalmente controláveis.

Recursos humanos e automatizados: Limitações de pessoal ou algoritmos que suportam a remoção podem impactar a rapidez e precisão da ação.

Quanto ao ônus da prova, cabe ao provedor provar que agiu corretamente frente à ordem judicial para se eximir de responsabilidade, demonstrando que tomou todas as providências necessárias, dentro dos limites técnicos do serviço e dentro do prazo assinalado.

Portanto, recomenda-se que o provedor garanta a existência de um meio acessível para denúncias ou comunicação com usuários. Além disso, é essencial que o provedor tenha procedimentos internos claros para atender ordens judiciais rapidamente, dentro das capacidades técnicas da plataforma.

2.12.5 INTERPRETAÇÃO DO ART. 9º-E, (PROPOSTAS)

2.12.5.1. Eixo normativo: alcance jurídico da responsabilidade solidária

O termo "solidariamente responsáveis" deve ser lido à luz da jurisprudência do STF nas ADIs 6.449, 6.451, 6.467 e ADPF 403, que reconheceu o dever de cuidado ativo das plataformas. Interpretação: a solidariedade não implica culpa presumida automática, mas responsabilidade pela omissão em agir com diligência frente a riscos manifestos.

Paralelo internacional: Equivale ao *duty of care do Online Safety Act* (sec. 9) e ao *loss of safe harbour* do Rule 7 das *IT Rules* 2021.

2.12.5.2 Eixo procedimental: deveres de cooperação e fluxos de resposta

O art. 9º-E deve ser interpretado conjuntamente com o art. 9º-F da mesma Resolução e com os acordos de cooperação TSE-plataformas (2024). Interpretação: as plataformas têm obrigação positiva de manter canal prioritário 24/7 com o TSE, garantindo resposta a comunicações oficiais em prazos mensuráveis (*benchmark* ≤ 24 h).

Paralelo internacional: Remete ao regime de *trusted flaggers* (art. 22 DSA) e aos *Nodal Contact Persons* (Rule 4(1)(b), *IT Rules*).

2.12.5.3 Eixo material: delimitação das hipóteses de risco

Interpretação: cada hipótese deve ser aplicada somente quando houver risco concreto e mensurável à integridade do processo eleitoral, à vida, ou à segurança institucional.

Evita-se uso político da norma; Mantém-se aderência à jurisprudência de proteção à liberdade de expressão.

Critério prático: O TSE deve adotar um checklist de risco informacional, inspirado no art. 34 DSA (avaliação de riscos sistêmicos).

2.12.5.4 Compatibilização do art. 9º-E com o art. 28, §4º

O art. 28 §4º estabelece que o provedor só pode ser responsabilizado se, após ordem

judicial específica, não remover o conteúdo impulsionado. Ou seja, cuida-se de responsabilidade condicionada (reativa). Por outro lado, o art. 9º-E prevê que o provedor será solidariamente responsável se não promover a indisponibilização imediata de conteúdos ou contas que representem grave risco à integridade do processo eleitoral, à democracia e aos direitos fundamentais.

Portanto, à primeira vista, parece haver conflito:

- o §4º exige ordem judicial prévia;
- o 9º-E dispensa ordem e impõe ação imediata.

Interpretação compatibilizadora:

Em caso de impulsionamento pago que contenha conteúdo enquadrável nas hipóteses do art. 9º-E, prevalece o regime do art. 9º-E, por ser norma especial e posterior, voltada à tutela da integridade democrática.

Assim, a plataforma deve promover a indisponibilização imediata, sem aguardar ordem judicial, sob pena de responder solidariamente.

O art. 28, §4º permanece aplicável apenas aos casos de propaganda eleitoral paga ordinária, sem risco grave, em que a intervenção judicial é a via adequada e proporcional.

2126 EVIDÊNCIAS E ESTUDOS DE CASO

Estudo de caso: *Facebook fails to tackle election disinformation ahead of tense Brazilian election* (*Global Witness*, 2022)

A organização Global Witness realizou um experimento prático para testar a moderação do Facebook (Meta) durante o período pré-eleitoral brasileiro de 2022. Foram enviados dez anúncios em português - cinco com informações falsas sobre as eleições e cinco que visavam deslegitimar o processo eleitoral.

Resultado: todos os anúncios com desinformação foram aprovados pela plataforma, inclusive um que inicialmente havia sido rejeitado e depois foi liberado sem explicação.

Principais achados

A Meta não exigiu autorização de anúncios políticos, contrariando suas próprias políticas internas.

Os anúncios incluíam datas falsas de votação, ataques às urnas eletrônicas e deslegitimação do TSE.

As submissões foram feitas a partir do exterior (Nairóbi e Londres), o que não gerou nenhum alerta geográfico. O canal direto entre TSE e Meta - criado em 2022 - não impediu a aprovação de conteúdo falso.

Decisões do STF e do TSE (2022–2024)

STF, ADI 6449 e correlatas (2023): admitiu a responsabilização direta de plataformas por conteúdos ilícitos manifestos, consolidando a base constitucional para o art. 9º-E.

TSE, Consulta 0604054-46.2022.6.00.0000: reconheceu a legitimidade de remoção imediata de desinformação eleitoral grave, mesmo antes de decisão final.

TSE, Medida Cautelar 0600815-85.2022.6.00.0000: determinou a exclusão urgente de conteúdo manipulado por IA, antecipando o inciso V do art. 9º-E.

2.12.7 RECOMENDAÇÕES (NORMATIVAS E OPERACIONAIS)

2.12.7.1 Nível normativo-regulatório

Explicitar critérios de diligência e prazos

O termo "indisponibilização imediata" deve ser regulamentado pelo TSE por meio de instrução normativa complementar, fixando faixas de tempo proporcionais à gravidade do risco (exemplo inspirado nas *IT Rules*):

- Até 24h: conteúdo de incitação à violência, ódio ou ataque às instituições democráticas;
- Até 72h: deepfakes, desinformação complexa ou manipulação algorítmica comprovada;
- Até 5 dias: casos que demandem verificação de autenticidade jornalística.
- Racional: cria previsibilidade e evita a insegurança jurídica do termo "imediata", sem desvirtuar a urgência eleitoral.

Integrar salvaguardas e contraditório diferido

Introduzir mecanismo de revisão pós-pleito (por exemplo, "painel de transparência eleitoral digital"), em que as plataformas apresentem os casos de remoção imediata e as justificativas de decisão.

O usuário impactado poderá solicitar revisão administrativa ou judicial após o término do período eleitoral.

Racional: compatibiliza a urgência democrática com os direitos de liberdade de expressão e devido processo.
Instituir dever formal de documentação

Determinar que todas as medidas tomadas sob o art. 9º-E sejam documentadas com logs auditáveis contendo: data/hora, ID do conteúdo, motivo, tipo de risco e decisão final.

Esses dados deverão integrar relatórios de transparência obrigatórios enviados ao TSE e publicados após as eleições (modelo do art. 15 DSA).

Racional: converte o dever de reação em dever de rastreabilidade e *accountability* pública, aproximando-se dos padrões europeus.

Harmonizar com o ECA Digital e o Marco Civil

Promover interpretação convergente entre o art. 9º-E e o art. 29 da Lei 15.211/2025, consolidando o modelo brasileiro de responsabilidade solidária mitigada.

O TSE pode expedir enunciado de súmula administrativa ou resolução conjunta com o CNJ e o CGI.br, estabelecendo o entendimento de que a ilicitude manifesta dispensa ordem judicial (critério do STF nas ADIs 6.449 e 6.451).

Racional: reforça a coerência sistêmica entre normas eleitorais, civis e de proteção de dados.

21272 Nível procedimental-operacional

Estabelecer fluxos padronizados de resposta

Inspirar-se nos "*Notice and Action Protocols*" do DSA (art. 16 e 17) e dos "*Safety Codes of Practice*" britânicos:

- Criação de canal 24/7 exclusivo para comunicações do TSE e da Procuradoria Eleitoral;
- Definição de etapas de resposta: (i) recebimento, (ii) análise inicial, (iii) decisão e (iv) retorno institucional;
- Obrigação de *acknowledgment* automático ao TSE em até duas horas do recebimento.

Adotar modelo de "*trusted flagger* eleitoral"

Formalizar o TSE e entidades credenciadas (por ex., *fact-checkers* e observatórios universitários) como sinalizadores de confiança, com prioridade de tratamento similar ao art. 22 DSA.

Reforçar, por acordo, a obrigação de resposta acelerada (≤ 24 h) às notificações desses atores.

Reforçar mecanismos de detecção preventiva

Exigir que as plataformas implementem sistemas automáticos de detecção de conteúdo manipulado por IA (*deepfake detection*) durante o período eleitoral.

Incorporar a exigência de rotulagem clara e automática para conteúdos gerados por IA, conforme o inciso V.

Criar matriz de risco informacional eleitoral

O TSE deve instituir matriz baseada nos critérios do art. 34 DSA e dos Ofcom Risk Assessments, com indicadores como:

- alcance e velocidade de disseminação;
- impacto potencial sobre o voto;
- grau de coordenação (*botnets*, desinformação organizada).

Essa matriz servirá para graduar a resposta das plataformas e o nível de sanção aplicável.

21273 Nível sistêmico-estrutural

Cooperação internacional

Estabelecer protocolos de cooperação com autoridades eleitorais da UE e do Reino Unido, trocando dados sobre práticas de mitigação de desinformação e aplicação do DSA e do OSA.

Incentivar participação brasileira em iniciativas multilaterais como o *EU Code of Practice on Disinformation* e a *Global Partnership on AI* (GPAI).

Transparência pública e pesquisa independente

Obrigar plataformas a abrirem repositórios de anúncios e conteúdos removidos, permitindo auditoria por pesquisadores e imprensa (modelo *Ad Library* do DSA, art. 39).

Estimular convênios com universidades para análise de impacto de políticas de moderação.

2128 RISCOS, SALVAGUARDAS E DIREITOS

O art. 9º-E foi criado justamente para responder a riscos informacionais e institucionais detectados no processo eleitoral brasileiro que, segundo o TSE e estudos internacionais, ameaçam a integridade democrática e exigem reação imediata.

A resposta a esses riscos não pode sacrificar direitos fundamentais.

Por isso, o art. 9º-E deve ser interpretado dentro de um sistema de salvaguardas mínimas, que garantem proporcionalidade, transparência e devido processo, em linha com padrões internacionais.

21281 Salvaguarda da proporcionalidade

Nenhum conteúdo deve ser removido sem a verificação mínima de dano potencial e relação com as hipóteses do art. 9º-E.

- Critérios recomendados (matriz TSE):
- Evidência de falsidade ou manipulação intencional;
- Grau de risco à integridade do processo eleitoral;
- Alcance e impacto da publicação;
- Contexto de circulação (coordenado, automatizado, pago etc.).

Referência: DSA, art. 35(3) – medidas "eficazes, proporcionadas e adequadas."

21282 Salvaguarda da rastreabilidade e transparência

Cada decisão de indisponibilização deve ser documentada, motivada e registrada em logs auditáveis.

Medidas concretas:

- Relatórios de transparência pós-eleição (modelo art. 15 DSA).
- Indicação clara do motivo e base normativa da decisão.
- Publicação agregada (anonimizada) dos dados de remoção.

Referência: *Online Safety Act*, sec. 77 – periodic transparency reports.

21283 Salvaguarda do contraditório e revisão posterior

As remoções feitas durante o período eleitoral devem ser revisáveis após o pleito, garantindo direito de recurso diferido.

Proposta de implementação: "Painel de Transparência Eleitoral Digital" pós-eleição, com:

- direito de contestação;
- análise técnica e fundamentação;
- publicação das correções.

Referência: *IT Rules*, Rule 3(2)(a)(v) – direito de contestar remoções.

Em relação a direitos, a aplicação do art. 9º-E deve ser guiada por três eixos de direitos fundamentais interdependentes:

Direito à informação verdadeira e íntegra: A integridade informacional é condição para o exercício pleno da cidadania e para o voto consciente.

Direito à segurança digital e à não violência: Nenhum cidadão ou agente público pode ser alvo de ameaças, perseguições ou campanhas de ódio baseadas em sua atuação democrática.

Direito à liberdade de expressão responsável: A liberdade de expressão não abrange a desinformação maliciosa que compromete o funcionamento das instituições.

REFERÊNCIAS

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei n. 15.211, de 17 de setembro de 2025. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm. Acesso em: 12 dez. 2025.

BRASIL. Supremo Tribunal Federal. Informação à sociedade: RE 1.037.396 (Tema 987) e 1.057.258 (Tema 533) responsabilidade de plataformas digitais por conteúdo de terceiros. Brasília: STF, 2025. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/Informac807a771oa-768SociedadeArt19MCI_vRev.pdf. Acesso em: 10 dez. 2025.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 2019. Dispõe sobre propaganda eleitoral. Brasília, DF, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 10 dez. 2025

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 2024. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Brasília, DF, 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 10 dez. 2025.

GLOBAL WITNESS. Facebook fails to tackle election disinformation ahead of tense Brazilian election. Londres, 2022. Disponível em: https://www.globalwitness.org/en/campaigns/digital-threats/. Acesso em: 12 dez. 2025.

HALE, Scott A. et al. Fighting misinformation during the Brazilian elections: evidence from the 2022 fact-checking ecosystem. arXiv [preprint], 2024. Disponível em: https://arxiv.org/abs/2401.02395. Acesso em: 10 dez. 2025.

ÍNDIA. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Índia: Ministry of Electronics and Information Technology, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Acesso em: 10 dez. 2025.

REINO UNIDO. Online Safety Act (OSA). Londres, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 10 dez. 2025.

REINO UNIDO. Online Safety Act: explainer. Londres: Gov.uk, [2025?]. Disponível em: https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Bruxelas, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2024/900 do Parlamento Europeu e do Conselho de 13 de março de 2024 sobre a transparência e o direcionamento da propaganda política. União Europeia, 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202400900. Acesso em: 11 dez. 2025.

2.13 TRANSPARÊNCIA E REPOSITÓRIO DE ANÚNCIOS (ART. 27-A, I E II, § 3°; ART. 28, §§ 1° E 1º-A)

Danielly Gontijo

Art. 27-A. O provedor de aplicação que preste serviço de impulsionamento de conteúdos político-eleitorais, inclusive sob a forma de priorização de resultado de busca, deverá:

I - manter repositório desses anúncios para acompanhamento, em tempo real, do conteúdo, dos valores, dos responsáveis pelo pagamento e das características dos grupos populacionais que compõem a audiência (perfilamento) da publicidade contratada;

II – disponibilizar ferramenta de consulta, acessível e de fácil manejo, que permita realizar busca avançada nos dados do repositório que contenha, no mínimo:

a) buscas de anúncios a partir de palavras-chave, termos de interesse e nomes de anunciantes;

b) acesso a informações precisas sobre os valores despendidos, o período do impulsionamento, a quantidade de pessoas atingidas e os critérios de segmentação definidos pela(o) anunciante no momento da veiculação do anúncio;

c) coletas sistemáticas, por meio de interface dedicada (application programming interface – API), de dados de anúncios, incluindo seu conteúdo, gasto, alcance, público atingido e responsáveis pelo pagamento.

§ 3º As medidas previstas no caput deste artigo são de cumprimento permanente, inclusive em anos não eleitorais e períodos pré e pós-eleições.

Art. 28. A propaganda eleitoral na internet poderá ser realizada nas seguintes formas (Lei n.º 9.504/1997, art. 57-B, I a IV):

I - em sítio da candidata ou do candidato, com endereço eletrônico comunicado à Justiça Eleitoral e hospedado, direta ou indiretamente, em provedor de aplicação de internet estabelecido no país;

II - em sítio do partido político, da federação ou da coligação, com endereço eletrônico comunicado à Justiça Eleitoral e hospedado, direta ou indiretamente, em provedor de aplicação de internet estabelecido no país;

III - por meio de mensagem eletrônica para endereços cadastrados gratuitamente pela candidata ou pelo candidato, pelo partido político, pela federação ou pela coligação desde que presente uma das hipóteses legais que autorizam o tratamento de dados pessoais, nos termos dos arts. 7º e 11 da Lei n.º 13.709/2018 ;

IV - por meio de blogs, redes sociais, sítios de mensagens instantâneas e aplicações de internet assemelhadas, dentre as quais aplicativos de mensagens instantâneas, cujo conteúdo seja gerado ou editado por:

a) candidatas, candidatos, partidos políticos, federações ou coligações, desde que não contratem disparos em massa de conteúdo nos termos do art. 34 desta Resolução (Lei n.º 9.504/1997, art. 57-J); ou

b) pessoa natural, vedada: (Redação dada pela Resolução n.º 23.732/2024)

1. a contratação de impulsionamento e de disparo em massa de conteúdo nos termos do art. 34 desta Resolução (Lei n.º 9.504/1997, art. 57-J);

2. a remuneração, a monetização ou a concessão de outra vantagem econômica como retribuição à pessoa titular do canal ou perfil, paga pelas(os) beneficiárias(os) da propaganda ou por terceiros.

§ 1º Os endereços eletrônicos das aplicações de que trata este artigo, incluídos os canais publicamente acessíveis em aplicativos de mensagens, fóruns online e plataformas digitais, salvo aqueles de iniciativa de pessoa natural, deverão ser comunicados à Justiça Eleitoral impreterivelmente:
I - no RRC ou no DRAP, se pré-existentes, podendo ser mantidos durante todo o período eleitoral os mesmos endereços eletrônicos em uso antes do início da propaganda eleitoral (Lei n.º 9.504/1997, art. 57-B, § 1º);
II - no prazo de 24 (vinte e quatro) horas a contar de sua criação, se ocorrer no curso da campanha.
§ 1º-A. Os provedores de aplicação que utilizarem sistema de recomendação a usuárias e usuários deverão excluir dos resultados os canais e perfis informados à Justiça Eleitoral nos termos do § 1º deste artigo e, com exceção das hipóteses legais de impulsionamento pago, os conteúdos neles postados.
Art. 29. [...]
§ 5º Todo impulsionamento deverá conter, de forma clara e legível, o número de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ) ou o número de inscrição no Cadastro de Pessoas Físicas (CPF) da pessoa responsável, além da expressão "Propaganda Eleitoral".
§ 6º A divulgação das informações exigidas no § 5º deste artigo é de responsabilidade exclusiva das candidatas, dos candidatos, dos partidos, das federações ou das coligações, cabendo aos provedores de aplicação de internet que permitam impulsionamento de propaganda eleitoral assegurar que seja tecnicamente possível às pessoas contratantes inserirem a informação, por meio de mecanismos de transparência específicos ou livre inserção, desde que sejam atendidas as disposições contratuais e requisitos de cada provedor.

2.13.1 VISÃO GERAL E OBJETIVOS

Objetivo: interpretar o alcance dos deveres de transparência previstos no Art. 27-A, I e II, §3º (repositório de anúncios e ferramentas de consulta/consulta via API) e nos §§1º e 1º-A do Art. 28 (comunicação de endereços eletrônicos à Justiça Eleitoral e exclusão de canais/perfis de resultados por sistemas de recomendação). A análise deve identificar requisitos mínimos de cumprimento, comparar com boas práticas internacionais (ex.: bibliotecas de anúncios da União Europeia, EUA etc.) e avaliar os impactos para fiscalização eleitoral, liberdade de expressão e *accountability* das plataformas.

Guia de Perguntas:

Sobre o Art. 27-A, I e II, §3º

- O que caracteriza um "repositório em tempo real"? Basta atualização diária, ou exige *near real-time*?
- Qual deve ser o nível de granularidade dos dados (valores, perfilamento, alcance) para cumprir o dever?
- Até onde vai a obrigação de transparência de critérios de segmentação sem ex-

por dados pessoais?

- O que torna uma ferramenta de consulta “acessível” e de “fácil manejo”? Interface pública? Relatórios exportáveis?
- A API deve permitir acesso aberto irrestrito (pesquisadores, imprensa, sociedade civil) ou apenas à Justiça Eleitoral?
- Quais métricas de confiabilidade e auditabilidade podem ser exigidas para avaliar a completude do repositório?

Sobre o Art. 28, §§1º e 1º-A

- Quais são as consequências jurídicas para candidaturas/partidos que não comunicarem seus canais no prazo?
- Como a Justiça Eleitoral deve gerir o banco de dados de endereços eletrônicos declarados? De forma pública ou restrita?
- De que forma a exclusão de canais/perfis de resultados pelos sistemas de recomendação impacta a liberdade de expressão e a visibilidade orgânica de candidaturas?
- Quais são as boas práticas comparáveis em outras jurisdições para mitigar riscos de manipulação algorítmica em períodos eleitorais?
- O dever de exclusão dos sistemas de recomendação deve abranger também conteúdos impulsionados ou apenas conteúdos orgânicos?
- Como compatibilizar essa obrigação com regras de neutralidade algorítmica e com a LGPD (no tratamento de dados para recomendação)?

2.13.2 BASE NORMATIVA (BRASIL)

TSE Res. 23.732/2024, Art. 27-A, I e II, § 3º - O dispositivo impõe ao provedor de aplicação que realiza impulsionamento de conteúdos político-eleitorais o dever de manter um repositório em tempo real com dados essenciais: conteúdo dos anúncios, valores gastos, responsáveis pelo pagamento, e características do público atingido (perfilamento). Também exige disponibilização de uma ferramenta de consulta acessível, que permita buscas por palavras-chave, termo de anunciantes, com acesso a valores, período, público atingido e critérios de segmentação, bem como interface de API para coleta sistemática desses dados.º § 3º dispõe que essas medidas de transparência são de cumprimento permanente, não apenas nos períodos eleitorais, mas também nos anos não eleitorais, pré e pós eleições. Essas obrigações (repositório + ferramenta + API) formam um núcleo normativo que determinam às plataformas prestar contas de suas operações de anúncios eleitoralizados de modo público/aberto, bem como permitir auditoria em tempo real ou quase real.

TSE Res. 23.732/2024, Art. 28, §§1º e 1º-A - O § 1º obriga as candidaturas, partidos, federações e coligações a comunicar à Justiça Eleitoral os endereços eletrônicos (sites, perfis, canais) onde farão propaganda eleitoral. Se esses endereços já existiam, devem ser comunicados no RRC ou DRAP; se surgirem durante a campanha, devem ser comunicados em até 24 horas. O § 1º-A impõe aos provedores de aplicação que utilizam sistemas de recomendação que excluam dos resultados (os algoritmos de recomendação) os canais/perfis previamente informados à Justiça Eleitoral, salvo nos casos legalmente permitidos de impulsionamento pago. Ou seja, a plataforma não deve promover organicamente ou recomendar programas orgânicos de perfis não comunicados, exceto quando aquele conteúdo for objeto legítimo

de impulsionamento. Esse regime busca garantir que todas as plataformas eleitorais sejam conhecidas pelo Judiciário eleitoral desde o início e que a visibilidade algorítmica - ou recomendação automática - de canais que não cumprirem essa comunicação seja restringida.

TSE Res. 23.732/2024, 29, §§ 5º e 6º - Todo conteúdo impulsionado deve exibir, de forma clara e legível, o número de inscrição no CPF ou CNPJ da pessoa responsável, acompanhado da expressão "Propaganda Eleitoral". A divulgação dessas informações é de responsabilidade exclusiva de candidatas, candidatos, partidos, federações ou coligações. Aos provedores de aplicação que permitam o impulsionamento cabe garantir meios técnicos para que as pessoas contratantes possam inserir tais dados, seja por mecanismos próprios de transparência, seja por livre inserção, observadas as regras contratuais e os requisitos da plataforma.

Contexto regulatório adjacente:

STF - Repercussão Geral Tema 987 e Tema 533. Modulação do art. 19 do Marco Civil da Internet - dever de agir das plataformas (mesmo sem ordem judicial) - transparência de anúncios é um dos elementos desse papel ativo.

Decisão estabelece que, em casos de conteúdo ilícito ou que afete bens jurídicos primordiais (honra, Estado Democrático de Direito, discurso de ódio etc.), as plataformas devem remover ou tornar indisponível o conteúdo independentemente da ordem judicial, sob pena de responsabilidade. Isso dialoga diretamente com a exigência de repositório/comunicação - se as plataformas devem agir proativamente para remover conteúdo nocivo, elas precisam saber exatamente quais anúncios estão ativos, como são segmentados e quem os financia - o que só é possível com transparência.

2.1.3.3 METODOLOGIA DE *BENCHMARKING*

Seleção de jurisdições: UE (DSA), Reino Unido (OSA), Índia (*IT Rules*).

Unidades de comparação (possíveis critérios):

Repositório de anúncios e dados disponíveis: abrangência mínima (conteúdo, valores, público, critérios de segmentação), periodicidade de atualização (tempo real vs. prazos específicos), escopo temporal (apenas eleições ou caráter permanente, como no § 3º do art. 27-A)

Acessibilidade e consulta pública: idioma local, interface mobile e compatibilidade com acessibilidade (deficiência visual, auditiva), facilidade de busca avançada (palavra-chave, anunciante, público-alvo), disponibilidade de APIs abertas para coleta sistemática por sociedade civil, imprensa, acadêmicos e autoridades.

Comunicação de endereços eletrônicos e canais (Art. 28, § 1º): obrigatoriedade de registro prévio e prazos (ex.: 24 horas no Brasil), publicidade desses cadastros (banco de dados aberto ou restrito), medidas de auditoria e verificação de autenticidade dos canais declarados.

Regras sobre recomendação algorítmica (Art. 28, § 1º-A): obrigações de excluir canais não registrados dos sistemas de recomendação, deveres de transparência sobre critérios de ranqueamento e priorização, limites entre recomendação orgânica e impulsionamento pago.

Devido processo e governança: mecanismos de contestação por anunciantes/candidaturas quando houver erro em registros ou exclusão de canais; identificação de responsáveis internos nas plataformas (ex.: compliance officer eleitoral); auditorias periódicas e relatórios públicos de conformidade.

Transparência ampliada e prestação de contas: relatórios públicos periódicos de gastos e alcance dos anúncios eleitorais; dashboards de acesso simplificado para eleitoras/es; cooperação institucional com autoridades eleitorais e agências independentes de checagem.

Mitigação de abusos: salvaguardas contra manipulação do repositório (ex.: inserção de dados falsos); prevenção de uso indevido de APIs (rate limits, autenticação); Mecanismos de sanção a anunciantes que descumprirem regras (ex.: exclusão de anúncios, multas, bloqueio de contas).

Critério	União Europeia - *Digital Service Act* (DSA)	Reino Unido - *Online Safety Act* (OSA)	Índia – *IT Rules*
Repositório de anúncios e dados disponíveis	Art. 39 DSA: Abrangência mínima: definida no art. 39(2): conteúdo; anunciante; pagador; período; parâmetros de direcionamento (inclusive exclusões); identificação de comunicações comerciais; total de destinatários e, quando aplicável, agregados por Estado-Membro. Não inclui "valor gasto". Periodicidade / atualização: repositório durante a exibição e por 1 ano após; o DSA não usa a expressão "tempo real", mas exige ferramenta pesquisável e APIs e "esforços razoáveis" para garantir exatidão e completude. Escopo temporal: caráter permanente e geral (não limitado a eleições) enquanto houver exibição de anúncios, + 1 ano.	SS. 77 e 78 OSA: Não há dever de biblioteca pública de anúncios, nem API pública, nem requisitos explícitos de "tempo real". O que existe: Relatórios de transparência por notificação da OFCOM (ss.77 e 78), que podem incluir métricas decididas pela autoridade. Publicidade de anúncios políticos / perfis: ausente no OSA (ao contrário do art. 27-A brasileiro). *Em consulta, a sociedade civil pediu dados em formatos reutilizáveis (CSV/JSON) e dashboards - a Ofcom registrou o pedido, mas não impôs obrigação de "open data"/API nesta fase.	Não existe repositório público de anúncios; há transparência relatorial e rotulagem: (i) Rule 4(1)(d): relatórios mensais (SSMIs) com números de remoções, inclusive as proativas; (ii) Rule 18(3): relatórios mensais (publishers); (iii) Rule 19(1)(2): disclosure público mensal de queixas, ações e ordens (iv) Rule 4(3): rotulagem de publicidade. Não há obrigação de repositório em (near) real-time, sem granularidades mínimas (valores, alcance, perfilamento) expostas pública e cumulativamente; sem API aberta.

Acessibilidade e consulta pública	Acesso público + busca avançada: art. 39(1) exige ferramenta pesquisável que permita consultas multicritério, além de APIs. APIs abertas/integração: art. 39(1) (APIs) e art. 44(1)(d),(f) (normas para interfaces/APIs e interoperabilidade do repositório). Acessibilidade (pessoas com deficiência): o DSA incentiva códigos de conduta em matéria de acessibilidade, com objetivos de design acessível e disponibilização de informações/formulários de modo acessível. (art. 47). (Não há menção explícita a "mobile"/idioma local no art. 39; isso tende a surgir via normas/códigos e boas práticas de UX.)	S. 72 - Acessibilidade: o OSA exige clareza e acessibilidade em termos de serviço (e em como são explicados os processos de content reporting e complaints): Consulta pública / busca avançada / API: não há obrigação de ferramenta pública de busca nem de API aberta (isso é típico do art. 27-A brasileiro). Relatórios públicos: existem transparency reports (ss.77 e 78), mas o OSA deixa a OFCOM definir conteúdo e formato; não há menção a API. *A Ofcom publicará os relatórios das plataformas em seu site, numa área única, e afirma que engajará a sociedade civil para presentation of data "levando em conta acessibilidade" (inclusive para públicos vulneráveis).	Há comandos de acessibilidade / linguagem e de "prominent publication"; não há API ou requisitos de busca avançada: (i) Rule 3(1)(a) e (b) - língua/idioma - regras, política de privacidade e user agreement em inglês ou em línguas do Oitavo Anexo, na língua de escolha do usuário; (ii) Rule 3(2) - definição de "prominently publish" (claramente visível na home / homescreen) - reforça facilidade de acesso a informações obrigatórias; (iii) Rule 3(1)(m) (princípio de acessibilidade) e Rule 3(1)(n) e respeito a direitos. Não há previsão de API aberta ou busca avançada para dados de anúncios.
Comunicação de endereços eletrônicos e canais	Não há no DSA obrigação de registro prévio de canais/perfis de campanha perante autoridade eleitoral, tampouco prazo de 24h. As exigências de transparência são outras (p.ex., relatórios periódicos, base pública de decisões).	OSA, ss. 23 e 102: não há dispositivo equivalente ao §1º do art. 28 (RRC/DRAP e 24h). OSA foca em registros internos e prestação de informações à OFCOM (s.23 – record-keeping) e em notificações / solicitações de informação pela OFCOM (s.102).	Aproximação parcial (setorial): (i) Rule 18(1)(2) envio de dados ao MIB por publishers (prazo de 30 dias). (ii) Rule 5 intermediários devem informar publishers sobre o dever de fornecer dados e podem dar selo de verificação visível a quem cumprir.

Regras sobre recomendação algorítmica	Transparência de parâmetros e controle do usuário: art. 27 obriga explicar por que conteúdos são sugeridos e permitir alterar parâmetros; para VLOPs/VLOSEs, art. 38 garante opção não-perfilada. Não há exigência de excluir "canais não registrados" de resultados de recomendação. Normas e interfaces: art. 44 promove padrões e interfaces (inclusive para apresentar parâmetros de recomendação).	Não há a regra de excluir canais do sistemas de recomendação. S. 72. Transparência / termos sobre processos: S.72 exige que os termos detalhem "o sistema e os processos para reporte / queixas", prazos, etc. Relatórios de transparência podem exigir dados sobre sistemas e processos (a critério da OFCOM), mas o texto legal não traz mandatório específico sobre algoritmos de recomendação comparável ao §1º-A do art. 28. Anúncios pagos vs. orgânico: o OSA trata de fraudulent advertising, mas não impõe um repositório / rotulagem pública semelhante ao art. 27-A.	Não há a regra de exclusão de canais dos sistemas de recomendação. Há apenas: (i) Rule 4(3) rotulagem de conteúdo publicitário (ii) Rule 4(4) - deveres ao usar ferramentas automatizadas - proporcionalidade, privacidade, revisão humana e avaliação de viés/justiça Sem regras sobre neutralidade / ranqueamento de conteúdo político ou limites entre recomendação orgânica e impulsionamento pago.
Devido processo e governança	Auditoria independente de VLOPs/VLOSEs e follow-up com relatório de execução (governança/aprendizado organizacional). Relatórios de transparência periódicos (art. 24) – accountability pública geral. (Mecanismos formais de contestação por anunciantes/candidaturas existem no DSA para usuários em geral via sistema interno de reclamações e resolução extrajudicial - compõem o devido processo no DSA.)	S. 72: Queixas e reporte (devido processo do usuário): determina que os termos de serviço devem resumir o procedimento para tratamento de reclamações, incluindo os prazos dentro dos quais as decisões devem ser tomadas e como os usuários podem recorrer. S.104. Auditoria / supervisão: Reports by skilled persons (auditoria independente determinada pela OFCOM): S. 102. Pedidos formais de informação (governança): S. 77 e 78 - Relatórios de transparência públicos (accountability). S. 23. Revisões e registros internos.	Há previsão sobre denúncias e governança, sem trilhos específicos de auditoria eleitoral: (i) Rule 3 (2) (a) (i) Grievance Officer e prazos: reconhecer em 24h e resolver em 15 dias; certos casos devem ser resolvidos em 72h; (ii) Rule 3A - GAC – Grievance Appellate Committee (recurso online; meta de decisão em 30 dias); (iii) Rule 4(1)(a)-(c) Oficiais internos (SSMIs): Chief Compliance Officer, Nodal Contact Person (24/7) e Resident Grievance Officer; (iv) Rule 4 (1) (d) Relatório de conformidade mensal Sem: obrigação específica de auditorias independentes periódicas sobre bibliotecas de anúncios ou conformidade eleitoral.

Transparência ampliada e prestação de contas	Relatórios públicos e base pública e legível por máquina de decisões/razões (incl. art. 24(5)). Cooperação com autoridades e pesquisadores: acesso a dados (art. 40), inclusive explicações sobre algoritmos; art. 44 prevê padrões para facilitar isso. Códigos de conduta para toda a cadeia de publicidade on-line (art. 45) – reforçam prestação de contas.	Ss. 77 e 78 - Relatórios públicos (S. 77): Conteúdo dos relatórios (Schedule 8 - s.78) Dashboards / "biblioteca de anúncios" e cooperação com checadores: não há obrigação específica (fica no desenho de relatórios/ obrigações que a OFCOM vier a exigir). *A OFCOM vai publicar, além dos relatórios das plataformas, os seus próprios relatórios (core anual + temáticos) para dar visão setorial e comparável.	Correspondência parcial: (i) Rules 4(1)(d), 18(3) - Relatórios mensais (SSMIs) e publishers; (ii) Rule 19 (1) (2) - Divulgação pública mensal de queixas/ordens (iii) Rule 3(1)(j) Cooperação com autoridades: fornecer informações a órgãos governamentais no máximo em 72h (com finalidade e ordem por escrito). *Sem: exigência de dashboards voltados ao eleitor, ou de relatórios públicos de gastos/alcance de anúncios eleitorais.
Mitigação de abusos	Integridade do repositório e APIs: o DSA impõe que as informações sejam exatas e completas e prevê normas e interoperabilidade/APIs via art. 44. Não detalha "rate-limits", mas habilita a padronização técnica para garantir segurança e confiabilidade. Sanções a anunciantes x plataformas: o DSA se estrutura para responsabilizar plataformas (com poderes de supervisão e sanções administrativas). Não cria sanções diretas específicas a anunciantes no âmbito do repositório; códigos de conduta (art. 45) podem endereçar a cadeia de intermediários e práticas de transparência.	Não há "repositório/API" para proteger, mas existem deveres e poderes relevantes: fraudulent advertising (Ss. 38, 39, 40) APIs/rate-limits: não há referência no OSA a APIs públicas ou limites técnicos específicos; tais aspectos só aparecem, se for o caso, na notificação de relatório (ss. 77 e 78). *No OSA, como a obrigação é de "reporting" e não de repositório de ads, o foco é na qualidade/consistência dos dados reportados e na possibilidade de escrutínio público ao publicar tudo em um só lugar.	Correspondência parcial (genérico): (i) Rule 4(6) Mecanismo de ticket / acompanhamento de reclamações (SSMIs) - transparência processual (ii) Rule 4(8)(a)-(c) Devido processo em remoções proativas de conteúdo (notificação prévia ao usuário, chance de contestar); (iii) Rule 7 Perda de "safe harbour" por descumprimento das Rules; (iv) Rule 3(1)(l) Relato de incidentes de cibersegurança ao CERT-In - reforça integridade sistêmica. * Sem: salvaguardas específicas contra manipulação de repositório de anúncios (p.ex., dados falsos), APIs (rate-limits/ autenticação) ou sanções específicas a anunciantes eleitorais.

Análise Adicional:

Critério	Regulamento (UE) 2024/900 do Parlamento Europeu e do Conselho de 13 de março de 2024 sobre a transparência e o direcionamento da propaganda política
Repositório de anúncios e dados disponíveis	O art. 13 cria o repositório europeu com portal público, exigindo formato machine-readable e consulta por múltiplos critérios; a retenção é de 7 anos e a disponibilização se dá a partir da primeira publicação (com 72h para quem não é VLOP). O conteúdo mínimo vem do art. 12 (aviso): patrocinador, valores por anúncio e totais da campanha, período, contexto eleitoral e resumo das técnicas de direcionamento e parâmetros/dados usados. Há ainda links do aviso para o repositório e para o portal único.
Acessibilidade e consulta pública	O art. 12(3) exige que os avisos sejam facilmente acessíveis, apresentados na língua do anúncio e em conformidade com requisitos de acessibilidade, inclusive com mais de um canal sensorial. O art. 13(1)(a) determina acesso ao público via portal com consultas multi-critérios. O art. 13(6) manda a Comissão definir API e autenticação normalizada para permitir acesso público e serviços de pesquisa de fácil utilização.
Comunicação de endereços eletrônicos e canais	Inexistente no Regulamento Europeu. O Regulamento estrutura o ecossistema de propaganda (conteúdo, avisos, repositório, targeting), sem prever cadastro compulsório de canais/perfis perante autoridade, ao contrário do art. 28, §1º da Resolução do TSE. O escopo do instrumento europeu (definições: "propaganda política" e "anúncio") confirma esse foco.
Regras sobre recomendação algorítmica	Não há regra europeia equivalente à exclusão de recomendação por falta de cadastro. Em vez disso, o Regulamento Europeu se ancora em rótulo / aviso (arts. 11 e 12), repositório (art. 13) e regras/limites de direcionamento e distribuição (v.g., proibições de dados sensíveis e deveres de transparência de parâmetros e fontes de dados).
Devido processo e governança	O Regulamento cria mecanismo de indicação de anúncios possivelmente não conformes (art. 15) e prevê tratamento célere de notificações, especialmente no último mês antes da eleição/referendo (art. 24 e recitais 105-106) Há autoridades competentes com poderes de solicitar informações, advertir, ordenar cessação e aplicar sanções (art. 16(4)-(5)). Também existem pontos de contato e coordenação europeia entre autoridades, em articulação com o DSA (Reg. 2022/2065).
Transparência ampliada e prestação de contas	O art. 14 exige informação periódica agregada por campanha (montantes, uso de técnicas de direcionamento / distribuição) como anexo ao relatório de gestão do editor e disponibilização às autoridades competentes. O art. 13 garante portal público com busca e, via API/atos de execução, acesso do público e de terceiros aos avisos e bases de dados para análise e apresentação dos dados.
Mitigação de abusos	O Art. 12(3)(4)(6)(7) impõe garantias de exatidão, obrigação de correção imediata ("sem demora injustificada"), acessibilidade fácil e visível, e conservação por sete anos, devendo os detalhes técnicos ser definidos em atos complementares da Comissão. O Art. 13(6) trata de metadados padronizados, autenticação e API comum, reduzindo assimetria e possíveis manipulações de coleta e agregação. Em execução, o art. 25 prevê sanções efetivas, proporcionais e dissuasivas, com teto de 6% do rendimento/orçamento do patrocinador/editor ou do volume de negócios mundial do editor, e considera especialmente graves infrações a artigos-chave (11, 12, 13, 15, 16 e 18) no último mês antes da eleição/referendo.

2.13.4 *BENCHMARK* INTERNACIONAL (SÍNTESE COMPARATIVA)

União Europeia – DSA

Art. 39: obriga VLOPs/VLOSEs a manter repositório público com ferramenta pesquisável (consultas multicritério) e APIs, válido durante a veiculação do anúncio e por 1 ano após; o repositório deve omitir dados pessoais de destinatários e ser exato e completo. O n.º 2 lista os campos mínimos (conteúdo do anúncio; anunciante; pagador; período de exibição; principais parâmetros de direcionamento/inclusão e exclusão; identificação de comunicações comerciais; número total de usuários alcançados e, quando aplicável, agregados por Estado-Membro) - não inclui campo "gasto".

Art. 26 (publicidade nas plataformas em linha) complementa o tema: para cada anúncio exibido, o usuário deve identificar, em tempo real, que se trata de anúncio, quem é o anunciante e quem pagou, e ver os principais parâmetros de direcionamento e como alterá-los.

Art. 27 (transparência dos sistemas de recomendação) exige explicar, em linguagem clara, os parâmetros principais dos recomendadores, por que conteúdos são sugeridos e opções para o usuário alterar esses parâmetros; a funcionalidade deve ser de acesso direto e fácil. Para VLOPs/VLOSEs, o art. 38 impõe ao menos uma opção não baseada em perfis.

Art. 40 (acesso regulatório) garante acesso a dados para o coordenador nacional e a Comissão, inclusive explicações sobre a lógica e testagem de sistemas algorítmicos (recomendação e publicidade), reforçando o ecossistema de supervisão.

Reino Unido - *Online Safety Act* (OSA)

O OSA não regula o processo eleitoral em si (como campanhas, financiamento ou propaganda), mas estabelece regras de transparência democrática digital). Mas há regras visam garantir que o debate político e eleitoral online ocorra de forma livre, informada e verificável, limitando o poder opaco das plataformas sobre conteúdos de natureza política (S.17, em especial).

S. 17 (conteúdo de importância democrática) - conteúdo de importância democrática definido como aquele destinado a contribuir para o debate político democrático no Reino Unido. Obriga as plataformas de Categoria 1 (grandes plataformas, como redes sociais) a: (i) manter termos de serviço claros explicando como tratam esse tipo de conteúdo (S. 17 (4)); (ii) aplicar tais regras de forma transparente e consistente (S. 17 (5)). O objetivo é impedir decisões arbitrárias ou discriminatórias na moderação de discursos políticos, partidários ou eleitorais. Em resumo: transparência sobre como e por que conteúdos políticos são removidos, reduzidos ou priorizados.

S. 77 e S. 78 (relatórios de transparência): no OSA não há obrigação específica de "biblioteca pública de anúncios" nem API pública comparável ao art. 27-A. O ponto mais próximo é o regime de relatórios de transparência exigidos por notificação da OFCOM: a OFCOM pode enviar uma notificação de relatório de transparência a um provedor de serviço regulado, exigindo que o provedor publique um relatório de transparência (s. 77 (1)), a notificação deve indicar: (a) as informações que devem ser incluídas no relatório; (b) a forma como

o relatório deve ser apresentado; (c) o momento em que o relatório deve ser publicado (s. 77 (2)). Em suma: o OSA permite que a OFCOM imponha relatórios públicos (com conteúdo, formato e periodicidade definidos pela autoridade), mas não obriga um repositório de anúncios com busca avançada e API de acesso público como faz o art. 27-A.

S. 23 e S. 72 (dever de manutenção de registros e acessibilidade dos termos de serviço) O OSA não possui um dever equivalente de registro/ comunicação de canais (URLs, perfis) à autoridade eleitoral. Os dispositivos mais próximos tratam de transparência, termos de serviço, registros e prestação de informações à OFCOM, não de cadastro eleitoral: todo provedor de um serviço abrangido pela Parte 3 deve agir de modo a garantir que sejam feitos e mantidos registros escritos de: toda avaliação de risco exigida; toda revisão realizada; toda decisão, medida ou providência adotada em conformidade com qualquer dever estabelecido nesta Parte. Ao cumprir esse dever, o provedor deve considerar a importância de manter tais registros completos, precisos e atualizados. (S. 23). Os termos de serviço devem ser claros e acessíveis e devem resumir o sistema e os processos utilizados para o relato de conteúdo e para o tratamento de reclamações, incluindo os prazos para as decisões. (S. 72).

Ou seja, há transparência e registro perante a OFCOM, mas não um cadastro eleitoral de canais.

Em suma: há aproximação parcial entre o art. 27-A (transparência) e os Sections 77-78 (relatórios de transparência) do OSA. Não há equivalentes no OSA para o cadastro eleitoral de canais (§1º do art. 28) nem para a exclusão de recomendação de canais não comunicados (§1º-A do art. 28); há obrigações sobre termos de serviço, transparência e controles de usuário, mas não uma regra específica para "desindexar/desrecomendar" canais por falta de comunicação à autoridade.

Índia - *IT Rules* 2021

Não há nas *IT Rules* um dever expresso de: (i) manter repositório público de anúncios político-eleitorais; (ii) oferecer busca avançada; ou (iii) abrir API. Há, porém, deveres gerais de transparência e relatórios periódicos, que funcionam como aproximações:

Rule 4(1)(d) (relatório de conformidade mensal pelos SSMIs - significant social media intermediaries) - determina publicar relatório periódico de conformidade todos os meses, incluindo o número de links removidos ou desativados em decorrência de qualquer monitoramento proativo.

Rule 18(3) (relatórios mensais de publishers - notícias e conteúdo online): determina publicar relatório periódico de conformidade todos os meses, mencionando os detalhes das reclamações recebidas e as medidas adotadas a respeito.

Rule 19 (1)(2) (divulgação pública mensal de reclamações, medidas e ordens recebidas) determina que o publisher e o órgão autorregulador façam uma divulgação verdadeira e completa, que deve ser exibida publicamente e atualizada mensalmente.

Rule 4(3) (rotulagem de conteúdo publicitário nos SSMIs) identificação clara como "*advertised / marketed / sponsored / owned / exclusively controlled".*

Rule 3(1) (acessibilidade/clareza como princípio transversal) determina adotar todas as medidas razoáveis para garantir a acessibilidade, juntamente com a transparência.

Quanto à regra de comunicação dos canais / perfis à Justiça Eleitoral, a aproximação mais próxima é setorial (mídia/notícias), não eleitoral: (i) Rule 18 (*Furnishing of information*): publishers de notícias e "online curated content" devem informar ao Ministério da Informação e Radiodifusão (MIB) os dados da entidade (prazo 30 dias para quem inicia operações após os Rules). (ii) Rule 5 (*News and current affairs*): intermediários devem publicar aviso para publishers de notícias de que forneçam ao MIB os detalhes de suas contas (*user accounts*) e podem exibir um "*verification mark*" para quem cumpriu o Rule 18. Diferença: no Brasil, o §1º vale para candidaturas / partidos / federações / coligações e tem prazo de 24h; na Índia, o dever é voltado a publishers (mídia) e o prazo padrão é 30 dias; as *IT Rules* não determinam um banco público dos endereços declarados (há *disclosure* mensal de *grievances*, não de canais).

Quanto à regra de excluir canais/perfis declarados dos resultados de sistemas de recomendação, salvo impulsionamento pago, não há equivalente nas *IT Rules*; o que há de mais próximo é: (i) Rule 4(3) (rotulagem de conteúdo *"advertised/marketed/sponsored…"*) - transparência sobre natureza publicitária do conteúdo, não sobre recomendação algorítmica. (ii) Rule 4(4) (uso de ferramentas automatizadas, com salvaguardas de proporcionalidade, privacidade, acurácia / viés e *oversight* humano).

Regulamento Europeu sobre transparência e o direcionamento da propaganda política

Art. 13. O núcleo do art. 27-A (repositório público de anúncios político-eleitorais + ferramenta de consulta avançada + coleta sistemática via API) tem paralelo direto no art. 13 do Regulamento europeu, que cria o repositório europeu de anúncios de cariz político em linha, com acesso ao público por meio de um portal único, exigindo que as informações sejam publicadas em formato legível por máquina e permitam consultas com múltiplos critérios; além disso, há retenção de 7 anos e referências a atos de execução da Comissão para padronizar estrutura de dados, metadados, autenticação e uma interface comum de programação de aplicações (API) para possibilitar acesso e agregação de dados (busca e análise) ao público e a terceiros (incluindo serviços de pesquisa). As regras sobre API, metadados e autenticação normalizada aparecem expressamente no n.º 6 do art. 13, com objetivos de permitir acesso público aos avisos de transparência e viabilizar serviços de pesquisa de fácil utilização no portal.

Art. 11 e 12. O conteúdo mínimo que "alimenta" o repositório decorre do art. 12 (o "aviso de transparência" que acompanha cada anúncio), elencando, entre outros, a identificação do patrocinador, montante pago por anúncio e total da campanha, período, referência eleitoral, sumário das técnicas de direcionamento e parâmetros/dados usados, e links para o próprio anúncio no repositório e para o portal do repositório. O art. 11 complementa exigindo rótulo visível ("propaganda política") no próprio anúncio, ligação ao aviso de transparência e metadados que assegurem o vínculo entre ambos. Em termos de atualização, o art. 13 adota a lógica de disponibilidade "desde a primeira publicação" do anúncio, e há uma janela de até 72 horas para quem não seja VLOP/serviço de grande dimensão, o que traduz, na prática, uma exigência de quase tempo real para plataformas maiores e prazo curto para os demais. O §3º do art. 27-A da Resolução do TSE (cumprimento permanente) encontra eco na retenção de 7 anos do repositório (o que sinaliza dever contínuo, para além dos ciclos eleitorais), bem como no desenho de acesso público e perene por portal único.

Já quanto ao art. 28, §1º da Resolução do TSE (comunicação de endereços/canais à Justiça Eleitoral), não há um equivalente europeu direto: o Regulamento disciplina transpa-

rência e direcionamento de propaganda e não cria um cadastro obrigatório de "endereços eletrônicos oficiais" de candidaturas perante autoridade eleitoral. Essa linha de controle de canais fica fora do escopo do Regulamento Europeu (que regula o serviço de propaganda política e seu ecossistema, não a inscrição de "páginas/perfis") - vide escopo e definições do art. 3, focadas no que é "propaganda política" e "anúncio de cariz político".

Por fim, o art. 28, §1-A da Resolução do TSE (excluir dos sistemas de recomendação canais/perfis não comunicados) tampouco tem par europeu específico neste Regulamento. O Regulamento Europeu centra-se em rótulo/aviso, repositório, reporte periódico e regras de targeting/distribuição, inclusive proibições de dados sensíveis e deveres de transparência do direcionamento, mas não impõe um "*downranking* / exclusão" por falta de cadastro do canal; em vez disso, restringe técnicas de direcionamento e exige transparência sobre parâmetros de distribuição, com foco em proteção de dados e integridade do debate.

2.13.5 INTERPRETAÇÃO DO ART. 27-A, I E II, § 3º; ART. 28, §§ 1º E 1º-A (PROPOSTAS)

A leitura integrada organiza-se em três eixos:

Repositório público + ferramenta de consulta (art. 27-A, I e II)

O repositório deve assegurar observabilidade do ecossistema de anúncios. Para cada anúncio político-eleitoral impulsionado: identificador único; campos normalizados (conteúdo criativo e variações; anunciante/pagador e cadeia de intermediação; período; valor e moeda; formatos; canais); critérios de segmentação e exclusões (incluindo "*look-alike*"/expansão algorítmica); e metadados de entrega (impressões, alcance, frequência, tipo de dispositivo e localização apenas em nível agregado compatível com privacidade). A ferramenta de consulta não pode ser um buscador simples: requer API pública estável, documentação, limites razoáveis e exportação em massa, para pesquisa acadêmica, jornalismo investigativo e fiscalização.

Como padrão de qualidade, pode se adotar o modelo europeu: publicação no repositório em até 72 horas após a primeira exibição.

Rótulo visível e informativo (art. 28, §§1º e 1º-A)

A identificação deve ser persistente em todos os pontos de contato (criativo, landing page, repositório e, quando possível, em compartilhamentos), com: a marca "Propaganda Política", o patrocinador e o motivo de exibição (principais parâmetros de direcionamento), além de link direto para a ficha no repositório (chave de correspondência única). A interface não pode degradar ou ocultar o rótulo.

Parâmetros de segmentação e limites (DSA art. 26; Regulamento Europeu art. 18)

A referência a "grupos populacionais (perfilamento)" do art. 27-A poderia espelhar o DSA: além do rótulo, divulgação dos principais parâmetros utilizados (ou evitados) para a veiculação, condição para avaliar microdirecionamento, vieses e alcance. Observa-se a ve-

dação de categorias especiais de dados e a proibição de direcionamento a menores, com filtros preventivos. Em aderência ao DSA, dados pessoais de destinatários não integram o repositório; métricas de entrega devem ser agregadas (p.ex., por município/estado ou faixas amplas). Tudo isso se harmoniza com a LGPD (finalidade, necessidade, segurança e regras para dados sensíveis/crianças e adolescentes).

Auditorias e cooperação (art. 27-A, §3º; OSA).

O §3º concretiza-se com trilhas de auditoria completas (logs de criação/edição/ativação/pausa; alterações de segmentação e orçamento; rejeições e recursos), relatórios periódicos padronizados e mecanismos de entrega de dados sob sigilo à Justiça Eleitoral (e peritos). Esse desenho se alinha ao *record-keeping and review* e aos relatórios de transparência inspirados no OSA, fortalecendo a *accountability* sem ampliar indevidamente a exposição pública de dados pessoais.

Em síntese:

Art. 27-A, I e II, §3º

O que caracteriza um "repositório em tempo real"? "Tempo real" deve ser interpretado como near real-time, ou seja, atualização contínua ou com atraso máximo de até 72 horas, conforme o padrão europeu (art. 13(4) do Regulamento UE 2024/900).

Nível de granularidade dos dados: O repositório deve conter, no mínimo: identificador único do anúncio, conteúdo criativo e variações, anunciante/pagador, período, valor e moeda, formatos, canais, critérios de segmentação e exclusões (inclusive *look-alike*) e metadados de entrega (impressões, alcance, frequência, dispositivo, localização agregada). Deve-se adotar granularidade suficiente para permitir auditoria, mas com dados agregados para proteger privacidade - p.ex., distribuição geográfica por município ou estado, sem microdados pessoais.

Limite da transparência de segmentação e proteção de dados pessoais: A obrigação atinge parâmetros utilizados (ou evitados), categorias de público e critérios de targeting/exclusão, mas não dados individuais. Assim, o provedor deve divulgar estruturas de perfilamento e indicadores agregados de entrega, em conformidade com a LGPD (art. 6º, princípios da finalidade, necessidade e segurança) e com o art. 26(2) e 39(2) do DSA, que veda divulgação de dados pessoais dos destinatários.

Ferramenta "acessível" e de "fácil manejo": Deve possuir interface pública pesquisável, com busca por palavra-chave, anunciante e critérios de segmentação, exportação de relatórios e compatibilidade com acessibilidade (visual, auditiva, mobile). Padrão de referência: art. 39(1) DSA e art. 13(1) e (6) do Regulamento Europeu, que exigem API pública e formatos legíveis por máquina.

Abertura da API: A API deve ser pública, estável e documentada, permitindo acesso a pesquisadores, imprensa, sociedade civil e Justiça Eleitoral. O acesso pode prever limites técnicos (rate limits) e autenticação normalizada, conforme modelo europeu, mas não pode restringir-se à Justiça Eleitoral - sob pena de frustrar o caráter de transparência pública previsto no §3º.

Métricas de confiabilidade e auditabilidade: Devem incluir: (i) Taxa de atualização (percentual de anúncios publicados no prazo de até 48h); (ii)Integridade dos metadados (campos completos, sem omissões); (iii) Logs de criação, edição e ativação/pausa; (iv) Relatórios periódicos de auditoria independente, como previsto no DSA (arts. 24 e 40) e sugerido no OSA (sections 77-78).

Art. 28, §§1º e 1º-A

Consequências jurídicas da não comunicação de canais: Omissão configura descumprimento do art. 28, §1º, podendo gerar sanções eleitorais (p.ex., suspensão de propaganda irregular, multa, enquadramento por publicidade não identificada ou irregular). A ausência de registro autoriza a exclusão desses canais dos resultados de recomendação (art. 28, §1º-A).

Gestão do banco de dados pela Justiça Eleitoral: Deve ter caráter público e verificável, como cadastro oficial de canais eleitorais, porém com proteção de dados pessoais (LGPD). A publicidade deve abranger identificação do canal/perfil e vínculo com candidatura/partido, sem incluir dados sensíveis ou pessoais de administradores.

Impacto da exclusão de canais em sistemas de recomendação: A exclusão limita a visibilidade orgânica, mas visa preservar integridade e rastreabilidade do debate eleitoral, impedindo promoção automática de canais não verificados. Deve-se aplicar o princípio da proporcionalidade, garantindo mecanismos de recurso e revisão (devido processo algorítmico, como no DSA art. 17 e OSA s.72).

Boas práticas internacionais: União Europeia: DSA (art. 27) - transparência dos parâmetros de recomendação e opção de feed não perfilado; Regulamento UE 2024/900 - transparência de targeting e proibição de dados sensíveis; Reino Unido (OSA, s.17) - obriga clareza e consistência sobre tratamento de conteúdos de importância democrática. Essas experiências indicam que mitigação de manipulação algorítmica exige transparência sobre parâmetros, opções de controle do usuário e auditoria independente.

Abrangência da exclusão (impulsionado vs. orgânico): A obrigação de exclusão refere-se apenas aos conteúdos orgânicos de canais não registrados. Anúncios impulsionados permanecem permitidos se contratados conforme a lei e declarados no repositório (art. 27-A).

Compatibilização com neutralidade algorítmica e LGPD: A exclusão é compatível se fundada em obrigação legal e interesse público (art. 7º, II, LGPD), com tratamento limitado a dados necessários para identificação e exclusão de perfis não comunicados. Deve-se garantir transparência dos critérios de recomendação (art. 27 DSA) e controle do usuário, preservando a neutralidade algorítmica e evitando discriminação indevida de candidaturas.

2.13.6 EVIDÊNCIAS E ESTUDOS DE CASO

Caso NetLab UFRJ - “Faturar um Milhão é Fácil: Publicidade Política no TikTok e o Desequilíbrio da Disputa Eleitoral em 2024” (NetLab, 2025): O relatório do NetLab (UFRJ) analisou a circulação de 137 anúncios político-eleitorais sobre Pablo Marçal (PRTB) no TikTok durante as eleições municipais de 2024. Embora a plataforma alegue proibir publicidade política, os anúncios estavam disponíveis em sua Biblioteca de Conteúdo Comercial europeia,

o que evidenciou que campanhas brasileiras foram exibidas a usuários da UE, mas não documentadas no Brasil - devido à ausência de repositório público local. O estudo demonstrou falhas graves de moderação, opacidade na identificação de anunciantes e risco de interferência transnacional, reforçando a importância da implementação efetiva do Art. 27-A da

Resolução TSE 23.732/2024.

Caso G*lobal Witness - "Facebook fails to tackle election disinformation ads ahead of tense Brazilian election" (Global Witness, 2024)*: A ONG *Global Witness* testou os mecanismos de detecção de anúncios políticos no Facebook e no TikTok durante o ciclo eleitoral brasileiro de 2022-2024. Anúncios contendo desinformação explícita e violações às regras eleitorais foram aprovados pelas plataformas, mesmo após revisão manual. O estudo evidenciou que as políticas de transparência autorregulatórias não são suficientes, reforçando a necessidade de repositórios públicos auditáveis, APIs abertas e sanções proporcionais para garantir a integridade eleitoral.

2.13.7 RECOMENDAÇÕES (NORMATIVAS E OPERACIONAIS)

(Normativas) (i) Regulamentar campos mínimos obrigatórios do repositório (espelhando art. 27-A e os campos do DSA art. 39), incluindo parâmetros de segmentação, orçamento, período, criativos e catálogo de versões; (ii) fixar padrões de rótulo (tamanho, posição, persistência, contraste) e chave de consulta para o repositório; (iii) detalhar prazos de publicação (SLA) e retenção; (iv) exigir relatórios periódicos de transparência com métricas padronizadas, inspirados no OSA s. 77-78; v) definir obrigações de registro e revisão compatíveis com OSA s. 23 (inclusive justificativas quando se adotarem medidas alternativas).

(Operacionais – provedores) (i) disponibilizar API pública versionada, com documentação e amostras, e exportação em massa; (ii) manter logs assinados (hash-chain) e trilhas de decisão; (iii) publicar relatórios de auditoria (sumários), além das auditorias internas/externas já previstas no § 3º; (iv) adotar testes A/B de rótulo (usabilidade e memorabilidade); (v) instituir rotas de resposta rápida para requisições da Justiça Eleitoral; (vi) publicar matriz de riscos e planos de mitigação específicos para períodos eleitorais (coerente com o "risks → mitigations" do DSA e com o enfoque do OSA em relatórios).

(Operacionais – autoridade / justiça) (i) definir esquemas de dados oficiais e validadores; (ii) operar repositório espelho (cópias periódicas) para preservação probatória; (iii) estabelecer programa de "pesquisador confiável" com acesso avançado (com salvaguardas de privacidade) nos moldes de acesso regulado previsto no DSA; (iv) criar painéis públicos com indicadores-chave (completude, tempo de exposição, gasto por segmentação) para *accountability*.

Riscos, salvaguardas e direitos

Riscos: (i) "Efeito vitrine" (adversários exploram dados estratégicos do anunciante), (ii) *overblocking* por medo de sanção, (iii) sub-declaração de segmentação (campos "genéricos"), (iv) discriminação via *microtargeting* opaco, (v) riscos de privacidade por granularidade

excessiva de entrega, (vi) assimetria de poder informacional entre plataformas e candidatos pequenos.

Salvaguardas: (i) granularidade agregada de métricas de entrega (para não reidentificar), (ii) distinção entre campos públicos e campos sob sigilo (disponíveis para autoridade), (iii) notificação e motivação quando anúncios forem rejeitados ou rotulados de forma agravada, com meios de recurso claros (alinhado ao espírito do OSA s. 20-21 sobre reporting/complaints), (iv) auditorias independentes e *logs* invioláveis (*record-keeping* do OSA s. 23), v) avaliação de impacto periódica para períodos eleitorais.

Direitos: (i) do eleitor à informação clara e em linguagem acessível (coerente com "*easy to access, easy to use and transparent*" do OSA s. 20/72), (ii) do anunciante à liberdade de expressão e à motivação de medidas restritivas (OSA s. 17 e s. 22), (iii) de candidatos/partidos a tratamento isonômico nos rótulos e na aplicação de políticas (DSA: transparência não discriminatória; OSA s. 17 exige neutralidade quanto a diversidade de opinião).

REFERÊNCIAS

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 dez. 2025.

BRASIL. Supremo Tribunal Federal. Informação à sociedade: RE 1.037.396 (Tema 987) e 1.057.258 (Tema 533) responsabilidade de plataformas digitais por conteúdo de terceiros. Brasília: STF, 2025. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/Informac807a771oa768SociedadeArt19MCI_vRev.pdf. Acesso em: 10 dez. 2025.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 2019. Dispõe sobre propaganda eleitoral. Brasília, DF, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 10 dez. 2025

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 2024. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Brasília, DF, 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 10 dez. 2025.

COMISSÃO EUROPEIA. Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065. Official Journal of the European Union, [S. l.], 2024. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403014. Acesso em: 10 dez. 2025.

GLOBAL WITNESS. Facebook fails to tackle election disinformation ahead of tense Brazilian election. Londres, 2022. Disponível em: https://globalwitness.org/en/campaigns/digital-threats/facebook-fails-to-tackle-election-disinformation-ads-ahead-of-tense-brazilian-election/. Acesso em: 12 dez. 2025.

ÍNDIA. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Índia: Ministry of Electronics and Information Technology, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Acesso em: 10 dez. 2025.

LABORATÓRIO de Estudos de Internet e Redes Sociais (NetLab). Faturar um milhão é fácil: publicidade política no TikTok e o desequilíbrio da disputa eleitoral em 2024. Rio de Janeiro, 2025. Disponível em: https://netlab.eco.ufrj.br/post/faturar-um-milhao. Acesso em: 12 dez. 2025.

REINO UNIDO. Online Safety Act (OSA). Londres, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 10 dez. 2025.

REINO UNIDO. Online Safety Act: explainer. Londres: Gov.uk, [2025?]. Disponível em: https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Bruxelas, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2024/900 do Parlamento Europeu e do Conselho de 13 de março de 2024 sobre a transparência e o direcionamento da propaganda política. União Europeia, 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202400900. Acesso em: 11 dez. 2025.

2.14 VEDAÇÃO À SIMULAÇÃO DE INTERLOCUÇÃO COM A PESSOA CANDIDATA OU OUTRA PESSOA REAL E DEVER DE INFORMAÇÃO QUANTO AO USO DE CHATBOTS, AVATARES E CONTEÚDOS SINTÉTICOS COMO ARTIFÍCIO PARA INTERMEDIAR A COMUNICAÇÃO DE CAMPANHA COM PESSOAS NATURAIS (ART. 9º-B, §3º)

Elaine Gomes dos Santos

> **Art. 9º-B. A utilização na propaganda eleitoral, em qualquer modalidade, de conteúdo sintético multimídia gerado por meio de inteligência artificial para criar, substituir, omitir, mesclar ou alterar a velocidade ou sobrepor imagens ou sons impõe ao responsável pela propaganda o dever de informar, de modo explícito, destacado e acessível que o conteúdo foi fabricado ou manipulado e a tecnologia utilizada. (Incluído pela Resolução n.º 23.732/2024)**
> **[...]**
> **§ 3º O uso de chatbots, avatares e conteúdos sintéticos como artifício para intermediar a comunicação de campanha com pessoas naturais submete-se ao disposto no caput deste artigo, vedada qualquer simulação de interlocução com a pessoa candidata ou outra pessoa real. (Incluído pela Resolução n.º 23.732/2024)**

21.4.1 VISÃO GERAL E OBJETIVOS

Objetivo: realizar análise comparada do §3º do art. 9º-B, da Resolução n.º 23.610/2024 do Tribunal Superior Eleitoral, com eventuais obrigações previstas em outras jurisdições.

Guia de perguntas:

- Sobre o §3º do art. 9º-B:
- Quais são as semelhanças e diferenças dos normativos do Brasil, União Europeia, Reino Unido e Índia em matéria de simulação de interlocução de um candidato em campanha com uma pessoa natural?

21.4.2 BASE NORMATIVA (BRASIL)

Resolução n.º 23.610/2024, do Tribunal Superior Eleitoral

Sobre o §3º do art. 9º-B: a previsão, com um dois objetivos simples e diretos, busca: (i) garantir ao destinatário que quando houver o uso de *chatbot*, avatar(es) e conteúdo(s) sintético(s) em comunicação de campanha a mesma deve estar acompanhada da informação explícita, destacada e acessível de que eles ou seus outputs são conteúdos fabricados ou manipulados por alguma tecnologia; e, (ii) que não é permitida a simulação de interlocução com o(a) candidato(a) quando não se tratar do(da) próprio(a) na outra ponta do processo de comunicação (Brasil, 2019).

21.4.3 METODOLOGIA DE *BENCHMARKING*

Seleção de jurisdições: UE (DSA), Reino Unido (OSA) e Índia (*IT Rules*).

Unidade de comparação: Sobre o §3º do art.9º-B: existe, nos normativos, a proibição de simulação de interlocução de um candidato em campanha com uma pessoa natural?

Critério	União Europeia - *Digital Service Act* (DSA)	Reino Unido - *Online Safety Act* (OSA)	Índia – *IT Rules*
Proibição de simulação de interlocução de um candidato em campanha com uma pessoa natural?	Artigo 25.º Conceção e organização da interface em linha 1. Os fornecedores de plataformas em linha não podem conceber, organizar ou explorar as suas interfaces em linha de forma a enganar ou manipular os destinatários do seu serviço ou de forma a distorcer ou prejudicar substancialmente de outro modo a capacidade dos destinatários do seu serviço de tomarem decisões livres e informadas [...] Artigo 34.º Avaliação dos riscos 1. Os fornecedores de plataformas em linha de muito grande dimensão e de motores de pesquisa em linha de muito grande dimensão identificam, analisam e avaliam diligentemente todos os riscos sistémicos na União decorrentes da conceção ou do funcionamento do seu serviço e dos seus sistemas relacionados, incluindo os sistemas algorítmicos, ou decorrentes da utilização dos seus serviços. Efetuam as avaliações de risco até à data de aplicação referida no artigo 33.º, n.º 6, segundo parágrafo, e, posteriormente, pelo menos uma vez por ano, e, em qualquer caso, antes da introdução de funcionalidades suscetíveis de terem um impacto crítico nos riscos identificados nos termos do presente artigo. Esta avaliação dos riscos incidirá especificamente nos seus serviços, será proporcionada aos riscos sistémicos, tendo em conta a sua gravidade e probabilidade, e incluirá os seguintes riscos sistémicos: [...] c) Quaisquer efeitos negativos reais ou previsíveis no discurso cívico e nos processos eleitorais, bem como na segurança pública.	Não prevê.	Part II – Due Diligence by Intermediaries and Grievance Redressal Mechanism 3. Due diligence (1) Due diligence by an intermediary: [...] (b) the intermediary shall inform its rules and regulations, privacy policy and user agreement to the user in English or any language specified in the Eighth Schedule to the Constitution in the language of his choice and shall make reasonable efforts by itself, and to cause the users of its computer resource to not host, display, upload, modify, publish, transmit, store, update or share any information that, [...] (v) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any misinformation or information which is patently false and untrue or misleading in nature or, in respect of any business of the Central Government, is identified as fake or false or misleading by such fact check unit of the Central Government as the Ministry may, by notification published in the Official Gazette, specify;

2.14.4 *BENCHMARK* INTERNACIONAL (SÍNTESE COMPARATIVA)

União Europeia (DSA): Não prevê proibição expressa, mas proíbe condutas próximas sob fundamentos mais amplos. A normativa brasileira se atenta a proibir um usuário a simular uma interlocução não real sem aviso, enquanto o art. 25.º do DSA proíbe os fornecedores de plataformas – logo, não estamos falando do mesmo sujeito – a permitir que as suas interfaces possibilitem enganar ou manipular os destinatários. Da mesma forma, temos o art. 34.º, n.º 1, alínea "c" prevendo que efeitos negativos reais ou previsíveis aos processos eleitorais são considerados como um risco sistêmico. Logo, em um plano de fundo comum entre os normativos, temos uma proibição de manipulação de interface e a preocupação de efeitos negativos em eleições.

Reino Unido (OSA): Não há previsão expressa específica.

Índia (*IT Rules*): Não possui proibição expressa específica, porém prevê que o intermediário deve despender esforços para não "*deceives*" ou "*misleads*" o destinatário sobre a origem da mensagem. Em um plano de fundo comum, tanto a norma brasileira como esta proíbem o ato de enganar o destinatário sobre quem dá origem ao conteúdo das mensagens em uma comunicação.

2.14.5 INTERPRETAÇÃO DO §3º DO ART. 9º-B

O §3º do art. 9º-B deve ser interpretado como uma norma de proteção reforçada à autenticidade da comunicação eleitoral, voltada a impedir que tecnologias de IA sejam utilizadas para simular interação humana ou personalização enganosa entre candidaturas e eleitoras(es). Ao submeter o uso de *chatbots*, avatares e conteúdos sintéticos às mesmas exigências de transparência do *caput* (isto é, aviso explícito, destacado e acessível de que o conteúdo é artificial) o dispositivo busca preservar a integridade do discurso político e evitar a criação de vínculos emocionais ou de confiança baseados em falsificação identitária. A vedação à "simulação de interlocução" deve ser compreendida de modo amplo, abrangendo tanto a imitação direta da candidata ou candidato quanto o uso de personagens ou assistentes virtuais que aparentem representar pessoas reais sem aviso claro de sua natureza sintética. A norma brasileira impõe um dever positivo de rotulagem e design responsável, exigindo que a mediação automatizada seja sempre identificável e auditável. Assim, o §3º funciona como um instrumento de *accountability* comunicacional, que não proíbe o uso de Inteligência Artificial (IA) em campanhas, mas condiciona sua legitimidade à observância de padrões de transparência, controle humano e impossibilidade de engano quanto à identidade ou autenticidade da interlocução.

2.14.6 EVIDÊNCIAS E ESTUDOS DE CASO

Caso da ferramenta *Lex* do candidato à Câmara Municipal de São Paulo pela Rede, Pedro Markun: o candidato teve seu chat de inteligência artificial bloqueado pela Meta em

11 de setembro de 2024. De acordo com a empresa, a conta "foi banida pelo sistema de integridade do WhatsApp por ferir a política do aplicativo que explicitamente proíbe o uso da Plataforma do WhatsApp Business por políticos ou partidos, candidatos e campanhas políticas". De acordo com o candidato, um cidadão "pode perguntar para a *Lex* sobre projetos de lei que afetam seu bairro, por exemplo, e ela responderá de forma clara, permitindo que ele acompanhe, reclame e cobre ações". Markun defende que o bloqueio seria uma censura. Apesar do bloqueio pela Meta não ter sido realizado com base no parágrafo do artigo da resolução do Tribunal Superior Eleitoral, o caso releva uma segunda camada importante para o tema: que as diretrizes das plataformas podem atuar como impeditivos do uso de ferramentas de IA por candidatos políticos. Pedro Markun, ou "Pedro da IA" como se identificava nas redes sociais, não se elegeu nas últimas eleições. Em pesquisa ao perfil oficial do Instagram é possível identificar que a *Lex* também funcionava no aplicativo Telegram. Porém, ao testar se o chat ainda respondia no aplicativo, não houve retorno da ferramenta.

2.14.7 RECOMENDAÇÕES (NORMATIVAS E OPERACIONAIS)

Definir, por meio de resolução que atualizaria a redação da Resolução n.º 23.610/2019, o que configura e não configura uma "comunicação de campanha".

Definir, por meio de resolução que atualizaria a redação da Resolução n.º 23.610/2019, o que configura e não configura uma "simulação de interlocução".

2.14.8. RISCOS, SALVAGUARDAS E DIREITOS

Riscos

Simulação enganosa e manipulação emocional: o principal risco é o uso de chatbots e avatares que simulam interação humana de forma convincente, induzindo o eleitor a acreditar que conversa com a própria candidata ou com pessoa real. Essa prática gera falsa percepção de proximidade e confiança, com alto potencial persuasivo e distorção da autonomia do voto.

Desinformação automatizada e amplificação algorítmica: sistemas de IA podem disseminar conteúdos descontextualizados ou incorretos com aparência de veracidade, reproduzindo padrões de discurso e emoção humanos. O risco é agravado pela escala automatizada, que permite replicar interações artificiais com milhares de eleitores simultaneamente.

Falsificação identitária e erosão da autenticidade do debate: o uso de avatares hiper-realistas ou vozes sintéticas pode resultar na falsificação de identidade de candidatos, apoiadores ou figuras públicas, comprometendo a confiança nas comunicações oficiais e no ecossistema informacional eleitoral.

Assimetria de informação e opacidade técnica: a falta de transparência sobre o funcionamento, treinamento e controle humano das ferramentas de IA dificulta a detecção de irregularidades, fragilizando a fiscalização eleitoral e favorecendo campanhas com maior poder tecnológico.

Violação de dados pessoais e sensíveis: chatbots eleitorais podem processar dados de perfil, preferências políticas ou emocionais de eleitores para personalizar respostas, criando riscos de microdirecionamento político e à integridade do voto.

Risco de sobre-regulação ou autocensura tecnológica: medidas excessivamente restritivas podem desincentivar o uso legítimo de ferramentas de IA para fins informativos e educativos, prejudicando a inovação democrática e a liberdade de expressão.

Salvaguardas

Rotulagem visível e persistente: todo conteúdo ou interação automatizada deve conter aviso claro, contínuo e perceptível sobre sua natureza sintética. Esse aviso deve ser uma frase cuja clareza encontre todos os públicos, principalmente os vulneráveis.

Supervisão humana obrigatória: o uso de chatbots ou avatares eleitorais deve ser condicionado à supervisão e revisão humanas. Cada conteúdo ou interação deve ter um responsável identificado, capaz de intervir, corrigir erros e responder pela comunicação. Contudo, esta é uma sugestão que também encontra dificuldade prática. Se toda comunicação precisar passar por um humano antes de ser enviada, podemos ter uma demora excessiva na comunicação, gerando desinteresse nos indivíduos interessados em utilizá-la. Por outro lado, se a revisão ocorrer após o envio da mensagem, com um prazo máximo curto para o procedimento ser realizado, também podemos ter o lado ruim da ferramenta, como o caso de envio de uma informação inverídica. Um meio termo possível é a verificação posterior acompanhada de um aviso em cada mensagem de que a informação será verificada no prazo informado.

Dessa forma, a utilidade da ferramenta é mantida e se cria uma consciência no destinatário da mensagem que uma determinada informação possui um prazo para ser checada. Assim, também teríamos a criação dessa responsabilidade específica para os interessados em utilizar a ferramenta.

Transparência funcional e documentação técnica mínima: exigir que cada sistema automatizado mantenha um documento único contendo o tipo de IA utilizada, fontes de dados, parâmetros de personalização e política de revisão humana para ser consultada pela justiça eleitoral quando solicitado.

Auditoria independente e mecanismos de denúncia: prever auditorias periódicas de conformidade conduzidas por peritos independentes credenciados pelo TSE, além de canal público de denúncia para interações artificiais enganosas ou não rotuladas.

Direitos

Direito do eleitor à autenticidade comunicacional: o eleitor tem o direito de saber com quem está interagindo, sendo informado de forma clara e destacada quando a comunicação é mediada por IA. Esse direito decorre do princípio da boa-fé e da transparência (art.

6º, VI, LGPD) e integra a autodeterminação informacional eleitoral.

Direito à informação clara e acessível: as mensagens automatizadas devem ser redigidas em linguagem simples, com rótulos visuais e auditivos acessíveis a pessoas com deficiência, garantindo acessibilidade comunicacional.

Direito à proteção de dados e à privacidade política: nenhum sistema de IA eleitoral pode coletar, cruzar ou inferir dados de preferências políticas sem consentimento explícito e informado. O eleitor tem direito a conhecer as categorias de dados tratados e a finalidade do uso.

Direito à revisão e à reparação: em caso de dano reputacional ou desinformação decorrente de uso irregular de IA (como falsificação de imagem ou voz), o candidato e o eleitor têm direito à correção célere, à retratação pública e à responsabilização do agente infrator.

REFERÊNCIAS

AMADO, Guilherme; MOURA, Athos. Meta bloqueia chat de inteligência artificial de candidato em SP. Metrópoles, Brasília, 2024. Coluna Guilherme Amado. Disponível em: https://www.metropoles.com/colunas/guilherme-amado/meta-bloqueia-chat-de-inteligencia-artificial-de-candidato-em-sp. Acesso em: 12 dez. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 dez. 2025.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 2019. Dispõe sobre propaganda eleitoral. Brasília, DF, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 10 dez. 2025

ÍNDIA. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Índia: Ministry of Electronics and Information Technology, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Acesso em: 10 dez. 2025.

MARKUN, Pedro. A LEX agora está no Telegram! [Postagem]. Instagram, 26 set. 2024. Disponível em: https://www.instagram.com/p/DAYnTcdODjK/. Acesso em: 12 dez. 2025.

MARKUN, Pedro. A LEX segue sendo bloqueada no Whatsapp pela Meta! [Postagem]. Instagram, 28 set. 2024. Disponível em: https://www.instagram.com/p/DAeXoMHS286/. Acesso em: 12 dez. 2025.

MONITCHELE, Marília. Conheça o homem que quer eleger uma IA como vereadora e incomodou a Meta. Veja, São Paulo, 2024. Seção Ideias. Disponível em: https://veja.abril.com.br/ideias/conheca-o-homem-que-quer-eleger-uma-ia-como-vereadora-e-incomodou-a-meta/. Acesso em: 12 dez. 2025.

REINO UNIDO. Online Safety Act (OSA). Londres, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Bruxelas, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. Acesso em: 10 dez. 2025.

2.15 VEDAÇÃO AO IMPULSIONAMENTO DE CONTEÚDO FALSO OU DESCONTEXTUALIZADO (ART. 9º-D, §§ 3º E 5º)

Thiago Marcílio

Art. 9º-D. [...]
§ 3º A Justiça Eleitoral poderá determinar que o provedor de aplicação veicule, por impulsionamento e sem custos, o conteúdo informativo que elucide fato notoriamente inverídico ou gravemente descontextualizado antes impulsionado de forma irregular, nos mesmos moldes e alcance da contratação.
§ 5º As ordens para remoção de conteúdo, suspensão de perfis, fornecimento de dados ou outras medidas determinadas pelas autoridades judiciárias, no exercício do poder de polícia ou nas ações eleitorais, observarão o disposto nesta Resolução e na Res.-TSE n.º 23.608/2019, cabendo aos provedores de aplicação cumpri-las e, se o integral atendimento da ordem depender de dados complementares, informar, com objetividade, no prazo de cumprimento, quais dados devem ser fornecidos.

2.15.1 VISÃO GERAL E OBJETIVOS

Objetivo: analisar a extensão e aplicação da resposta ao impulsionamento de conteúdos vedados notoriamente inverídicos ou gravemente descontextualizados, com ênfase nos conteúdos ofensivos de cunho sexual, conforme o Art. 9º-D, §§ 3º e 5º da Resolução TSE 23.732/2024, e compará-la com modelos regulatórios estrangeiros sobre integridade informacional em campanhas eleitorais.

Objetivo secundário: propor parâmetros técnicos e cronograma de implementação para garantir que plataformas, partidos e candidatos observem o art. 9º-D de forma efetiva e proporcional.

Perguntas-guia:

- Quais são os critérios normativos e operacionais para caracterizar "fato notoriamente inverídico" e "gravemente descontextualizado"?
- Qual a natureza jurídica do dever de vedação: preventiva, corretiva ou sancionatória?
- Como equilibrar integridade eleitoral e liberdade de expressão? Incluir notas sobre o PLP 112, que está no Senado.
- Que mecanismos de auditoria e transparência podem assegurar o cumprimento da vedação?

2.15.2 BASE NORMATIVA (BRASIL)

Norma principal:

Resolução TSE n.º 23.732/2024, art. 9º-D, caput e §§ 3–5º.

Caput: veda o impulsionamento de conteúdo que veicule fato notoriamente inverídico ou gravemente descontextualizado capaz de comprometer a integridade do processo eleitoral.

§ 3º A Justiça Eleitoral poderá determinar que o provedor de aplicação veicule, por impulsionamento e sem custos, o conteúdo informativo que elucide fato notoriamente inverídico ou gravemente descontextualizado antes impulsionado de forma irregular, nos mesmos moldes e alcance da contratação.

5º: As ordens para remoção de conteúdo, suspensão de perfis, fornecimento de dados ou outras medidas determinadas pelas autoridades judiciárias, no exercício do poder de polícia ou nas ações eleitorais, observarão o disposto nesta Resolução e na Res.-TSE n.º 23.608/2019, cabendo aos provedores de aplicação cumpri-las e, se o integral atendimento da ordem depender de dados complementares, informar, com objetividade, no prazo de cumprimento, quais dados devem ser fornecidos." (NR)

Legislação correlata:

- Lei 9.504/1997, arts. 57-B a 57-F (propaganda eleitoral na internet);
- Lei 12.965/2014 (Marco Civil da Internet);
- Lei 13.709/2018 (LGPD) – proteção de dados de eleitores;
- Código Eleitoral, art. 243, IX – vedação à divulgação de fatos sabidamente inverídicos;
- ECA Digital, 15.211/2025 – proteção da infância a adolescência no ambiente digital
- Jurisprudência STF/STJ: RE 1.037.396 (STF – responsabilidade de provedores pós-notificação); ADI 7261 (STF – combate à desinformação no pleito 2022).

Contexto regulatório:

A Resolução 23.732 integra uma resposta institucional à intensificação de desinformação em campanhas digitais. O art. 9º-D consolida o entendimento do TSE como autoridade de integridade informacional, fixando um dever de cuidado ampliado a partidos, candidatos, provedores e impulsionadores.

2.15.3 METODOLOGIA DE *BENCHMARKING*

Seleção de jurisdições comparadas:

- **União Europeia:** *Digital Services Act* (DSA - Reg. 2022/2065);
- **Reino Unido:** *Online Safety Act* (2023) e códigos da Ofcom;
- **Índia:** *IT Rules 2021 e Model Code of Conduct* (ECI).

Critérios de comparação:

- Tipificação de conteúdo proibido;
- Mecanismos de detecção e bloqueio preventivo;
- Fluxo de resposta (tempo máximo para remoção ou rótulo);
- Garantias de liberdade de expressão e recurso;
- Transparência dos anúncios e repositórios públicos;
- Integração com autoridades eleitorais;
- Governança interna e auditorias de risco.

Justificativa: a amostra abrange modelos de democracia consolidada (UE, RU) e do Sul Global (Índia), permitindo avaliar tanto arcabouços de compliance quanto desafios de enforcement em contextos de alta polarização e baixa capacidade institucional.

2.15.4 *BENCHMARK* INTERNACIONAL (SÍNTESE COMPARATIVA)

Jurisdição	Dispositivo análogo ao caput (vedar/mitigar impulsionamento de desinformação eleitoral)	Dispositivo análogo ao § 3º (ordem para veicular conteúdo corretivo por destaque/ impulsionamento)	Dispositivo análogo ao § 5º (cumprimento de ordens: remoção, dados etc.	Observações
União Europeia – DSA	DSA arts. 34-35 (avaliação e mitigação de riscos sistêmicos, incluindo riscos a processos eleitorais, com medidas como redução de alcance, rotulagem, ajustes de recomendação e desmonetização) (Atos Digitais da UE).	Sem previsão explícita de "impulsionamento corretivo"; o mais próximo: art. 36 (mecanismo de resposta a crises) que pode exigir dar proeminência a informações oficiais em situações excepcionais; e orientações da Comissão para eleições (VLOPs) que pedem elevar conteúdos de fontes confiáveis em períodos eleitorais (Atos Digitais da UE).	DSA art. 9 (ordens para atuar contra conteúdo ilegal) e art. 10 (ordens para fornecer informações): dever de cumprir e informar efeitos, requisitos formais e ponto de contato; transparência ao usuário afetado (Atos Digitais da UE).	O Código de Práticas sobre Desinformação (2022) pode ser usado como medida de mitigação sob o DSA; não cria dever de "contrapropaganda paga", mas apoia de-amplificação e transparência de anúncios (Estratégia Digital Europeia).
União Europeia – TTPA (Reg. 2024/900	Regras de transparência e segmentação de publicidade política, limitando direcionamento e exigindo rótulos/ arquivos de anúncios, o que restringe o uso de impulsionamento opaco em campanhas; aplicável integralmente a partir de out. 2025 (EUR-Lex).	Sem ordem de "impulsionamento corretivo"; o TTPA atua via transparência/ limitação de targeting e não por contramensagem imposta (EUR-Lex).	Sem canal próprio de ordens; combina-se com DSA art. 9-10 para ordens e fiscalização (autoridades nacionais/ Comissão) (Atos Digitais da UE).	Plataformas anunciaram suspensão de anúncios políticos na UE por dificuldades de conformidade ao TTPA, o que impacta diretamente o impulsionamento eleitoral pago (Reuters).

Reino Unido – *Online Safety Act* (OSA) + *Ofcom Code*	Deveres de segurança para reduzir risco e tirar do ar conteúdo ilegal; a Ofcom detalha, em códigos de prática, medidas sobre moderação, anúncios/recomendação e governança, afetando amplificação/impulsionamento de conteúdos nocivos (inclusive em contextos eleitorais conforme riscos) (Gov.UK).	Não há previsão expressa para forçar veiculação de conteúdo corretivo por impulsionamento; a Ofcom pode exigir sistemas e processos (p. ex., dar destaque a informações confiáveis via design), mas não contrapropaganda paga (www.ofcom.org.uk).	Poderes da Ofcom para emitir notices (informação, cumprimento, uso de tecnologia) e impor sanções por descumprimento dos deveres -funcionalmente análogo à exigência de cumprir ordens administrativas/judiciais (Legislação do Reino Unido).	A implementação é regulatória por códigos (2024-2025), o que permite calibrar exigências para períodos eleitorais via guidance setorial (Gov.UK).
Índia – *IT Rules* 2021 (atualizadas)	Rule 3(1) (due diligence) e Rule 4(3) (rotulagem clara de conteúdo patrocinado/"advertised/ sponsored"); coordenação com ECI durante eleições (SOPs de 2024) reforça remoção rápida de conteúdos eleitorais falsos; impacto direto sobre impulsionamento de peças enganosas.	Não há figura de "impulsionamento corretivo"; as medidas concentram-se em remoção/rotulagem e comunicações oficiais da ECI para correção pública (Eleições Lokshabha 2024).	Rule 3(1)(a)(ii): intermediários devem receber e acatar ordens do governo/ autoridades ou tribunais; Rule 4(2): identificação do first originator mediante ordem; prazos rápidos para certos conteúdos (p.ex., 24h).	

Síntese: há convergência global na proibição do financiamento e amplificação de desinformação eleitoral, ainda que com graus diversos de *enforcement*. O modelo brasileiro – art. 9º-D – alinha-se à tendência europeia de *due diligence* eleitoral, mas carece de métricas operacionais de cumprimento e de relatórios públicos.

Dispositivos análogos ao art. 9º-D, I (termos e políticas de conteúdos):

Jurisdição	Instrumento central	Dispositivos análogos ao art. 9º-D, I (termos e políticas de conteúdo	Deveres complementares (moderação/ transparência	Notas p/ contexto eleitoral
União Europeia – DSA	Reg. (UE) 2022/2065 (DSA)	Art. 14: termos e condições transparentes; publicação nas línguas oficiais dos países atendidos; aplicação objetiva e não discriminatória.	Art. 16 (notice & action); Art. 17 (statement of reasons); Art. 15 (relatórios de transparência); Arts. 34-35 (VLOPs: avaliação e mitigação de riscos sistêmicos, incluindo desinformação).	Diretrizes eleitorais sob o DSA orientam medidas de mitigação (dar proeminência a fontes oficiais, ajustes de recomendação) em períodos eleitorais.

UE – Reg. de Transparência e Direcionamento de Publicidade Política (TTPA)	Reg. (UE) 2024/900	Requer políticas internas para rotulagem clara, repositórios e governança de anúncios políticos (transparência e controle de targeting).	Interage com o DSA (ordens e supervisão); aplicação plena a partir de out/2025.	Pressiona plataformas a rever políticas de anúncios políticos (algumas anunciaram suspensão na UE).
Reino Unido – *Online Safety Act* (OSA)	*Online Safety Act* 2023 + Ofcom Codes/	Deveres de ter e aplicar termos de serviço (inclui definição legal de "terms of service" – s.236) e sistemas/processos para reduzir riscos; categorised services têm obrigações adicionais sobre termos e user empowerment.	Cap. 5: s.77-s.78 (transparency reports); Ofcom emite códigos de prática com medidas de moderação/execução; implementação em fases.	Ofcom publicou guias e cronograma de conformidade; códigos calibram exigências para períodos sensíveis.
Índia – *IT Rules* 2021	Information Technology (Intermediary Guidelines & Digital Media Ethics Code) Rules 2021 (atualizadas)	Rule 3(1)(a)-(b): publicar regras/termos de serviço e informar o que é proibido; dever de aplicação; mecanismos de queixa e prazos.	Rule 3(2) (prazo de 24h/15 dias p/ queixas); Rule 4 (deveres adicionais p/ grandes plataformas); GAC (instância recursal).	Em eleições, a ECI aciona SOPs para remoção rápida e coordenação com plataformas.
Alemanha – NetzDG	Netzwerkdurchsetzungsgesetz (NetzDG)	Não regula "termos" em si, mas obriga procedimento eficaz e transparente para queixas - na prática, exige políticas de conteúdo claras e aplicadas.	§ 3: remoção em 24h (manif. ilícito) ou 7 dias; § 2: relatórios semestrais; agentes de contato na Alemanha; diretrizes de multas.	Serve como "piso" de execução e transparência para políticas de conteúdo.

2.15.5 PROPOSTA DE INTERPRETAÇÃO DO ART. 9º-D, I (DEVERES E ALCANCE)

O § 3º do art. 9º-D da Resolução TSE n.º 23.732/2024 permite que a Justiça Eleitoral determine o impulsionamento gratuito de conteúdo corretivo, o dispositivo busca restabelecer a simetria comunicacional rompida pela disseminação de fatos notoriamente inverídicos ou gravemente descontextualizados. Trata-se de uma medida de natureza reparatória e pedagógica, não punitiva, cuja finalidade é reequilibrar o ambiente de deliberação pública em contextos de dano informacional relevante. O dispositivo concretiza o princípio do reequilíbrio informacional eleitoral, segundo o qual o Estado pode, de forma proporcional e limitada, atuar para restaurar o direito coletivo à verdade factual quando a desinformação impulsionada ameaça à integridade do processo democrático.

A expressão "nos mesmos moldes e alcance da contratação" indica que o impulsionamento corretivo deve reproduzir as condições técnicas originais do anúncio irregular - mesma plataforma, segmentação, duração e amplitude de alcance - de modo a compensar a distorção gerada pelo uso indevido de recursos de impulsionamento. Ao impor a veiculação "sem custos", o TSE reforça o dever de cooperação e diligência das plataformas digitais, que passam a ser corresponsáveis pela recomposição da integridade informacional. O conteúdo a ser impulsionado, por sua vez, deve ter caráter meramente informativo, destinado a esclarecer o público, e não a promover qualquer candidato ou partido. Essa obrigação, que encontra paralelo no art. 36 do *Digital Services Act* da União Europeia - que autoriza dar proeminência a informações oficiais em situações de crise -, aproxima o modelo brasileiro das diretrizes europeias de mitigação de riscos sistêmicos à integridade eleitoral, preservando a liberdade de expressão e evitando censura prévia.

Já o § 5º do mesmo artigo consolida o dever de cooperação técnica entre as plataformas e a Justiça Eleitoral, determinando que ordens de remoção de conteúdo, suspensão de perfis e fornecimento de dados sejam cumpridas de forma objetiva e tempestiva. O dispositivo traduz uma obrigação de diligência digital compatível com os arts. 9 e 10 do *Digital Services Act* e com as Rules 3 e 4 do regulamento indiano *IT Rules* 2021, que impõem prazos curtos e respostas verificáveis a determinações judiciais. Ao exigir que o provedor informe, dentro do prazo, quais dados complementares são necessários ao integral cumprimento da ordem, o TSE institucionaliza uma forma de boa-fé processual aplicada ao ambiente digital: a plataforma deve responder tecnicamente, indicando o que é possível realizar, o que depende de informações adicionais e quais limitações técnicas existem, assegurando transparência e rastreabilidade.

Quanto ao inciso I do art. 9º-D da Resolução TSE n.º 23.732/2024 transforma um dever genérico de moderação em uma obrigação específica de governança informacional. Ao exigir que os provedores de aplicação elaborem e apliquem termos de uso e políticas de conteúdo compatíveis com o objetivo de impedir ou reduzir a circulação de informações notoriamente falsas ou gravemente descontextualizadas, o dispositivo vincula as plataformas a um padrão verificável de diligência e transparência durante o processo eleitoral.

Essa obrigação não se limita à publicação de regras formais, mas abrange sua efetiva aplicação, especialmente em períodos de campanha. As plataformas devem demonstrar mecanismos operacionais - como canais de denúncia, revisão de conteúdo, restrição a impulsionamentos irregulares, relatórios de transparência e cooperação com a Justiça Eleitoral - capazes de dar concretude ao dever previsto.

A estrutura desse dever segue a lógica descrita por José Casalta Nabais em "O Dever Fundamental de Pagar Impostos" (1998) e em estudos posteriores sobre a teoria dos deveres fundamentais. Para Nabais, os deveres públicos não são meros limites aos direitos, mas instrumentos de realização dos próprios direitos fundamentais, sendo organizados segundo três dimensões:

- deveres primários, que impõem condutas positivas necessárias à preservação de bens constitucionalmente relevantes;
- deveres secundários ou de concretização, que especificam o conteúdo do dever primário por meio de normas infraconstitucionais; e
- deveres instrumentais, que garantem a efetividade prática desses deveres por meio de mecanismos procedimentais e de fiscalização.

Sob essa ótica, o art. 9º-D, I, concretiza um dever primário de proteção da integridade eleitoral, transformando-o em dever secundário aplicável às plataformas, que devem estruturar seus próprios instrumentos de prevenção e resposta à desinformação. Ao mesmo tempo, cria deveres instrumentais de execução - como relatórios de transparência, revisão de conteúdo e cooperação técnica com a Justiça Eleitoral - que asseguram a efetividade do dever originário.

A interpretação deve seguir o princípio da responsabilidade compartilhada pela integridade informacional, segundo o qual o Estado define parâmetros normativos e as plataformas executam medidas proporcionais de mitigação de risco. Essa leitura aproxima o modelo brasileiro de instrumentos internacionais como o art. 14 do *Digital Services Act* (UE), que exige a aplicação diligente e transparente dos termos de serviço, e das *IT Rules* 2021 da Índia, que impõem regras claras e mecanismos de contestação.

Portanto, o art. 9º-D, I, deve ser compreendido como um comando que operacionaliza a moderação preventiva e auditável, convertendo o dever abstrato de moderação em obrigação concreta de governança, com critérios de proporcionalidade, publicidade e prestação de contas voltados à proteção da integridade do processo eleitoral.

2.15.6 EVIDÊNCIAS E ESTUDOS DE CASO

Eleições Brasil 2022 (TSE): casos de impulsionamento indevido identificados em relatórios da Justiça Eleitoral (Google Ads, Meta Ad Library); remoções em até 48 h reduziram alcance de desinformação.

Eleições EUA 2020: Twitter e Meta suspenderam anúncios políticos durante período crítico; relatórios mostram queda de propagação de falsidades sobre votação por correio. Eleições Índia 2024: uso de IA generativa em campanhas motivou regras de rotulagem e sanções a impulsionadores de conteúdo falso.

A aplicação dos §§ 3º e 5º do art. 9º-D encontra suporte em experiências recentes no Brasil e no exterior que demonstram a viabilidade de mecanismos de correção informacional e de cooperação técnica entre plataformas e autoridades eleitorais.

No contexto brasileiro, o Programa Permanente de Enfrentamento à Desinformação

(PPED) do TSE, iniciado em 2019, consolidou práticas de checagem institucional, comunicação oficial e resposta rápida em parceria com plataformas digitais. Durante as eleições de 2022, o Tribunal determinou a retirada de impulsionamentos irregulares e publicou mensagens corretivas sobre o funcionamento das urnas e datas de votação, experiências que inspiram o modelo de impulsionamento corretivo gratuito previsto no § 3º. Essas ações foram operacionalizadas com base em convênios que já preveem canais diretos de notificação e cumprimento de ordens, o que antecipa o espírito de cooperação técnica do § 5º.

No plano internacional, o *Digital Services Act* da União Europeia (arts. 9, 10 e 36) estabelece deveres análogos: as plataformas devem cumprir ordens judiciais e administrativas e podem ser obrigadas a dar proeminência a informações oficiais durante crises, inclusive em períodos eleitorais. As orientações eleitorais da Comissão Europeia (2024) reforçam essa prática ao exigir mitigação de riscos de desinformação e destaque de fontes verificadas.

Na Índia, as *IT Rules* 2021 impõem aos intermediários a remoção em 24 horas de conteúdo falso eleitoral e o fornecimento célere de dados às autoridades, enquanto na Alemanha o NetzDG prevê a remoção em 24 horas de conteúdos manifestamente ilegais e relatórios semestrais de conformidade.

2.15.7 RECOMENDAÇÕES (NORMATIVAS E OPERACIONAIS)

Nível	Medida	Prazo sugerido	Responsáve
1	Revisão automática de conteúdo patrocinado por termos eleitorais sensíveis	Permanente	Plataforma
2	Suspensão imediata de impulsionamento após notificação ou identificação interna	≤ 24 h	Plataforma/ contratante
3	Relatório público trimestral sobre impulsionamentos bloqueados ou rotulados	A cada 3 meses (quinzenal em ano eleitoral)	Plataforma
4	Avaliação de impacto da desinformação em campanhas digitais (AII-Eleitoral)	Anual / eleições	Partidos e provedores
5	Canal direto com o TSE para alertas de alto risco	Contínuo	Provedor principal

Cronograma factível (2026):

- 1º trimestre 2026: publicação de guia técnico pelo TSE; formação de grupo de trabalho com plataformas;
- 2º trimestre 2026: implantação piloto de sistema de monitoramento em tempo real;
- 3º trimestre 2026: testes de resposta rápida e auditorias externas;
- Eleições 2026: aplicação plena das obrigações do art. 9º-D.

2.15.8 RISCOS, SALVAGUARDAS E DIREITOS

Liberdade de expressão: evitar remoções automáticas; priorizar rotulagem e desmonetização quando não houver ilícito manifesta.

Devido processo: garantir aviso ao impulsionador e direito de recurso interno (DSA art. 17).

Proporcionalidade: ação graduada conforme risco à integridade do pleito.

Privacidade: respeito à LGPD nos dados de denunciantes e impulsionadores; eliminação de logs após fins eleitorais.

REFERÊNCIAS

ALEMANHA. Bundesamt für Justiz. Netzwerkdurchsetzungsgesetz (NetzDG). Bonn: Bundesamt für Justiz, 2022. Disponível em: https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Hasskriminalitaet/20220721_NetzDG.pdf?_blob=publicationFile&v=2. Acesso em: 12 dez. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. Guia de boas práticas para tratamento de dados em campanhas eleitorais. Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_lgpd_final.pdf. Acesso em: 12 dez. 2025.

BRASIL. Lei nº 9.504, de 30 de setembro de 1997. Dispõe sobre normas para as eleições. Brasília, DF: Presidência da República, 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 11 dez. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei n. 15.211, de 17 de setembro de 2025. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm. Acesso em: 12 dez. 2025.

BRASIL. Supremo Tribunal Federal. Informação à sociedade: RE 1.037.396 (Tema 987) e 1.057.258 (Tema 533) responsabilidade de plataformas digitais por conteúdo de terceiros. Brasília: STF, 2025. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/Informac807a771oa768SociedadeArt19MCI_vRev.pdf. Acesso em: 10 dez. 2025.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 2019. Dispõe sobre propaganda eleitoral. Brasília, DF, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 10 dez. 2025

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 2024. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Brasília, DF, 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 10 dez. 2025.

BRASIL. Tribunal Superior Eleitoral. Eleições 2024: confira as novidades para a propaganda eleitoral na internet. Brasília, 2024. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Marco/eleicoes-2024-confira-as-novidades-para-a-propaganda-eleitoral-na-internet. Acesso em: 12 dez. 2025.

COMISSÃO EUROPEIA. The strengthened code of practice on disinformation 2022. [S. l.]: Comissão Europeia, 2022. Disponível em: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation. Acesso em: 10 dez. 2025.

FUNDAÇÃO GETULIO VARGAS. TSE e desinformação: conceitos relevantes e sua compreensão no Brasil. Rio de Janeiro: FGV, 2024. Disponível em: https://direitorio.fgv.br/publicacao/tse-e-desinformacao-conceitos-relevantes-e-sua-compreensao-no-brasil. Acesso em: 12 dez. 2025.

ÍNDIA. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Índia: Ministry of Electronics and Information Technology, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Acesso em: 10 dez. 2025.

INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA. Construindo consensos: deep fakes nas eleições de 2024. Brasília, 2024. Disponível em: https://www.idp.edu.br/arquivos/cedis/IDP%20%20LIA%2C%20CEDIS%20e%20ETHICS4AI%20-%20Nota%20T%C3%A9cnica%20-%20Construindo%20Consensos%20-%20Deep%20Fakes%20nas%20Elei%C3%A7%C3%B5es%20de%202024.pdf. Acesso em: 12 dez. 2025.

NABAIS, José Casalta. O dever fundamental de pagar impostos. Coimbra: Livraria Almedina, 1998.

OFCOM. Protecting people from illegal harms online: statement & codes. Londres: Ofcom, 2024. Disponível em: https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/statement-protecting-people-from-illegal-harms-online. Acesso em: 10 dez. 2025.

REINO UNIDO. Online Safety Act (OSA). Londres, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 10 dez. 2025.

SUNSTEIN, C. R. Liars: falsehoods and free speech in an age of deception. Oxford: Oxford University Press, 2021. Disponível em: https://global.oup.com. Acesso em: 12 dez. 2025.

UNIÃO EUROPEIA. Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Bruxelas, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. Acesso em: 10 dez. 2025.

2.16 AGÊNCIAS DE VERIFICAÇÃO DE FATOS INDEPENDENTES (ART. 9º-D, §§ 1º E 2º)

Matheus de Oliveira Ferreira

Art. 9º-D. [...]
§ 1º A classificação de conteúdos pelas agências de verificação de fatos, que tenham firmado termo de cooperação com o Tribunal Superior Eleitoral, será feita de forma independente e sob responsabilidade daquelas.
§ 2º As checagens realizadas pelas agências que tenham firmado termo de cooperação serão disponibilizadas no sítio eletrônico da Justiça Eleitoral e outras fontes fidedignas poderão ser utilizadas como parâmetro para aferição de violação ao dever de diligência e presteza atribuído a candidata, candidato, partido político, federação e coligação, nos termos do *caput* deste artigo." (NR)

2.16.1 VISÃO GERAL E OBJETIVOS

Objetivo: analisar os parágrafos 1º e 2º do art. 9º da Resolução TSE n.º 23.610/2024 e comparar com as estratégias adotadas por outras jurisdições de combate à desinformação.

Guia de perguntas:

Sobre o § 1º:

- Quais são os critérios para garantir que a checagem é feita de "forma independente"?
- Quais são as semelhanças e diferenças entre os marcos regulatórios de verificação de fatos do Brasil, União Europeia, Reino Unido e Índia?

Sobre o § 2º:

- O que são "outras fontes fidedignas"?

2.16.2 BASE NORMATIVA (BRASIL)

Norma principal: Res. TSE 23.610/2019, Art. 9, §§ 1º e 2º:

§ 1º: Assegura que a classificação de conteúdos realizada pelas agências que firmarem termo de cooperação com o TSE deve ocorrer de forma independente. A manutenção dessa independência é condição essencial para preservar a imparcialidade e a credibilidade das verificações, assegurando que o processo de checagem transcorra sem qualquer tipo de influência política ou partidária que possa comprometer sua integridade.

§ 2º: Estabelece o processo de disponibilização das checagens no site da Justiça Eleitoral. Outros parâmetros de fontes fidedignas também são reconhecidos para aferir o dever de verificação. Nesse contexto, observa-se a inexistência de critérios claros para conceituar o que constitui informação "fidedigna" pode resultar em insegurança jurídica e questionamentos sobre as decisões adotadas pelo TSE. Além disso, o objetivo desse parágrafo é a responsabilidade dos atores políticos quanto à verificação das informações que utilizam em

suas campanhas eleitorais. A finalidade, portanto, é garantir que o debate político seja pautado em fatos verdadeiros e verificáveis.

Legislação correlata:

Marco Civil da Internet (Lei 12.965/2014): arts. 2, 3, e 4, II; define princípios para o uso da internet, liberdade de expressão, responsabilidade dos provedores de aplicação

Código Civil (Lei n.º 10.406/2002): proteção dos direitos da personalidade e da vida privada, especialmente quanto à responsabilidade civil decorrente da atuação de agências de verificação de fatos e de agentes políticos.

Lei 9.504/1997, arts. 57-B a 57-F (propaganda eleitoral na internet); e Código Eleitoral, art. 243, IX – vedação à divulgação de fatos sabidamente inverídicos.

2.16.3 METODOLOGIA DO *BENCHMARKING*

Seleção de jurisdições comparadas:

- **União Europeia:** *Digital Services Act* (DSA - Reg. 2022/2065) e *Code of Conduct on Disinformation*;
- **Reino Unido:** *Online Safety Act* (2023);
- **Índia:** *IT Rules* 2021.

Unidades de comparação:

Há, nas jurisdições comparadas, mecanismos de cooperação de verificadores de fatos, semelhantes ao adotado pela Justiça Eleitoral brasileira?

Jurisdição		Dispositivo análogo ao § 1º (Independência das agências	Dispositivo análogo ao § 2º (Publicação das checagens feitas pelas agências)	Dispositivo análogo ao § 2º (Publicação das checagens feitas pelas agências)
Identificação e Rotulagem	Art. 45 (Códigos de Conduta) (Atos Digitais da UE) Incentivo a criação de Códigos de Conduta pelas empresas e organizações, com o objetivo de facilitar a aplicação do DSA.	Não há previsão.	Art. 37 (Auditoria independente anual) 1(b): "quaisquer compromissos assumidos em conformidade com os códigos de conduta referidos nos artigos 45º (...)" (Atos Digitais da UE).	O DSA exige que plataformas de grande porte comprovem que estão cumprindo os compromissos dos códigos de conduta criados sob o art. 45.

União Europeia – Code of Conduct on Disinformation	Compromissos de empoderamento a comunidade de verificação de fatos (The Code of Conduct on Disinformation)	Compromisso 30 (Cooperação com a comunidade de verificação de fatos): Os Signatários Relevantes comprometem-se a criar um modelo de cooperação transparente, organizado, inclusivo, financeiramente viável e imparcial com a comunidade de verificação de fatos da União Europeia, abrangendo os recursos e o apoio oferecidos às organizações de checagem de fatos. Compromisso 33 (Padrões dos verificadores de fato): As organizações de verificação de fatos participantes comprometem-se a atuar de forma ética e transparente, em conformidade com padrões rigorosos de integridade, e a preservar sua independência. Medida 33.1: Os Signatários Relevantes deverão cumprir os requisitos estabelecidos em instrumentos reconhecidos, tais como o Código de Princípios da Rede Internacional de Checagem de Fatos (IFCN), do qual devem ser signatários verificados, ou o futuro Código de Integridade Profissional destinado a organizações europeias independentes de verificação de fatos. (The Code of Conduct on Disinformation).	Medida 31.3: Prevê a criação de um repositório europeu de conteúdo verificado, em parceria entre as plataformas digitais, o European Digital Media Observatório (EDMO) e as organizações independentes de verificação de fatos. Esse repositório centraliza as checagens produzidas em toda a UE. Além disso, é administrado pelos verificadores de fatos e também tem acesso aberto para os pesquisadores, as plataformas e o público.	O Código de Conduta é um instrumento, que está relacionado ao DSA, com o objetivo de combater a desinformação online a partir de compromissos feitos pelas plataformas digitais e organizações de verificação de fatos e entidades da sociedade civil.

Reino Unido – *Online Safety Act* (OSA)	Não há previsão para combater a desinformação eleitoral, exceto nos casos que envolvem interferência estrangeira (Gov.UK; What is the *Online Safety Act*? Here's what you need to know).	Não há previsão.	A OSA não assegura que pesquisadores ou agências de verificação de fatos recebam acesso rápido aos dados de plataformas digitais e motores de busca relacionados à circulação de informações falsas ou enganosas nesses ambientes online. (What is the *Online Safety Act*? Here's what you need to know).	A Lei de Uso e Acesso de Dados de 2025 determinará que as empresas digitais disponibilizam informações a pesquisas independentes voltadas à segurança online. Com essa medida, o governo deverá assegurar que as organizações de verificação de fatos tenham acesso aos dados fornecidos pelas plataformas digitais. (https://www.legislation.gov.uk/ukpga/2025/18/part/2).
Índia – *IT Rules* 2021 + Emenda de 2023	Regra 3(1)(b)(v): Estabelece que as plataformas removam "informações falsas ou enganosas sobre negócios do governo" identificadas por uma Fact Check Unit .	Não há previsão.	Não há previsão.	Após a Emenda de 2023, foi criada uma unidade governamental de verificação de fatos relacionada a informações sobre o governo, Fact Check Unit (FCU). No entanto, a Suprema Corte da Índia suspendeu a criação da FCU do governo, pois levanta preocupações sobre a independência, transparência e direitos fundamentais.

2.16.4 *BENCHMARK* INTERNACIONAL (SÍNTESE COMPARATIVA)

União Europeia (UE)

O modelo europeu, por meio do *Digital Services Act* (DSA) e do *Code of Practice on Disinformation*, reconhece os verificadores como atores independentes para combater a desinformação.

A União Europeia apoia e financia o *European Digital Media Observatory* (EDMO), responsável por coordenar uma rede de pesquisadores, verificadores e agências independentes. Trata-se, portanto, não de uma agência que checa fatos para auxiliar um órgão estatal, mas de uma comunidade colaborativa, voltada à cooperação e à troca de boas práticas.

O sistema europeu articula a atuação dos verificadores por meio do EDMO, exigindo transparência, publicação de relatórios públicos e adesão a padrões éticos internacionais, como os definidos pelo Código de Princípios da International *Fact-Checking Network* (IFCN).

Além disso, o documento promove o empoderamento da comunidade de verificação de fatos com base em quatro compromissos centrais: Cooperação entre os membros de verificação de fatos; Uso e integração das checagens nos serviços dos signatários; Acesso dos verificadores de fatos a informações relevantes; e Adoção de padrões para operar.

Assim, a verificação de fatos é tratada, no contexto europeu, como uma função estruturante da governança digital europeia, não apenas como instrumento de fiscalização pontual, mas como mecanismo permanente de transparência, responsabilidade e integridade informacional.

Reino Unido – OSA

A legislação não reconhece os verificadores de fatos de forma institucional. Isto é, o combate à desinformação é exigido pelas plataformas digitais, sob supervisão da Ofcom, e se limita a conteúdos ilegais ou prejudiciais. Apesar disso, existem iniciativas de checagem (como a *Full Fact*), mas sem vínculo normativo ou cooperação estatal.

Índia – *IT Rules*

Por sua vez, a legislação indiana buscou centralizar o processo de verificação de fatos por meio da emenda de 2023. Apesar dessa tentativa de controle estatal, ainda atuam no país organizações independentes certificadas pela IFCN, que seguem padrões internacionais de transparência, independência e metodologia, como a *Alt News* e a *India Today Fact Check.*

2.16.5 INTERPRETAÇÃO DO ART. 9, §1 E § 2º À LUZ DO *BENCHMARKING* INTERNACIONAL

O § 1º do art. 9º reforça a autonomia e a independência das agências de verificação de fatos, alinhando-se às boas práticas europeias e aos padrões da IFCN e da EFCSN, (*European Fact-Checking Standards Network*, [202-?]).

Assim como o Código de Conduta sobre Desinformação da União Europeia, a Resolução TSE estabelece um modelo de cooperação institucional entre o poder público e os verificadores independentes, garantindo a autonomia metodológica e a responsabilidade exclusiva das agências pelas classificações.

O dispositivo reforça a credibilidade do processo eleitoral, ao prever que a Justiça Eleitoral possa se apoiar nas checagens produzidas por agências independentes, as quais exercem sua atividade com autonomia técnica e sem qualquer interferência da própria Justiça Eleitoral.

Quanto ao § 2º do art. 9º materializa o princípio da transparência, ao determinar que as checagens realizadas pelas agências de verificação de fatos sejam publicadas no portal da Justiça Eleitoral, conferindo visibilidade e controle social ao processo de combate à desinformação. Essa publicação permite que o cumprimento do dever de diligência por parte dos agentes políticos seja aferido de forma concreta e verificável. Trata-se de uma analogia prevista no Código de Desinformação e nas diretrizes da Rede Europeia de Normas de Verificação de Fatos (EFCSN). Além disso, o Código de Boas Práticas sobre Desinformação atua de forma complementar às regras éticas e de transparência para os signatários.

Por fim, a previsão de "outras fontes fidedignas" amplia o escopo probatório, possibilitando o uso de diferentes evidências e evitando a concentração da autoridade sobre a verdade. Assim, o dispositivo institui um modelo combinado de responsabilidade, que concilia o dever de diligência do agente público com a aferição baseada em checagens independentes.

A síntese comparativa demonstra que, entre as jurisdições analisadas, somente o Brasil e a União Europeia possuem referências normativas ao papel das agências de verificação de fatos independentes, ainda que em contextos distintos e com graus diferentes de institucionalização. No caso do modelo europeu, possui uma política pública contínua de verificação de fatos, reconhecida no DSA e no Código.

2.16.6 EVIDÊNCIAS E ESTUDOS DE CASO

Dalban vs. Romania: Nesse caso, entendeu-se que a condenação de um jornalista por difamação de um senador representou violação à liberdade de expressão. A decisão do Tribunal Europeu de Direitos Humanos ressaltou que não seria razoável exigir do profissional a comprovação plena da veracidade das informações publicadas, sobretudo porque as autoridades tampouco conseguiram demonstrar de maneira definitiva que as alegações eram falsas (Tribunal Europeu de Direitos Humanos, 1999).

Agentstvo televideniya Novosti, OOO v. Ukraine: O Tribunal Europeu de Direitos Humanos concluiu que a emissora ucraniana agiu de má-fé, pois divulgou informações imprecisas e sem a devida verificação. A reportagem apresentou fatos ainda em debate como se fossem comprovados, utilizando linguagem sensacionalista e desrespeitosa, o que comprometeu a credibilidade do conteúdo e violou os princípios do jornalismo responsável (Voorhoof *et al*., 2022).

Magyar Jeti Zrt v. Hungary: foi reconhecida uma proteção ampliada à atividade jornalística ao tratar da inserção de hiperlinks em publicações. O Tribunal entendeu que o simples ato de vincular um conteúdo controverso - inclusive potencialmente falso - não implica, por si só, responsabilidade do jornalista. Contudo, admitiu a possibilidade de responsabilização caso fique comprovado que houve endosso, reprodução intencional ou má-fé na divulgação do material (Tribunal Europeu de Direitos Humanos, 2018).

2.16.7 RECOMENDAÇÕES (NORMATIVAS E OPERACIONAIS)

Criar um comitê consultivo entre o Tribunal Superior Eleitoral (TSE), plataformas, agências e pesquisadores.

Garantir acesso aos dados de plataformas para pesquisas independentes e verificação de fatos, especialmente em anúncios políticos e conteúdos impulsionados.

Introduzir relatórios anuais de transparência das ações das plataformas e do TSE no combate à desinformação.

Estabelecer um repositório digital público de checagens eleitorais, centralizado e acessível.

Necessidade de criar critérios para a identificação de “outras fontes fidedignas”.

Adotar padrões de independência, transparência e metodologia internacionalmente reconhecidos nos termos de cooperação, como o *International Fact-Checking Network* – IFCN.

Estimular a pluralidade de agências para reduzir o risco de viés.

Criar medidas de cooperação/códigos de conduta entre as plataformas digitais e agências de verificação de fatos. Essa obrigação permite uma resposta rápida a conteúdos “notoriamente inverídicos”.

Adotar auditorias para avaliação das agências.

2.16.8 RISCOS, SALVAGUARDAS E DIREITOS

Riscos:

Ao concentrar a coordenação e a publicação das checagens realizadas por agências parceiras, o TSE pode ser percebido como um agente controlador, o que representa risco à pluralidade de fontes e pode gerar percepções de censura ou restrição à liberdade de expressão.

A expressão "outras fontes fidedignas" amplia a utilização de diferentes bases confiáveis de informação para aferir a desinformação pela Justiça Eleitoral. No entanto, por não especificar quais critérios definem a confiabilidade dessas fontes, pode gerar insegurança jurídica e subjetividade na aplicação da norma. É necessário definir parâmetros claros e objetivos para assegurar imparcialidade, transparência e credibilidade nas checagens.

Salvaguardas:

Direito à transparência pública: O TSE deve publicar relatórios de impacto e das metodologias de cooperação entre as agências de verificação.

Transparência pública: criar um portal de checagens, com metodologia, critérios e resultados disponíveis a qualquer cidadão.

Pluralidade institucional: promover diversidade de fontes e agências (regionais, acadêmicas, jornalísticas) para evitar monopólio de checagem.

Direitos:

Liberdade de expressão: garantir que a checagem não resulte em censura.

Direito à informação: a verificação deve ampliar o acesso à informação, não restringi-lo.

Privacidade e proteção de dados: qualquer compartilhamento de dados deve observar a LGPD.

REFERÊNCIAS

BRASIL. Lei nº 9.504, de 30 de setembro de 1997. Dispõe sobre normas para as eleições. Brasília, DF: Presidência da República, 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 11 dez. 2025.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 dez. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 dez 2025.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.610, de 2019. Dispõe sobre propaganda eleitoral. Brasília, DF, 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 10 dez. 2025

COMISSÃO EUROPEIA. The strengthened code of practice on disinformation 2022. [S. l.]: Comissão Europeia, 2022. Disponível em: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation. Acesso em: 10 dez. 2025.

EUROPEAN FACT-CHECKING STANDARDS NETWORK. Code of standards. Paris, [202-?]. Disponível em: https://efcsn.com/code-of-standards/. Acesso em: 12 dez. 2025.

FULL FACT. The Online Safety Act and Misinformation: What you need to know. Disponível em: https://fullfact.org/policy/online-safety-act/. Acesso em: 12 dez. 2025.

ÍNDIA. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Índia: Ministry of Electronics and Information Technology, 2021. Disponível em: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Acesso em: 10 dez. 2025.

ÍNDIA. Press Information Bureau. MeitY notifies PIB fact check unit as fact checker of Central Government. Government of India, 2024. Disponível em: https://www.pib.gov.in/PressRelese-Detailm.aspx?PRID=2015786. Acesso em: 12 dez. 2025.

ÍNDIA. Supreme Court. Guild of Editors of India vs. The Union of India. Civil Appeal Nos. 4509-4511 of 2024. Julgado em 21 mar. 2024. Disponível em: https://supremetoday.ai/doc/judgement/INDSC00000011453. Acesso em: 12 dez. 2025.

REINO UNIDO. Online Safety Act (OSA). Londres, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 10 dez. 2025.

REINO UNIDO. Data (Use and Access) Act 2025. Parte 2. Reino Unido, 2025. Disponível em: https://www.legislation.gov.uk/ukpga/2025/18/part/2. Acesso em: 12 dez. 2025.

TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Case of Dalban v. Romania (Application n. 28114/95), par. 49, 1999. Disponível em: https://hudoc.echr.coe.int/eng?i=001-58306. Acesso em: 12 dez. 2025.

TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Magyar Jeti Zrt v. Hungary (Application no. 11257/16). Julgado em 4 dez. 2018. Estrasburgo: Tribunal Europeu de Direitos Humanos. Disponível em: https://hudoc.echr.coe.int/eng?i=001-187930. Acesso em: 12 dez. 2025.

UNIÃO EUROPEIA. Digital Services Act (DSA): Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Bruxelas, 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065. Acesso em: 10 dez. 2025.

VOORHOOF, Dirk et al. Freedom of Expression, the Media and Journalists: Case-law of the European Court of Human Rights. 7. ed. Strasbourg: European Audiovisual Observatory, 2022. Disponível em: https://globalfreedomofexpression.columbia.edu/publications/freedom-of-expression-the-media-andjournalists-case-law-of-the-european-court-of-human-rights-7th-edition/. Acesso em: 12 dez. 2025.

PARTE III - TABELA UNIFICADA DAS RECOMENDAÇÕES NORMATIVAS E OPERACIONAIS

Observação: As recomendações apresentadas nesta seção partem da premissa de que é necessário disciplinar a granularidade das obrigações previstas na Resolução TSE n.º 23.610/2019 dirigidas às plataformas digitais, por meio de parâmetros objetivos. Plataformas e mecanismos de busca de grande dimensão devem submeter-se a deveres mais rigorosos, compatíveis com seu impacto informacional no processo eleitoral. Destaca-se, ainda, que a definição desses critérios para a aplicação diferenciada das obrigações exige amplo debate técnico e institucional no âmbito da competência normativa do Tribunal Superior Eleitoral, a fim de garantir proporcionalidade, coerência regulatória e aderência às especificidades do ecossistema digital.

Bloco 1: Governança, Adequação e Dever de Cuidado (Ações Proativas e Estruturais)

Este bloco reúne as recomendações focadas na estruturação interna das plataformas e na formalização dos deveres de diligência, visando a prevenção e a mitigação de riscos sistêmicos.

Subtema do Bloco 1	Recomendações	Fonte na Parte II
1.1. Formalização da Governança (VLOPs e VLOSEs)	**Transformar termos e políticas em instrumentos de governança pública:** O Tribunal Superior Eleitoral (TSE) deve editar uma orientação interpretativa que reconheça que os termos de uso e políticas de conteúdo constituem documentos regulatórios, e não meramente contratuais.	I. Adequação de Políticas e Documentos
	Estabelecer requisitos mínimos de conteúdo das políticas eleitorais: Por meio de resolução ou instrução complementar, o TSE deve definir elementos mínimos que devem constar dos termos de uso, densificando o conceito de conteúdo político-eleitoral previsto no art. 27-A, § 1º da Res. 23.610/2019.	
	Elaborar e divulgar guias operacionais para provedores sobre as novas obrigações.	III. Cadastro
	Governança e Estrutura Interna: Nomear um responsável interno (Grievance Officer, residente no país) com dados de contato públicos, e realizar auditorias independentes periódicas e avaliação de impacto em anos eleitorais.	IV. Canais de Denúncia
	Termos de Uso Direcionados: Inserir nos termos de uso das plataformas direcionamento específico para anúncios político-eleitorais e regras claras sobre impulsionamento e monetização em períodos eleitorais.	VI. Função Social e Dever de Cuidado
	***Accountability* Multinível e Granular:** Formalizar o princípio da proporcionalidade, impondo obrigações mais rigorosas a plataformas de grande porte (VLOPs e VLOSEs). Exigir que essas plataformas criem uma "função de conformidade" (compliance) destacada e independente, reportando diretamente ao órgão de administração, seguindo o modelo do DSA.	IX. Prestação de Contas, Relatórios de Impacto e Adequação de Tecnologia
	Harmonização Normativa: Promover interpretação convergente entre o art. 9º-E da Resolução 23.610/2019, o	XII. Responsabilidade Civil e Administrativa

	ECA Digital e o Marco Civil, estabelecendo que a ilicitude manifesta dispensa ordem judicial.	das Plataformas na Obrigação de Indisponibilização Imediata dos Conteúdos Graves (e Contas) nos Casos de Risco
	Definição de "Comunicação de Campanha": Definir, por meio de resolução que atualizaria a redação da Resolução n.º 23.610/2019, o que configura e não configura uma "comunicação de campanha".	XIV. Vedação à Simulação de Interlocução
1.2. Cadastro e Cooperação Institucional	**Prazos de resposta** a alertas oficiais do TSE.	I. Adequação de Políticas e Documentos
	Governança compartilhada: Adotar um modelo de corregulação (governo + plataformas), inspirado em experiências internacionais como a Ofcom (Reino Unido) e o Digital Services Coordinator (UE).	II. Adoção e Publicização de Medidas
	Definir quais provedores estão obrigados ao cadastro: Por meio de resolução, definir quais provedores de aplicação (redes sociais, mecanismos de busca, serviços de streaming, aplicativos de mensagens e marketplaces de publicidade digital) estão obrigados ao cadastro para prestação de serviço de impulsionamento.	III. Cadastro
	Atualização do registro: Determinar que o registro junto à Justiça Eleitoral seja atualizado a cada eleição ou sempre que houver alteração de controle societário, políticas de transparência, local de armazenamento de dados ou modelo de impulsionamento.	
	Vincular o cadastro à assinatura de um termo de compromisso que obrigue o provedor a: preservar logs de impulsionamento, responder a requisições da Justiça Eleitoral em prazo reduzido, publicar relatórios de transparência eleitoral (quantidade de anúncios, origem e volume financeiro) e adotar protocolos de moderação compatíveis.	
	Prever a suspensão temporária ou definitiva do cadastro em caso de descumprimento das obrigações, com divulgação pública dos casos de provedores suspensos ou inabilitados.	
	Integrações Institucionais e Cooperação: Estabelecer convênios e canais dedicados com órgãos eleitorais e fomentar a criação de sinalizadores de confiança (*trusted flaggers*), garantindo prioridade no processamento de denúncias.	IV. Canais de Denúncia
	Criação de Força-Tarefa: Criar uma força-tarefa das plataformas nos períodos eleitorais, em parceria com o TSE e agências de checagem de fatos, para possibilitar respostas de notificação e ação mais rápidas.	VI. Função Social e Dever de Cuidado
	Fomentar programas de integridade eleitoral digital que envolvam universidades, entidades civis e pesquisadores independentes, para produzir dados públicos sobre impulsionamento e seus efeitos sociais.	VIII. Impulsionamento digital de propaganda eleitoral
	Formalização da Corregulação: Formalizar o incentivo à elaboração de códigos de conduta facultativos (corregulação) e exigir que os provedores mantenham registros escritos das medidas adotadas em consonância com esses códigos.	IX. Prestação de Contas, Relatórios de Impacto e Adequação de Tecnologia

	Fluxos Padronizados de Resposta: Criar canal 24/7 exclusivo para comunicações do TSE/Procuradoria Eleitoral, com obrigação de *acknowledgment* automático em até duas horas do recebimento.	XII. Responsabilidade Civil e Administrativa das Plataformas na Obrigação de Indisponibilização Imediata dos Conteúdos Graves (e Contas) nos Casos de Risco
	Modelo *Trusted Flagger* Eleitoral: Formalizar o TSE e entidades credenciadas (*fact-checkers*, observatórios) como sinalizadores de confiança, com prioridade de tratamento (resposta acelerada: 24h).	
	Manter um canal direto com o TSE para alertas de alto risco (de forma contínua).	XV. Vedação ao Impulsionamento de Conteúdo Falso ou Descontextualizado
	Criar um comitê consultivo entre o Tribunal Superior Eleitoral (TSE), plataformas, agências e pesquisadores.	XVI. Agências de verificação de fatos independentes
1.3. Prevenção e Mitigação de Riscos	**Protocolos de rotulagem e checagem de fatos.**	
	Incluir obrigação de revisão pré-eleitoral e pós-pleito das políticas: Determinar que, até 60 dias antes do pleito, as plataformas enviem ao TSE e divulguem publicamente uma atualização ou relatório de integridade eleitoral, com ajustes de termos e processos; e, até 60 dias após, divulguem relatório avaliativo com dados de impacto e planos de melhoria.	I. Adequação de Políticas e Documentos
	Evitar a autorregulação simbólica: Sem fiscalização efetiva e métricas claras, o dever de agir se torna autorregulação simbólica, esvaziando o propósito normativo do art. 9°-D.	II. Adoção e Publicização de Medidas
	Prevenção de Abuso: Prever sanções para notificações manifestamente infundadas (incluindo suspensão temporária de denunciantes abusivos) e preferir medidas graduais, como rotulagem ou limitação de alcance, à remoção total, para preservar a liberdade de expressão.	IV. Canais de Denúncia
	Planejamento e Execução de Ações Corretivas e Preventivas: Exigir o aperfeiçoamento de sistemas algorítmicos de recomendação para mitigar a circulação de desinformação.	V. Correção e Prevenção e Proteção de Dados
	Avaliação de Risco: O provedor deve elaborar, em ano eleitoral, uma avaliação de impacto de seus serviços sobre a integridade do processo eleitoral para implementar medidas eficazes.	
	Controle da Monetização: Adotar a proibição ou maior controle das regras de monetização de anúncios eleitorais, garantindo mecanismos de transparência para pesquisas por parte dos usuários.	VI. Função Social e Dever de Cuidado
	Criar protocolos de auditoria cooperativa, permitindo que o Tribunal Superior Eleitoral (TSE) e as plataformas avaliem conjuntamente riscos de desinformação e manipulação algorítmica.	VIII. Impulsionamento digital de propaganda eleitoral
	Avaliação de Impacto Eleitoral (AIE): Detalhar os parâmetros mínimos para a AIE (Art. 9º-D, V), exigindo que cubram explicitamente a identificação e mitigação de riscos sistêmicos e que se avalie o impacto das medidas de segurança sobre a liberdade de expressão e a privacidade.	IX. Prestação de Contas, Relatórios de Impacto e Adequação de Tecnologia
	Vigência Contínua: Deixar claro que o dever de prestação de contas do art. art. 9º-D se aplica de forma contínua, inclusive fora do período de campanha.	

	Adequação Tecnológica: Realizar o teste e adaptação de sistemas algorítmicos (incluindo sistemas de recomendação) e correção de critérios. Plataformas de grande alcance devem se esforçar para identificar proativamente conteúdos relacionados à integridade eleitoral.	
	Incentivos Regulatórios: Estabelecer mecanismos de incentivo regulatório para que plataformas adotem protocolos de prevenção, auditoria e transparência voluntária.	XI. Remoção de Conteúdo
	Corregulação e Prevenção: Favorecer a criação de acordos de corregulação e promover políticas de prevenção, com treinamento constante dos modelos de detecção de desinformação e *deepfakes* eleitorais.	
	Matriz de Risco: O TSE deve instituir matriz de risco informacional eleitoral (baseada em critérios como alcance, velocidade de disseminação e grau de coordenação), para graduar a resposta das plataformas e o nível de sanção.	XII. Responsabilidade Civil e Administrativa das Plataformas na Obrigação de Indisponibilização Imediata dos Conteúdos Graves (e Contas) nos Casos de Risco
	Cooperação Internacional: Estabelecer protocolos de cooperação com autoridades eleitorais da UE e do Reino Unido para troca de dados sobre práticas de mitigação.	
	Implementar a revisão automática de conteúdo patrocinado por termos eleitorais sensíveis (de forma permanente, a cargo da plataforma).	XV. Vedação ao Impulsionamento de Conteúdo Falso ou Descontextualizado
	Tornar obrigatória a Avaliação de Impacto da Desinformação em Campanhas Digitais (AII-Eleitoral) (anual/eleições, responsabilidade de Partidos e provedores).	
	Cronograma de Implementação: Publicação de guia técnico pelo TSE e formação de grupo de trabalho com plataformas (1º trimestre 2026); Implantação piloto de sistema de monitoramento em tempo real (2º trimestre 2026); Testes de resposta rápida e auditorias externas (3º trimestre 2026); Aplicação plena das obrigações do art. 9º-D (Eleições 2026).	
	Criar critérios para a identificação de "outras fontes fidedignas".	XVI. Agências de verificação de fatos independentes
	Adotar padrões de independência, transparência e metodologia internacionalmente reconhecidos nos termos de cooperação, como o International Fact-Checking Network – IFCN.	
	Estimular a pluralidade de agências para reduzir o risco de viés.	

Bloco 2: Transparência Ativa e Prestação de Contas (*Accountability*)

Este bloco aborda os requisitos de visibilidade e *accountability* exigidos das plataformas em relação aos seus mecanismos de publicidade e moderação, garantindo acesso público e auditável às informações.

Subtema do Bloco 2	Recomendações	Fonte na Parte II
2.1. Repositório Público e Acesso a Dados	**Criação de painel público de integridade digital:** É desejável um instrumento de transparência ativa e centralizada que reúna relatórios, termos e estatísticas	I. Adequação de Políticas e Documentos

	das plataformas, com atualização em tempo real durante as eleições.	
	Criar um repositório público e pesquisável no portal do TSE com a lista de provedores cadastrados, contendo nome da empresa, país de origem, URL principal, responsável de contato e status do cadastro (ativo, suspenso, revogado).	III. Cadastro
	Criar um portal público de denúncia de anúncios pagos veiculados por provedores não cadastrados.	
	Criar um repositório público de anúncios eleitorais, à semelhança do previsto no DSA e nas normas da Ofcom, permitindo o acesso a dados agregados sobre valores pagos, público-alvo, duração e contratantes.	VIII. Impulsionamento digital de propaganda eleitoral
	Relatórios de Conformidade: Incluir a obrigação de relatórios de conformidade por parte das plataformas, contendo dados sobre desligamentos, denúncias, decisões de moderação e volume de impulsionamentos.	
	Acesso a Dados para Pesquisa: Estabelecer um arcabouço normativo que garanta o acesso de pesquisadores e da sociedade civil a dados das plataformas para estudo independente da desinformação.	IX. Prestação de Contas, Relatórios de Impacto e Adequação de Tecnologia
	Relatórios Públicos de Anúncios: Exigir relatórios públicos de anúncios, conforme o modelo europeu (DSA Art. 39), adaptáveis ao tamanho dos agentes que realizam tratamento no contexto eleitoral.	X. Proteção de Dados
	Transparência Pública e Pesquisa: Obrigar plataformas a abrirem repositórios de anúncios e conteúdos removidos, permitindo auditoria por pesquisadores e imprensa.	XII. Responsabilidade Civil e Administrativa das Plataformas na Obrigação de Indisponibilização Imediata dos Conteúdos Graves (e Contas) nos Casos de Risco
	Regulamentação de Campos Mínimos: Regulamentar os campos mínimos obrigatórios do repositório (espelhando Art. 27-A), incluindo parâmetros de segmentação, orçamento, período, criativos e catálogo de versões.	XIII. Transparência e Repositório de Anúncios
	Padrões de Rótulo: Fixar padrões de rótulo (tamanho, posição, persistência, contraste) e chave de consulta para o repositório.	
	API Pública: Disponibilizar API pública versionada, documentada, com exportação em massa, para acesso de pesquisadores, imprensa, sociedade civil e Justiça Eleitoral.	
	Atualização em Tempo Real: O "tempo real" deve ser interpretado como *near real-time*, com atualização contínua ou com atraso máximo de até 72 horas.	
	Métricas de Auditabilidade: Exigir métricas de confiabilidade e auditabilidade, incluindo logs assinados e relatórios de auditoria (sumários).	
	Auditoria da Autoridade: O TSE deve operar um repositório espelho (cópias periódicas) para preservação probatória.	
	Garantir acesso aos dados de plataformas para pesquisas independentes e verificação de fatos,	XVI. Agências de verificação de fatos independentes

	especialmente em anúncios políticos e conteúdos impulsionados.	
	Estabelecer um repositório digital público de checagens eleitorais, centralizado e acessível.	
2.2. Transparência do Conteúdo e dos Canais	**Definição de parâmetros de publicização:** Estabelecer periodicidade mínima (ex.: semestral ou anual) para publicação das medidas adotadas. Deve-se determinar formato padronizado, que permita comparação entre plataformas (ex.: modelo de relatório público digital), e indicar o local obrigatório de divulgação.	II. Adoção e Publicização de Medidas
	Relatórios periódicos de conformidade: Exigir relatórios públicos contendo indicadores mensuráveis, como: número de conteúdos moderados, tempo médio de resposta, parcerias com verificadores, investimento em moderação e resultados de mitigação.	
	Auditorias internas e externas: Impor auditorias independentes, preferencialmente conduzidas por entidades técnicas, para verificar a veracidade dos dados divulgados. Além disso, prever auditorias internas obrigatórias em ano eleitoral, com relatórios enviados ao TSE e às autoridades competentes.	
	Transparência e sanções: Estabelecer sanções administrativas graduadas em caso de omissão ou publicação de informações falsas ou incompletas, além de garantir a publicação integral das auditorias e relatórios em formato acessível ao público e à imprensa.	
	Transparência e Métricas: Publicar relatórios periódicos públicos (trimestrais ou mais frequentes em anos eleitorais) em formato legível por máquina, contendo métricas sobre volume de denúncias, prazos médios de resposta, taxas de reversão, medidas proativas e uso de sistemas automatizados.	IV. Canais de Denúncia
	Transparência dos Resultados: Impor a publicização dos resultados das ações corretivas e preventivas para controle público e responsabilização.	V. Correção e Prevenção e Proteção de Dados
	Relatório Pós-Eleição: Publicar um relatório de transparência após cada eleição, permitindo avaliação pública e sugestões de melhoria por terceiros interessados.	VI. Função Social e Dever de Cuidado
	Definição de Conteúdo Mínimo e Harmonização: Coordenar o desenvolvimento de modelos harmonizados para os relatórios de transparência, especificando o conteúdo, periodicidade e formato (exigindo dados quantitativos sobre moderação, precisão de sistemas automatizados, recursos humanos e métricas de impacto).	IX. Prestação de Contas, Relatórios de Impacto e Adequação de Tecnologia
	Transparência Institucional: Obrigar o próprio TSE a publicar relatórios de transparência anuais baseados nas informações dos provedores.	
	Verificação Externa: Exigir a submissão a auditorias independentes anuais para as plataformas de grande porte, com os relatórios fundamentando não conformidades e incluindo recomendações operacionais.	

	Auditorias Independentes: Implementar auditorias independentes para avaliar se as decisões de moderação respeitam a normativa.	XI. Remoção de Conteúdo
	Dever Formal de Documentação: Determinar que todas as medidas tomadas sob o Art. 9º-E sejam documentadas com *logs* auditáveis (data/hora, ID do conteúdo, motivo, decisão final), integrando relatórios de transparência obrigatórios.	XII. Responsabilidade Civil e Administrativa das Plataformas na Obrigação de Indisponibilização Imediata dos Conteúdos Graves (e Contas) nos Casos de Risco
	Exigir relatório público trimestral sobre impulsionamentos bloqueados ou rotulados (quinzenal em ano eleitoral).	XV. Vedação ao Impulsionamento de Conteúdo Falso ou Descontextualizado
	Introduzir relatórios anuais de transparência das ações das plataformas e do TSE no combate à desinformação.	XVI. Agências de verificação de fatos independentes
	Adotar auditorias para avaliação das agências.	

Bloco 3: Fluxos de Moderação e Devido Processo Digital (Reação e Resposta)

Este bloco concentra as recomendações sobre a operacionalização dos mecanismos de Notice and Action (notificação e ação), os prazos de remoção de conteúdo ilícito e as salvaguardas processuais para usuários afetados.

Subtema do Bloco 3	Recomendações	Fonte na Parte II
3.1. Canais de Denúncia e Prazos	**Requisitos Operacionais e de Acessibilidade:** O canal de denúncia deve ter um botão "Denunciar" facilmente identificável, formulário padronizado que permita o envio de evidências e esteja disponível em português e idiomas locais. O sistema deve emitir recibo automático de recebimento.	IV. Canais de Denúncia
	Fluxos e Prazos de Tratamento: Adotar prazos escalonados e proporcionais: 24 horas para casos manifestamente ilícitos ou de risco grave; 72 horas para situações de prioridade alta; e até sete dias para análise padrão.	
	Fortalecer canais técnicos entre o TSE e provedores de aplicação, por meio de fluxos automatizados de verificação e desligamento de anúncios em período de *blackout*.	VIII. Impulsionamento digital de propaganda eleitoral
	Procedimentos de Remoção: Exigir procedimentos internos padronizados para remoção célere, mas fundamentada.	XI. Remoção de Conteúdo
	Regulamentação de Prazos: O termo "indisponibilização imediata" deve ser regulamentado pelo TSE por instrução normativa complementar, fixando faixas de tempo proporcionais à gravidade do risco (ex.: até 24h para incitação à violência, ódio ou ataque às instituições).	XII. Responsabilidade Civil e Administrativa das Plataformas na Obrigação de Indisponibilização Imediata dos Conteúdos Graves (e Contas) nos Casos de Risco
	Exigir a suspensão imediata de impulsionamento após notificação ou identificação interna (prazo sugerido: 24h).	XV. Vedação ao Impulsionamento de Conteúdo Falso ou Descontextualizado

3.2. Devido Processo e Salvaguardas	**Canais de apelação e revisão de moderação.**	I. Adequação de Políticas e Documentos
	Devido Processo e Recurso Interno: O usuário afetado por remoção deve receber uma declaração de motivos clara e acessível e o provedor deve manter um mecanismo interno de recurso com prazos razoáveis e garantia de revisão humana.	IV. Canais de Denúncia
	Comunicação Justificada e Recurso: Garantir comunicação imediata e justificada ao usuário afetado, com indicação clara do motivo da remoção, fundamento normativo e meios de recurso.	XI. Remoção de Conteúdo
	Contraditório Diferido: Introduzir mecanismo de revisão pós-pleito, no qual o usuário impactado possa solicitar revisão administrativa ou judicial após o término do período eleitoral.	XII. Responsabilidade Civil e Administrativa das Plataformas na Obrigação de Indisponibilização Imediata dos Conteúdos Graves (e Contas) nos Casos de Risco

Bloco 4: Integridade Algorítmica e Regras Específicas de IA/Dados

Este bloco aborda as regras relativas ao uso de sistemas de IA, deepfakes, chatbots e o tratamento de dados pessoais para fins eleitorais, exigindo transparência e limites no perfilamento. 1)

Subtema do Bloco 4	Recomendações	Fonte na Parte II
4.1 Transparência da IA e Rotulagem	**Regras sobre tratamento de deepfakes e conteúdos sintéticos.**	I. Adequação de Políticas e Documentos
	Padrões Mínimos para Aviso Unificado: O aviso deve ser padronizado como "Conteúdo produzido/manipulado por inteligência artificial".	VII. IA e Transparência na Propaganda Eleitoral
	Exibição Acessível: O aviso deve ter exibição simultânea a todo o conteúdo, fonte legível, alto contraste e tradução em LIBRAS quando houver vídeo, além de outros instrumentos de acessibilidade.	
	Registro para Auditoria: Exigir registro do uso de IA em metadados e protocolo de publicação.	
	Rotulagem Persistente (Modelo UE): Aplicar diretrizes da União Europeia sobre rótulo persistente, garantindo que os anúncios sejam visíveis, identificáveis, explicáveis e auditáveis.	
	Relatórios Públicos: Exigir relatórios públicos de peças que utilizaram IA (semelhante ao Art. 15 do DSA) e implementar sistemas de listas verificadas de propagandas com IA.	
	Definição de "Simulação de Interlocução": Definir, por meio de resolução que atualizaria a redação da Resolução n.º 23.610/2019, o que configura e não configura uma "simulação de interlocução".	XIV. Vedação à Simulação de Interlocução
4.2 Limites Algorítmicos e Recomendação	**Mitigação de Riscos Algorítmicos (Modelo DSA):** Plataformas de grande dimensão devem oferecer ao usuário pelo menos uma opção de sistema de recomendação que não se	V. Correção e Prevenção e Proteção de Dados

	baseie na definição de perfis, para dar controle sobre a coleta de dados.	
	Transparência de Sistemas Proativos (Modelo OSA): As plataformas devem incluir em suas declarações públicas informações sobre qualquer tecnologia proativa (algorítmica) utilizada para cumprir os deveres de segurança, incluindo o tipo de tecnologia, uso e funcionamento.	
	Exclusão de Canais: A Justiça Eleitoral deve gerir o banco de dados de endereços eletrônicos declarados com caráter público e verificável, mas protegendo dados pessoais. A exclusão dos sistemas de recomendação deve se referir apenas aos conteúdos orgânicos de canais não registrados.	XIII. Transparência e Repositório de Anúncios
4.3 Proteção de Dados e Perfilamento	**Proteção de Dados e Perfilamento:** Exigir acesso facilitado às informações sobre o tratamento de dados usados para perfilamento. Deve ser exigido o Relatório de Impacto à Proteção de Dados (RIPD) em casos de alto risco (tratamento em larga escala e tecnologias inovadoras para perfilamento).	V. Correção e Prevenção e Proteção de Dados
	Explicabilidade Algorítmica: Prever a explicação algorítmica mínima, permitindo que o usuário saiba por que recebeu determinado anúncio político.	VIII. Impulsionamento digital de propaganda eleitoral
	Atualização Regulatória: Atualizar continuamente as resoluções eleitorais para incluir novos fenômenos, como *deepfakes*, *microtargeting* e campanhas automatizadas.	
	Articulação com ANPD: É necessária a articulação com a Autoridade Nacional de Proteção de Dados (ANPD) para revisão das normas e condições para o tratamento de dados pessoais no contexto eleitoral.	X. Proteção de Dados
	Aviso de Transparência Eleitoral: Exigir aviso de transparência eleitoral, com seção específica e em destaque nas políticas.	

PARTE IV - CONSIDERAÇÕES FINAIS E SUGESTÕES DE IMPLEMENTAÇÃO

Tainá Aguiar Junquilho, Francisco Brito Cruz, Laura Schertel Mendes, Paula Pedigoni Ponce, Lucia Lucia Maria Teixeira Ferreira e Guilherme Antonio Balczarek Mucelin

4.1 CONTEXTO, PROBLEMA REGULATÓRIO E OBJETIVOS DO RELATÓRIO

O relatório "Integridade da informação nas eleições e plataformas digitais: caminhos para a corregulação" partiu do diagnóstico de que a comunicação política contemporânea foi profundamente transformada pela intermediação algorítmica e pela centralidade das grandes plataformas digitais.

Como se depreendeu da Parte I deste relatório, as eleições deixaram de ser processos circunscritos ao território e passaram a operar como fenômenos informacionais transnacionais, marcados pela circulação permanente de narrativas, dados e fluxos comunicacionais com alto potencial de manipulação. Nesse cenário, a proteção da integridade do processo democrático depende não apenas de respostas reativas a conteúdos ilícitos, mas de uma arquitetura regulatória que enfrente riscos sistêmicos do ecossistema digital, incluindo desinformação, descontextualização grave e formas de amplificação artificial de alcance. Com esse pano de fundo, o Tribunal Superior Eleitoral reformulou a disciplina da propaganda político-eleitoral na internet por meio da Resolução TSE nº 23.732/2024, que alterou substancialmente a Resolução TSE nº 23.610/2019 e introduziu, como elemento central, o art. 9º-D, impondo deveres positivos aos provedores de aplicação de internet para prevenção, mitigação e transparência em matéria de integridade informacional eleitoral.

O relatório descreveu, nesse sentido, essa mudança como uma inflexão regulatória relevante: o regime deixa de se concentrar apenas na remoção de conteúdos ilegais ou no cumprimento de decisões judiciais e passa a exigir das plataformas uma postura preventiva, baseada em governança interna, políticas coerentes, mecanismos de denúncia eficazes e prestação de contas pública. Nessa lógica, a integridade da informação é tratada como bem jurídico coletivo e como dimensão da cidadania digital, demandando coordenação institucional entre Justiça Eleitoral, plataformas e sociedade civil. A proposta de corregulação não é apresentada como privatização da regulação, mas como governança cooperativa supervisionada, na qual o TSE define objetivos e parâmetros públicos e as plataformas implementam meios técnicos e operacionais sob fiscalização, transparência e possibilidade de auditoria social. Como eixo metodológico, o relatório buscou avaliar o alcance jurídico dos deveres impostos pela normativa eleitoral às plataformas, identificar lacunas e propor aprimoramentos concretos para tornar o modelo efetivo. Além disso, enfatizou que a efetividade desse arranjo depende de quatro pilares: coerência normativa entre termos de uso e obrigações legais; transparência ativa sobre resultados de moderação e mitigação de risco; mecanismos de auditoria e revisão independentes; e compromisso institucional das plataformas com a integridade eleitoral como valor público transversal.

4.2 EVOLUÇÃO NORMATIVA, DEVERES DAS PLATAFORMAS E DENSIFICAÇÃO DA LÓGICA PREVENTIVA

Nas **Partes I e II**, este relatório percorreu um percurso sobre a evolução legislativa e infralegal da regulação da propaganda eleitoral na internet, destacando que a Lei nº 13.488/2017 foi o marco central ao reconhecer explicitamente o ambiente digital como espaço legítimo de propaganda eleitoral e ao instituir o impulsionamento como categoria jurídica própria, como exceção restrita à vedação geral de propaganda eleitoral paga na internet. A partir dessa base, as resoluções do TSE passaram a densificar o regime, incorporando definições operacionais e instrumentos compatíveis com práticas reais do ecossistema digital, como disparos em massa, publicidade segmentada e amplificação algorítmica. O texto destaca que, embora o núcleo legal tenha permanecido relativamente estável desde 2017, a dinâmica regulatória foi deslocada para o plano infralegal, em razão da velocidade das transformações tecnológicas, com a Justiça Eleitoral exercendo competência normativa para atualização do regime conforme o cenário de cada ciclo eleitoral.

Nesse contexto, a Resolução TSE nº 23.732/2024 é tratada como uma alteração qualitativa: a regulação deixa de se limitar à propaganda eleitoral em sentido estrito e passa a abranger conteúdos político-eleitorais em sentido mais amplo, reforçando obrigações de transparência e de mitigação de riscos. O relatório ressalta o papel do art. 9º-D como núcleo do microssistema de integridade informacional, ao impor ao provedor de aplicação deveres de adoção e publicização de medidas para impedir ou diminuir a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam atingir a integridade do processo eleitoral. Entre esses deveres estão a elaboração e aplicação de termos de uso e políticas de conteúdo compatíveis com esse objetivo e a implementação de instrumentos eficazes de notificação e canais de denúncia acessíveis a usuários e instituições.

A análise também destacou que a lógica preventiva não se esgota em mecanismos de denúncia: **o dever de cuidado** exige ações estruturais de correção e prevenção, aprimoramento de sistemas de recomendação, transparência dos resultados das ações tomadas, relatórios e avaliações de impacto em ano eleitoral. Para que essas obrigações sejam verificáveis, o relatório recomenda densificação por métricas, periodicidade e formatos de publicação, além de auditorias independentes para plataformas de grande porte. A proposta subjacente é que, sem indicadores mensuráveis e documentação auditável, o modelo tende a ser simbólico, com baixa capacidade de fiscalização e controle público.

4.3 CORREGULAÇÃO E PLANOS DE CONFORMIDADE.

O relatório consolidou a visão de que o modelo brasileiro se aproxima de paradigmas híbridos observados em marcos internacionais, como o *Digital Services Act* (União Europeia),

o *Online Safety Act* (Reino Unido) e as *IT Rules* (Índia), os quais estruturam deveres escalonados, transparência e avaliações de risco, com mecanismos de enforcement e supervisão. O *benchmarking* foi utilizado como ferramenta para identificar parâmetros comparáveis e inspirar a densificação das obrigações no Brasil, considerando também a necessidade de adequação à realidade do Sul Global.

Um ponto enfatizado é o cadastro previsto no art. 29, §9º, relativo a provedores que pretendam prestar serviço de impulsionamento de propaganda eleitoral. O relatório interpretou esse dispositivo como instrumento de *accountability* institucional e rastreabilidade digital, funcionando como porta de entrada regulatória para que a Justiça Eleitoral saiba quais atores intermedeiam fluxos de impulsionamento e quais estruturas técnicas operam a amplificação de conteúdo político-eleitoral. A leitura proposta é que o cadastro não deve ser compreendido como formalidade burocrática, mas como obrigação de compliance contínuo, com atualização de dados e compromisso com transparência técnica e financeira, permitindo auditoria e prevenção de práticas ilícitas.

A partir disso, o relatório recomenda clarificar o escopo de quem deve se cadastrar, evitando que intermediários relevantes escapem por modelos contratuais ou estruturas técnicas; exigir atualização periódica a cada eleição ou quando houver mudanças relevantes; e criar repositório público e pesquisável no portal do TSE com lista de provedores cadastrados, informações básicas e status do cadastro, permitindo verificação por campanhas e cidadãos.

Por fim, na **parte III** apresentou-se uma tabela unificada de recomendações normativas e operacionais, organizada em blocos temáticos, com ênfase em governança e dever de cuidado, transparência ativa, fluxos de moderação e devido processo, e integridade algorítmica com regras específicas para IA e dados. Como diretriz transversal, sustentou-se a necessidade de disciplinar a granularidade das obrigações conforme critérios objetivos, impondo deveres mais rigorosos a plataformas e serviços de grande impacto informacional, com proporcionalidade e coerência regulatória.

O avanço das tecnologias de inteligência artificial generativa tem ampliado a complexidade técnica envolvida na identificação, na avaliação e na contextualização de conteúdos sintéticos potencialmente danosos à integridade do processo eleitoral.

Nesse contexto, sugere-se a inclusão de dispositivos à Resolução TSE nº 23.610/2019 voltados especificamente aos provedores de sistemas de inteligência artificial. Propõem-se, portanto, obrigações técnicas e procedimentais destinadas a (i) permitir a identificação confiável de conteúdos sintéticos, (ii) viabilizar a apuração célere de irregularidades durante o período eleitoral e (iii) mitigar riscos de uso abusivo dessas ferramentas para fins de desinformação.

Com o objetivo de criar instrumentos de corregulação para a conformidade de plataformas digitais aos deveres já estabelecidos na Resolução TSE nº 23.610/2019, recomendamos a inserção de uma proposta em suas Disposições finais. A ideia não é criar novas obrigações, mas dar condições ao Tribunal de acompanhar o cumprimento de regras já estabelecidas a partir de estruturas já existentes.

Como demonstrado abaixo, a inserção de um art. 125-B na Resolução TSE nº 23.610/2019 consolida, em caráter transversal e sistemático, um instrumento de conformidade eleitoral voltado ao acompanhamento do cumprimento de deveres já estabelecidos no ordenamento, sem criação de novas obrigações materiais. A experiência recente evidencia que a fiscalização baseada exclusivamente em respostas pontuais (remoções específicas, p ex.) é insuficiente para lidar com riscos sistêmicos associados à mediação digital do debate público, como a circulação massiva de desinformação, a opacidade de mecanismos de recomendação e a exploração econômica de conteúdos ilícitos ou irregulares no contexto eleitoral.

O plano de conformidade eleitoral previsto no caput traduz os deveres de diligência dispersos ao longo da Resolução em compromissos procedimentais verificáveis, permitindo que cada provedor explicite, de modo transparente, como pretende cumprir as obrigações constantes dos arts. 9-D, 9-E, 27-A, 28, 29, 30, 32, 33, 33-A, 33-B, 34, 36, 38, 39 e 40. Trata-se de mecanismo de corregulação, que preserva a autonomia técnica das plataformas na definição de soluções operacionais, ao mesmo tempo em que cria parâmetros objetivos de auditabilidade, acompanhamento contínuo e avaliação de resultados, compatíveis com o papel central desses agentes na organização do espaço público digital durante o processo eleitoral.

A atribuição conferida à Corregedoria-Geral Eleitoral no âmbito do art. 125-B harmoniza-se diretamente com as competências já fixadas na Resolução TSE nº 23.742/2024, que lhe atribui a instauração e condução de procedimentos administrativos voltados à elucidação de fatos que possam representar risco à normalidade, à legitimidade e à isonomia do pleito.

Ao centralizar na Corregedoria a disciplina dos planos de conformidade, sua avaliação e eventual requisição de ajustes, o dispositivo aproveita uma estrutura institucional vocacionada à fiscalização técnica e preventiva, capaz de acompanhar riscos sistêmicos, expedir provimentos vinculantes e assegurar execução uniforme das normas eleitorais, sem prejuízo das competências decisórias do Plenário e da atuação do Ministério Público Eleitoral.

Os parágrafos detalham um modelo de conformidade estruturado, proporcional e baseado em risco, no qual prazos e gatilhos procedimentais claros asseguram previsibilidade regulatória, enquanto a definição de conteúdo mínimo evita soluções meramente declaratórias. O desenho combina flexibilidade — com dispensas para atores que apresentem baixo risco e possibilidade de ajustes graduais –, supervisão responsiva e transparência pública, além de criar incentivos institucionais ao vincular a conformidade aos regimes de creden-

ciamento e cadastro já existentes. Em conjunto, o arranjo aproxima a Justiça Eleitoral de práticas consolidadas de supervisão adotadas por outros reguladores, como a ANPD, fortalecendo uma governança preventiva, auditável e compatível com a complexidade do ambiente digital.

4.4 IMPLEMENTAÇÕES E SUGESTÕES

1. Obrigação para empresas de IA[11]

1.1. Art. 9-B. (...)

[NOVO PARÁGRAFO - declaração para conteúdo sintético impulsionado]

§ 5o: Os provedores de aplicação que ofertem impulsionamento de conteúdo político-eleitoral deverão disponibilizar, no fluxo de contratação de anúncios, campo específico e destacado para declaração de uso de conteúdo sintético por inteligência artificial e para inserção do aviso exigido no caput, de modo a facilitar o cumprimento do dever de informação.

[NOVO PARÁGRAFO - obrigações específicas de empresas de IA]

§6. Os provedores de aplicação de internet que ofereçam ferramentas de geração de conteúdo sintético devem:

I - fornecer à Justiça Eleitoral informações sobre os melhores meios de identificação de conteúdos sintéticos;
II - aderir a padrões técnicos que permitam a identificação de conteúdos sintéticos de cunho político eleitoral produzidos pelos seus sistemas.
III – implementar mecanismos técnicos de marcação automática dos conteúdos gerados, em formato detectável por máquinas e perceptível por humanos;
IV – implementar salvaguardas que impeçam a geração de imagens realistas de candidatos ou autoridades eleitorais em contextos de violência, nudez ou atos ilícitos;
VII – manter canal de denúncia específico para comunicação de uso indevido de suas ferramentas para fins de desinformação eleitoral.

11 O CEDIS-IDP participou das audiências públicas sobre as resoluções do TSE aplicáveis para as eleições de 2026 levando uma série de diferentes propostas. Disponível em: https://www.youtube.com/watch?v=fiaObjJcDJQ

1.2 Art 9º-C. (...)

[ALTERAÇÃO DE REDAÇÃO - melhor definição de deep fakes e da norma proibitiva]

Art. 9º-C. É vedada a utilização, na propaganda eleitoral, em qualquer forma ou modalidade, de conteúdo sintético gerado ou modificado por meio de inteligência artificial ou outra tecnologia digital para difundir fatos notoriamente inverídicos, inexistentes ou gravemente descontextualizados com potencial para enganar eleitores ou causar danos ao equilíbrio do pleito ou à integridade do processo eleitoral.

§ 1º Essa vedação aplica-se a qualquer conteúdo em formato de imagem, áudio, vídeo, texto ou combinação destes, gerado ou modificado por meio de inteligência artificial ou outra tecnologia digital para:

I – criar, substituir ou alterar a aparência, voz, movimentos ou características biométricas de pessoa viva, falecida ou fictícia;
II – simular declarações, comportamentos, posicionamentos ou ações nunca realizados pela pessoa representada;
III – produzir ou modificar documentos, imagens, vídeos, áudios ou registros com aparência de autenticidade;
IV – manipular em tempo real a aparência ou voz de pessoa, fictícia ou real, viva ou morta, durante transmissões ao vivo (lives).

§ 2º A proibição do caput e do § 1º aplica-se ainda que:

I – haja autorização prévia da pessoa representada;
II – o conteúdo vise a favorecer, e não a prejudicar, determinada candidatura;
III – a manipulação seja parcial ou incida sobre elementos aparentemente secundários do conteúdo.

§ 3º Não se aplica a proibição do § 1º ao conteúdo que:
I – seja manifestamente satírico, paródico ou ficcional, desde que não induza razoavelmente o eleitor a acreditar em sua autenticidade;
II – constitua reconstituição histórica, educacional ou jornalística com divulgação inequívoca de sua natureza sintética, nos termos do art. 9º-B.

1.3 Art 9º-D (...)

[NOVO PARÁGRAFO - obrigações de empresas de IA]

Art. 9-D. (...) §6º. Os provedores de aplicação de internet que ofereçam ferramentas de geração de conteúdo sintético estão sujeitos, no que couber, aos deveres estabelecidos neste artigo.

14. Art 9º-E(...)

[NOVOS INCISOS - responsabilidade solidária]

Art. 9-E.(...) V – de divulgação ou compartilhamento de conteúdo sintético gerado ou modificado por inteligência artificial ou tecnologia digital congênere em desacordo com as regras de rotulagem e vedações previstas nesta Resolução;

VI – de utilização de sistemas de inteligência artificial ou tecnologias digitais congênere para produção de conteúdo sintético para disseminação em massa de desinformação eleitoral.

[NOVO ARTIGO - obrigações de provedores para conter desinformação por meio de IA]

[novo artigo] Art. 9-I É dever dos provedores de aplicação de internet que permitam a veiculação de conteúdo político-eleitoral adotar medidas de devida diligência qualificada para identificar, rotular e mitigar a circulação de conteúdo político-eleitoral gerado ou modificado por inteligência artificial ou tecnologia digital congênere que viole as disposições desta Resolução.

§ 1º As medidas de que trata o caput devem incluir, minimamente:

I – a implementação de sistemas de detecção automática de conteúdo sintético em áudio, vídeo e imagem;
II – a implementação de funcionalidade obrigatória que exija, no ato do carregamento (upload), a declaração do usuário quanto ao uso de inteligência artificial na produção do conteúdo;
III – a manutenção da integridade dos metadados e marcas d'água digitais que identifiquem a origem sintética do conteúdo, inclusive em compartilhamentos internos na plataforma;
IV – a disponibilização de canal de denúncia específico e prioritário para que candidatas, candidatos, seus representantes legais, ou partidos, federações e coligações reportem o uso não autorizado de sua imagem ou voz em conteúdos sintéticos;
V – a instituição de protocolo de análise humana e resposta em prazo não superior a 4 (quatro) horas durante o período eleitoral para as denúncias recebidas via canal prioritário;
VI – a publicização periódica de relatório de transparência contendo as medidas adotadas, volume de conteúdos removidos e métricas de eficácia.
§ 2º O provedor de aplicação que detectar conteúdo ilícito de que trata esta Resolução ou for notificado de sua circulação deverá adotar providências imediatas e eficazes para fazer cessar o impulsionamento, a monetização, a circulação e o acesso ao conteúdo.

§ 3º É vedado às ferramentas de inteligência artificial generativa apresentar ou listar seletivamente, recomendar, sugerir, priorizar, organizar, ou classificar, nomes, candidaturas, programas de governo, perfis, canais, rankings, enquetes, ou quaisquer conteúdos similares relacionados à candidatas, candidatos, partidos políticos, federações ou coligações, devendo tais ferramentas limitar-se à remissão a listas de candidaturas oficiais completas e demais fontes oficiais da Justiça Eleitoral.

2. Corregulação: exigência de planos de conformidade

21. Disposições finais

Art. 125-B. Os provedores de aplicação de internet deverão, nos termos, prazos e diretrizes editados pela Corregedoria-Geral Eleitoral, elaborar plano de conformidade eleitoral destinado à prevenção e mitigação de riscos à integridade do processo eleitoral e efetivo cumprimento das obrigações presentes nos artigos 9-D, 9-E, 27-A, 28, 29, 30, 32, 33, 33-A, 33-B, 34, 36, 38, 39 e 40 desta Resolução.

§ 1º O plano de conformidade deverá ser apresentado em até 30 (trinta) dias após abertura de procedimento administrativo conforme o artigo 6º da Resolução TSE nº 23.742, sem prejuízo de atualizações posteriores quando houver alteração relevante de riscos ou de funcionalidades da plataforma.

§ 2º O plano de conformidade deverá conter, no mínimo:

I - deveres e medidas de conformidade apontadas para cada disposição desta Resolução;
II - critérios e indicadores mensuráveis e periódicos para acompanhamento de sua implementação.
III – prazos, resultados esperados e trajetória de alcance.

§ 3º Compete à Corregedoria-Geral Eleitoral disciplinar os termos de dispensa de apresentação de planos de conformidade em razão do baixo risco representado por provedores de aplicação de internet de pequeno porte ou sem relevância para o pleito e os meios de participação de candidaturas, partidos políticos e entidades da sociedade civil organizada no âmbito do procedimento administrativo previsto no § 1º.

§ 4º Os planos de conformidade de provedores de aplicação de internet deverão ser públicos e acessíveis aos eleitores, ressalvados itens que a divulgação possa representar ameaça à integridade do processo eleitoral e aos sistemas de segurança implementados pelos provedores de aplicação de internet para cumprimento da legislação eleitoral.

§ 5º A Corregedoria-Geral Eleitoral poderá determinar o cumprimento de deveres não contemplados nos planos entregues, bem como requisitar emendas, novos indicadores de efetividade ou auditoria independente, observados porte, impacto e grau de risco da aplicação de internet.

§ 6º O cumprimento do disposto no neste artigo constitui requisito para o credenciamento de que trata o art. 27-A, § 4o, e para o cadastro previsto no art. 29, § 9o.

3. Cooperação Institucional entre o TSE e a ANPD

Art. xx – O Tribunal Superior Eleitoral (TSE) articular-se-á com a Agência Nacional de Proteção de Dados (ANPD) para atuar de forma coordenada e colaborativa para garantir a proteção de dados pessoais no contexto da propaganda eleitoral em meios digitais, especialmente no que se refere:

I – ao tratamento de dados pessoais por partidos políticos, coligações, federações, candidatos, plataformas digitais e prestadores de serviços de publicidade eleitoral;
II – à análise de práticas de perfilamento, microdirecionamento, técnicas de distribuição de anúncios ou exclusão de conteúdos político-eleitorais com base em dados pessoais;
III – à apuração de infrações relativas à proteção de dados no âmbito do processo eleitoral;
IV – à emissão de orientações técnicas, pareceres conjuntos e manuais de boas práticas voltados à conformidade com a LGPD no período eleitoral;
V – à fiscalização de repositórios de anúncios políticos, quando houver uso de dados pessoais no direcionamento de conteúdo.

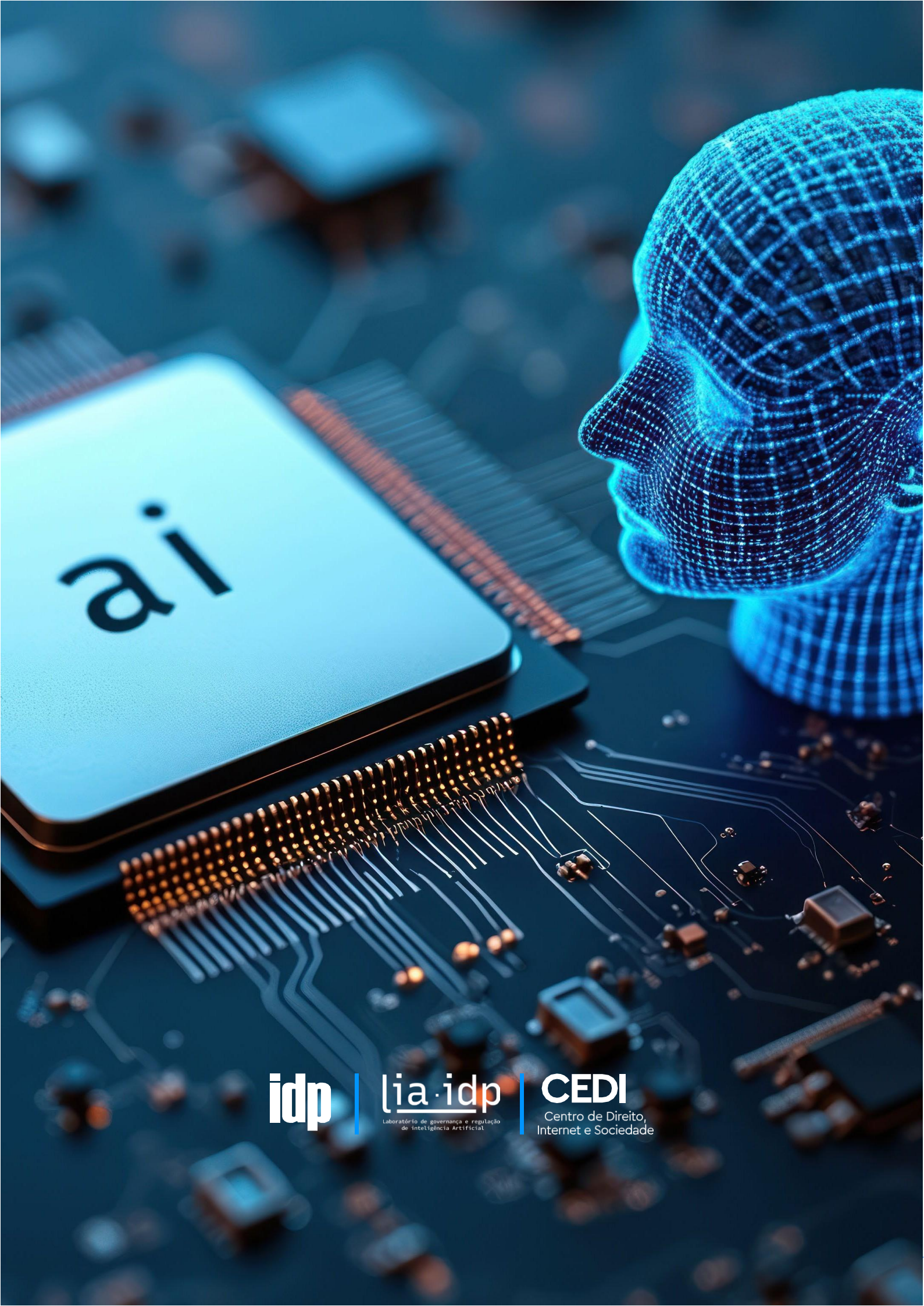
§1º. Para fins do disposto neste artigo, o TSE poderá firmar acordos de cooperação técnica, convênios ou instrumentos congêneres com a ANPD, com o objetivo de:

I – promover a troca de informações técnicas, regulatórias e de inteligência institucional;
II – estabelecer fluxos de comunicação e interoperabilidade de sistemas, respeitado o sigilo das informações e os princípios da finalidade e da minimização de dados;
III – coordenar ações de fiscalização, auditoria ou investigação conjunta, conforme suas competências legais e regulatórias;
IV – realizar programas conjuntos de capacitação, formação e eventos públicos voltados à integridade da informação eleitoral e à proteção de dados pessoais.

§2º. O TSE e a ANPD poderão instituir grupos de trabalho conjuntos, com representantes indicados por ambas as instituições, para a elaboração de estudos técnicos, guias, resoluções normativas e mecanismos de supervisão compartilhada no contexto eleitoral.

§3º. As ações decorrentes da cooperação institucional observarão os princípios da legalidade, necessidade, proporcionalidade, segurança, transparência e responsabilização, assegurando-se a proteção dos direitos dos titulares de dados e a integridade do processo eleitoral.

§4º. A atuação conjunta prevista neste artigo não afasta a autonomia decisória e fiscalizatória de cada órgão no exercício de suas competências constitucionais e legais, devendo prevalecer a cooperação institucional em regime de respeito mútuo e complementaridade.



idp | lia·idp
Laboratório de governança e regulação de inteligência Artificial
| CEDI
Centro de Direito, Internet e Sociedade