



CONTRIBUIÇÃO DATA PRIVACY BRASIL MINUTA PROPAGANDA ELEITORAL [RESOLUÇÃO TSE Nº 23.732/2024]

Bruno Bioni, Carla Rodrigues, Eduardo Mendonça,
Natasha Nóvoa e Rafael Zanatta

Fevereiro de 2026

Sobre a Data

A Data Privacy Brasil é uma organização que nasce da união entre uma escola e uma associação civil em prol da promoção da cultura de proteção de dados e direitos digitais no Brasil e no mundo. Fundada em 2018, a Data Privacy Brasil Ensino surgiu como um espaço para difundir e inovar no conhecimento sobre privacidade e proteção de dados no país. Com conteúdo adaptado para uma linguagem mais prática, com exercícios e estudos de caso, trata-se de uma escola para todos aqueles que se interessam e querem se aprofundar na temática da privacidade, proteção de dados e novas tecnologias.

A Associação Data Privacy Brasil de Pesquisa é uma organização da sociedade civil, sem fins lucrativos e suprapartidária, que promove a proteção de dados pessoais e outros direitos fundamentais a partir de uma perspectiva de justiça social e das assimetrias de poder.

A partir de 2023, as duas instituições se uniram para formar uma única organização, mantendo os mesmos princípios e atividades. Com o apoio de uma equipe multidisciplinar, realizamos formações, eventos, certificações, consultorias, conteúdos multimídia, pesquisas de interesse público e auditorias cívicas para a promoção de direitos em uma sociedade datificada marcada por assimetrias e injustiças. Por meio da educação, da sensibilização e da mobilização da sociedade, buscamos uma sociedade democrática em que as tecnologias estejam a serviço da autonomia e dignidade das pessoas.

Ficha técnica

Direção

Bruno Bioni, Mariana Rielli e Rafael Zanatta

Coordenação

Carla Rodrigues, Jaqueline Pigatto, Pedro Martins, Pedro Saliba e Victor Barcellos

Equipe

Barbara Yamasaki, Bianca Marques Eduardo Mendonça, Gabriela Vergili, Giovana Andrade, Isabelle Santos, João Paulo Vicente, Larissa Pacheco, Louise Karczeski, Luize Ribeiro, Matheus Arcanjo, Natasha Nóvoa, Pedro Henrique, Rafael Guimarães, Rennan Willian, Rodolfo Rodrigues e Vinicius Silva

Licença

Creative Commons

É livre a utilização, circulação, ampliação e produção de documentos derivados desde que citada a fonte original e para finalidades não comerciais.

Imprensa

Para esclarecimentos sobre o documento e entrevistas, entrar em contato pelo e-mail imprensa@dataprivacy.br.org

Introdução

A contribuição apresentada foi elaborada com base na expertise acumulada pela Data Privacy Brasil no acompanhamento dos impactos das tecnologias digitais sobre direitos fundamentais, democracia e processos eleitorais. Essa atuação inclui a produção do [relatório DivulgaCandContas e proteção de dados nas eleições: contribuições ao Superior Tribunal Eleitoral](#) em parceria com o IntenetLab, a participação na [audiência pública sobre as resoluções das eleições de 2024](#), com envio de [contribuições escritas à minuta de resolução sobre propaganda eleitoral](#) (Resolução nº 23.610, de 18 de dezembro de 2019) em 2024.

Soma-se a esse histórico o projeto [Eleições, desinformação e ilícito de dados](#), desenvolvido em 2022, e do [Observatório IA nas Eleições](#), em parceria com o Aláfia Lab, que mapeia o uso de inteligência artificial gerativa na produção, amplificação ou manipulação de conteúdos de conotação política com potencial impacto sobre a democracia brasileira desde as eleições municipais de 2024. A organização atua de forma contínua na análise das interações entre proteção de dados pessoais, sistemas automatizados, modelos de negócio das plataformas digitais e seus efeitos sobre a esfera pública, especialmente em contextos de alta sensibilidade democrática, como os períodos eleitorais.

Nesse contexto, as sugestões apresentadas buscam enfatizar a necessidade de critérios normativos mais objetivos e de salvaguardas regulatórias específicas que preservem, simultaneamente, a integridade do processo eleitoral, a isonomia entre candidaturas, partidos e demais atores políticos, e o exercício legítimo da liberdade de expressão. Nessa linha, busca-se fortalecer e atualizar o arcabouço normativo à luz das transformações observadas no ecossistema digital desde sua edição e das lições extraídas dos últimos ciclos eleitorais.

As sugestões ora apresentadas foram submetidas no âmbito da consulta pública promovida pelo Tribunal Superior Eleitoral, realizada entre 19 e 30 de janeiro de 2026, e refletem o compromisso da Data Privacy Brasil com o aprimoramento democrático da regulação eleitoral, com base em evidências, princípios de direitos fundamentais e na centralidade da proteção de dados pessoais para a integridade informacional das eleições. A organização seguirá contribuindo com o debate por meio de sua participação na audiência pública relativa à minuta de resolução sobre propaganda eleitoral deste ano.

A seguir, apresentam-se os principais pontos propostos pela Data Privacy Brasil no âmbito desta consulta pública. O texto de referência adotado é a própria [Resolução nº 23.732/2024](#), que disciplina a propaganda eleitoral, inclusive no ambiente digital.

Parte I – Impulsioneamento, Algoritmos e Ordem Informacional Democrática

Art. 3º-B. O impulsioneamento pago de conteúdo político-eleitoral relacionado aos atos previstos no caput e nos incisos do art. 3º desta Resolução somente é permitido durante a pré-campanha quando cumpridos cumulativamente os seguintes requisitos: (Redação dada pela Resolução nº 23.732/2024)

I - o serviço seja contratado por partido político, federação ou pela pessoa natural que pretenda se candidatar diretamente com o provedor de aplicação, com identificação, de forma inequívoca, de que se trata de conteúdo impulsioneado, que deve manter repositório público com dados sobre o impulsioneamento (Resolução TSE nº 23.732/2024, art. 27-A);

II - não haja pedido explícito de voto; (Incluído pela Resolução nº 23.732/2024)

III - os gastos sejam moderados, proporcionais e transparentes; (Incluído pela Resolução nº 23.732/2024)

IV - sejam observadas as regras aplicáveis ao impulsioneamento durante a campanha. (Incluído pela Resolução nº 23.732/2024)

Novo item proposto pelo TSE: Parágrafo único. Não caracteriza propaganda eleitoral antecipada negativa a crítica ao desempenho da administração pública, realizada por pessoa natural, ainda que ocorra a contratação de impulsioneamento, desde que ausentes elementos relacionados à disputa eleitoral.

Proposta minuta	Sugestão da Data Privacy Brasil
<p>Art. 3º-B. O impulsioneamento pago de conteúdo político-eleitoral relacionado aos atos previstos no caput e nos incisos do art. 3º desta Resolução somente é permitido durante a pré-campanha quando cumpridos cumulativamente os seguintes requisitos: (Redação dada pela Resolução nº 23.732/2024)</p> <p>Parágrafo único. Não caracteriza propaganda eleitoral antecipada negativa a crítica ao desempenho da administração pública, realizada por pessoa natural, ainda que ocorra a contratação de impulsioneamento, desde que ausentes elementos relacionados à disputa eleitoral.</p>	<p>Supressão do parágrafo único.</p>

Justificativa

A supressão do parágrafo único proposto pelo TSE mostra-se necessária, uma vez que a redação apresentada é ampla e indeterminada, carece de critérios objetivos que orientem sua aplicação, o que pode gerar insegurança jurídica e abrir margem ao uso do impulsionamento pago como instrumento indireto de propaganda eleitoral antecipada negativa. A formulação proposta torna o comando normativo indefinido e imprevisível, sobretudo quando confrontada com precedentes da Justiça Eleitoral que reconheceram como ilícitas estratégias de comunicação política notadamente envolvendo a atuação de influenciadores na difusão de cortes de conteúdo.

Em casos como os envolvendo Pablo Marçal¹, entendeu-se que conteúdos produzidos e divulgados por terceiros, ainda que sem pedido explícito de voto, podem configurar ilícito eleitoral quando inseridos em estratégia de promoção política antecipada. Situação semelhante foi observada no caso do Banco Master², no qual campanhas publicitárias formalmente desvinculadas da disputa eleitoral foram interpretadas como comunicação política indireta apta a influenciar o debate público em período sensível. Especialmente nas plataformas digitais, críticas aparentemente neutras à administração pública podem funcionar como mecanismos indiretos e antecipados de disputa eleitoral, com potencial de gerar impactos relevantes à integridade do processo eleitoral.

No contexto do ambiente digital contemporâneo, o impulsionamento pago não se limita à ampliação neutra de alcance de manifestações individuais. Trata-se de mecanismo inserido em um ecossistema informacional estruturado por algoritmos de recomendação, modelos de monetização por engajamento e técnicas avançadas de segmentação de públicos. Nessa realidade, a crítica política impulsionada passa a operar segundo lógicas típicas de campanhas profissionais de comunicação política, potencializando o impacto das mensagens e sua capacidade de influenciar a formação da opinião pública de forma direcionada e escalável.

Registre-se que, no ambiente digital, o impulsionamento pago integra um ecossistema informacional algorítmico e orientado ao engajamento, próximo às dinâmicas de campanhas profissionais. A proposta de supressão vai ao encontro do conceito de “ecossistema de informação” do Fórum Information & Democracy (Mansell et al., 2025), voltada à proteção da integridade eleitoral, desigualdades e da igualdade entre os atores políticos, preservada a liberdade de crítica com salvaguardas adequadas (Silberschneider, 2023; Szporer et al., 2024).

Deve-se reconhecer que o debate público contemporâneo é mediado por plataformas digitais, algoritmos de recomendação e modelos de monetização baseados em engajamento. Ao

¹ Como exemplo, cita-se o Processo 0600563-67.2024.6.26.0002 (TRE/SP), originário de ação proposta pelo prefeito de São Paulo/SP, Ricardo Nunes, em face de Pablo Marçal, por divulgação de conteúdo eleitoral ofensivo e inverídico na internet durante as eleições de 2024. Disponível em: <https://www.tre-sp.jus.br/comunicacao/noticias/2025/Marco/marcal-e-condenado-a-multa-de-r-15-mil-por-video-contra-nunes>. Acesso em 5 de fev. 2026.

² O caso do Banco Master envolve investigações sobre eventuais irregularidades financeiras que também estão sendo utilizadas em disputas de narrativas no ambiente digital, inclusive no contexto de campanha, levantando questões sobre os limites da propaganda eleitoral na internet. Disponível em: <https://agenciabrasil.ebc.com.br/politica/noticia/2026-02/senado-ins-tala-comissao-para-apurar-fraudes-do-banco-master>. Acesso em 5 de fev. 2026.

permitir o impulsionamento de conteúdos políticos por perfis sem vínculo formal nas campanhas, ampliam-se os riscos de uso estratégicos e assimétricos desses mecanismos, inclusive para difusão de conteúdos enganosos ou imprecisos, discurso de ódio e práticas que comprometam a integridade do debate público.



Parte II – Da suspensão e remoção de perfis e conteúdos

Art. 36. A requerimento do Ministério Público, de candidata, candidato, partido político, federação ou coligação, observado o rito previsto no art. 96 da Lei nº 9.504/1997, a Justiça Eleitoral poderá determinar, no âmbito e nos limites técnicos de cada aplicação de internet, a suspensão do acesso a todo conteúdo veiculado que deixar de cumprir as disposições da Lei nº 9.504/1997, devendo o número de horas de suspensão ser definido proporcionalmente à gravidade da infração cometida em cada caso, observado o limite máximo de 24 (vinte e quatro) horas (Lei nº 9.504/1997, art. 57-I; e Constituição Federal, art. 127). (Redação dada pela Resolução nº 23.671/2021)



§ 1º A cada reiteração de conduta, será duplicado o período de suspensão (Lei nº 9.504/1997, art. 57-I, § 1º).

§ 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 nº 9.504/1997, no âmbito e nos limites técnicos de cada provedor de aplicação de internet.

Novo item proposto pelo TSE: § 3º A remoção de perfis somente deve ser aplicada quando se tratar de usuário comprovadamente falso, relacionado a pessoa que sequer existe fora do mundo virtual (perfil automatizado ou robô) ou cuja as publicações estejam voltadas ao cometimento de crime.

Proposta minuta	Sugestão da Data Privacy Brasil
§ 3º A remoção de perfis somente deve ser aplicada quando se tratar de usuário comprovadamente falso, relacionado a pessoa que sequer existe fora do mundo virtual (perfil automatizado ou robô) ou cuja as publicações estejam voltadas ao cometimento de crime.	Parágrafo único. A ordem judicial de remoção deve indicar objetivamente o conteúdo ilícito e o nexo causal que justifique a exclusão de todo o perfil, em vez de apenas postagens específicas.

Justificativa

A inclusão do § 3º no art. 36 prevê a remoção de perfis, medida mais gravosa do que a suspensão temporária ou a retirada de conteúdo específico. Por isso, deve ser excepcional, proporcional e motivada. Sua adoção deve ficar restrita a hipóteses justificadas, com indicação mínima dos elementos que a sustentam, e precisa respeitar a atuação no âmbito e nos limites técnicos de cada aplicação, evitando ordens amplas ou inexecutáveis que ultrapassem o necessário para cessar a irregularidade.



Essa diretriz se harmoniza com o art. 57-I da Lei nº 9.504/1997, que subordina a suspensão ao art. 96, exige proporcionalidade à gravidade do caso, fixa teto temporal e prevê agravamento na reiteração. O desenho favorece resposta graduada e temporária; nesse marco, é coerente tratar a remoção de perfis como providência excepcional, pois seus efeitos são mais abrangentes e menos reversíveis. A medida demanda nexo demonstrável com a conduta apontada e a insuficiência de alternativas menos restritivas, sobretudo em período eleitoral.

Nesse sentido, o parágrafo único exige que a ordem indique objetivamente o conteúdo ilícito e o nexo causal que justifique excluir o perfil, e não apenas postagens, permitindo cumprimento tecnicamente delimitado e controle posterior. Isso reforça a rastreabilidade já prevista no art. 9º-G da Resolução TSE nº 23.610/2019. Literatura sobre integridade informacional e estudos no Brasil indicam que a identificação de contas inautênticas e bots depende de evidências e múltiplos critérios, o que recomenda evitar remoções amplas sem lastro verificável. Assim, o § 3º qualifica a intervenção e preserva a tutela eleitoral sem restringir indevidamente a participação política, a liberdade de expressão e o debate público.

A exigência de que a ordem judicial indique objetivamente o conteúdo ilícito e o nexo causal que justifique a exclusão integral do perfil também encontra respaldo em evidências empíricas e análises comparadas sobre a aplicação de medidas de remoção no contexto eleitoral digital. O relatório [Current Challenges in Digital Elections](#), do Weizenbaum Institute, recomenda o desenvolvimento de definições operacionais para conceitos-chave, a fim de assegurar aplicação consistente e dar orientação de conformidade para plataformas e campanhas. A experiência analisada no relatório, especialmente em relação a “deepfakes” e às dinâmicas de “virality”, demonstra que a ausência de critérios operacionais mínimos ampliou a variação interpretativa e a incerteza quanto aos limites de conformidade, dificultando a fiscalização e a aplicação consistente das regras em razão de interpretações divergentes e de ordens excessivamente genéricas.

Estudos aplicados ao cenário eleitoral brasileiro também reforçam a necessidade de rigor. Dias, Doca e Silva (p. 31, 2021) indicam que contas automatizadas podem aprender a linguagem digital e “copiar sua forma de interagir”, o que dificulta distinguir automação de comportamento humano apenas por sinais superficiais. Santos et al. (2021) propõem “incluir múltiplos critérios” e destacam abordagens combinadas, como análise estrutural de rede e análise lexical, para identificar contas com comportamento total ou parcialmente automatizado. Nesse contexto, recomenda-se evitar remoções amplas sem lastro mínimo, sobretudo em período eleitoral, e condicionar a medida a elementos verificáveis.

Assim, o § 3º, em conjunto com o parágrafo único proposto, deve operar como mecanismo de contenção e qualificação da intervenção judicial. Ao exigir a demonstração do caráter inautêntico ou automatizado da conta, bem como a explicitação do nexo causal entre a conduta identificada e a exclusão do perfil, a norma reduz o espaço para erros de enquadramento e assimetrias de aplicação, reforça a proporcionalidade da resposta estatal e viabiliza controle posterior das decisões. Com isso, preserva-se a efetividade da tutela eleitoral e a capacidade de resposta a abusos informacionais, sem impor restrições indevidas à participação política e ao debate público.

Além das sugestões formuladas no âmbito dos dispositivos expressamente indicados na minuta submetida à consulta pública, a Data Privacy Brasil também apresenta novas propostas de aprimoramento normativo relacionadas à Resolução TSE nº 23.732/2024, que promoveu atualizações relevantes na Resolução TSE nº 23.610/2019, a qual dispõe sobre a propaganda eleitoral

Essas propostas adicionais decorrem da compreensão de que as alterações recentemente incorporadas ao regime jurídico da propaganda eleitoral, especialmente no que se refere ao uso de plataformas digitais, impulsionamento de conteúdo e práticas de comunicação política mediadas por sistemas automatizados, demandam ajustes complementares e maior densidade regulatória. Também incluímos nossas recomendações específicas aos provedores de sistemas de IA. O objetivo é assegurar coerência sistêmica entre os dispositivos vigentes, reforçar a proteção de direitos fundamentais, em especial a proteção de dados pessoais e a integridade informacional, e mitigar riscos associados a estratégias opacas dos sistemas de IA para influência política no ambiente digital.

Minuta Resolução nº 23.732/2024	Proposta da Data privacy Brasil
<p>Art. 3º-B. O impulsionamento pago de conteúdo político-eleitoral relacionado aos atos previstos no caput e nos incisos do art. 3º desta Resolução somente é permitido durante a pré-campanha quando cumpridos cumulativamente os seguintes requisitos:</p> <p>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.</p> <p>§ 1º As informações mencionadas no caput deste artigo devem ser feitas em formato compatível com o tipo de veiculação e serem apresentadas:</p> <p>I – no início das peças ou da comunicação feitas por áudio;</p> <p>II – por rótulo (marca d'água) e na audiodescrição, nas peças que consistam em imagens estáticas;</p>	<p>§2º O disposto no caput e no §1º deste artigo não se aplica: (Incluído pela Resolução nº 23.732/2024)</p> <p>I - aos ajustes destinados a melhorar a qualidade de imagem, som e vídeo; (Incluído pela Resolução nº 23.732/2024)</p> <p>II - à produção de elementos gráficos de identidade visual, vinhetas e logomarcas; (Incluído pela Resolução nº 23.732/2024)</p> <p>III - a recursos de marketing de uso costumeiro em campanhas, como a montagem de imagens em que pessoas candidatas e apoiadoras aparentam figurar em registro fotográfico único utilizado na confecção de material impresso e digital de propaganda. (Incluído pela Resolução nº 23.732/2024)</p> <p>§ 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, devendo ser identificado de forma clara que se trata de sistema automatizado, vedada qualquer simulação de interlocução com a pessoa candidata ou outra pessoa real, assegurada a possibilidade de encerramento da interação automatizada. (Incluído pela Resolução nº 23.732/2024)</p>

<p>III – na forma dos incisos I e II desse parágrafo, nas peças ou comunicações feitas por vídeo ou áudio e vídeo;</p> <p>IV – em cada página ou face de material impresso em que utilizado o conteúdo produzido por inteligência artificial.</p> <p>§2º O disposto no caput e no §1º deste artigo não se aplica: (Incluído pela Resolução nº 23.732/2024)</p> <p>I - aos ajustes destinados a melhorar a qualidade de imagem ou de som; (Incluído pela Resolução nº 23.732/2024)</p> <p>II - à produção de elementos gráficos de identidade visual, vinhetas e logomarcas; (Incluído pela Resolução nº 23.732/2024)</p> <p>III - a recursos de marketing de uso costumeiro em campanhas, como a montagem de imagens em que pessoas candidatas e apoiadoras aparentam figurar em registro fotográfico único utilizado na confecção de material impresso e digital de propaganda. (Incluído pela Resolução nº 23.732/2024)</p> <p>§ 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 nº 23.732/2024)</p> <p>§ 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. (Incluído pela Resolução nº 23.732/2024)</p> <p>§ 5º, § 6º – Não correspondente</p>	<p>§ 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, com transparência quanto aos fundamentos da medida, notificação imediata ao responsável pela propaganda e indicação dos meios para sua contestação, sem prejuízo de apuração nos termos do § 2º do art. 9º-C desta Resolução. (Incluído pela Resolução nº 23.732/2024)</p> <p>§ 5º O aviso referido no caput deverá ser apresentado em linguagem simples, com tamanho e contraste adequados, e com recursos de acessibilidade, inclusive legenda, audiodescrição e Libras, quando compatíveis com o meio.</p> <p>§ 6º Sempre que tecnicamente possível, o aviso referido no caput deverá também constar em metadados ou marca persistente associada ao arquivo, de forma a permanecer identificável em republicações, recortes e reenvios.</p>
--	--

Justificativa

As disposições propostas nos §§ 2º a 6º buscam conferir precisão normativa, proporcionalidade e efetividade às regras sobre o uso de inteligência artificial e conteúdos sintéticos na propaganda eleitoral, ao mesmo tempo em que reduzem riscos de censura excessiva e de insegurança jurídica. Os ajustes meramente técnicos de imagem e som, de elementos gráficos de identidade visual e de recursos de marketing tradicionalmente utilizados em campanhas (§ 2º) delimita de forma objetiva o escopo da norma, evitando interpretações expansivas que poderiam inviabilizar práticas legítimas e consolidadas de comunicação política, sem impacto relevante sobre a percepção do eleitor ou sobre a autenticidade da mensagem política.

A disciplina específica do uso de chatbots, avatares e conteúdos sintéticos (§ 3º) enfrenta diretamente um dos principais vetores de risco à integridade do processo eleitoral no ambiente digital, que é a simulação de interlocução humana e a indução do eleitor a erro quanto à natureza da comunicação. Estudo conduzido por 22 organizações de mídia, em 2025, entre elas a DW e a BBC do Reino Unido, [avaliou respostas fornecidas por quatro dos assistentes de inteligência artificial mais utilizados no mercado](#) (Copilot, da Microsoft; Gemini, do Google; e Perplexity AI) e constatou que 45% das respostas apresentavam ao menos um problema significativo, 31% continham atribuições de fontes confusas e 20% havia erros factuais graves.

Esses riscos são agravados pelo fenômeno conhecido como “alucinação algorítmica”, no qual sistemas automatizados produzem informações equivocadas, narrativas falsas ou imagens irreais, podendo inclusive atribuir fatos inexistentes a pessoas reais ou simular comportamentos humanos com o objetivo de induzir confiança indevida - o termo “alucinar” abrange práticas como a invenção de informações, a ocultação de incertezas ou a afirmação falsa da condição humana do sistema - (Lemos, 2024). Nesse contexto, a exigência de identificação clara do caráter automatizado da interação, a vedação à simulação de comunicação com a pessoa candidata ou com terceiros reais e a garantia de encerramento da interação automatizada concretizam os princípios da transparência, da boa-fé informacional e da autonomia do eleitor, além de estarem em consonância com padrões internacionais de governança de sistemas automatizados.

Proposta minuta	Sugestão da Data Privacy Brasil
Art. 9º-C É vedada a utilização, na propaganda eleitoral, qualquer que seja sua forma ou modalidade, de conteúdo fabricado ou manipulado para difundir fatos notoriamente inverídicos ou descontextualizados com potencial para causar danos ao equilíbrio do pleito ou à integridade do processo eleitoral. (Incluído pela Resolução nº 23.732/2024)	Art. 9º-C É vedada a utilização, na propaganda eleitoral, qualquer que seja sua forma ou modalidade, de conteúdo fabricado ou manipulado para difundir fatos notoriamente inverídicos ou descontextualizados com potencial para causar danos ao equilíbrio do pleito ou à integridade do processo eleitoral. (Incluído pela Resolução nº 23.732/2024)

§ 1º É proibido o uso, para prejudicar ou para favorecer candidatura, de conteúdo sintético em formato de áudio, vídeo ou combinação de ambos, que tenha sido gerado ou manipulado digitalmente, ainda que mediante autorização, para criar, substituir ou alterar imagem ou voz de pessoa viva, falecida ou fictícia (deep fake). (Incluído pela Resolução nº 23.732/2024)

§ 2º O descumprimento do previsto no caput e no § 1º deste artigo configura abuso do poder político e uso indevido dos meios de comunicação social, acarretando a cassação do registro ou do mandato, e impõe apuração das responsabilidades nos termos do § 1º do art. 323 do Código Eleitoral, sem prejuízo de aplicação de outras medidas cabíveis quanto à irregularidade da propaganda e à ilicitude do conteúdo. (Incluído pela Resolução nº 23.732/2024)

§ 1º É proibido o uso, para prejudicar ou para favorecer candidatura, de conteúdo sintético em formato de áudio, vídeo ou combinação de ambos, que tenha sido gerado ou manipulado digitalmente, ainda que mediante autorização, para criar, substituir ou alterar imagem ou voz de pessoa viva, falecida ou fictícia (deep fake e variações como deepnude). (Incluído pela Resolução nº 23.732/2024)

§ 1º-B O provedor de aplicação que disponibilize ferramentas de inteligência artificial capazes de gerar ou manipular áudio, vídeo ou imagem deverá adotar medidas técnicas e de governança, proporcionais ao risco, para prevenir e mitigar a produção e a circulação de deep fakes vedados no § 1º. Devem ser incluídos mecanismos de bloqueio ou redução de funcionalidade em cenários de abuso, medidas de detecção, identificação e rastreabilidade do conteúdo gerado e canal efetivo e acessível de reporte, correção e revisão.

§ 1º-C As avaliações relativas aos modelos, sistemas e ferramentas de inteligência artificial de que trata o § 1º-B deverão considerar o estado da arte do desenvolvimento tecnológico para gestão de riscos conhecidos e razoavelmente previsíveis, inclusive com avaliadores independentes e exercícios de red-teaming, para medir desempenho e identificar vulnerabilidades.

§ 1º-D Verificada a circulação de conteúdo vedado no § 1º ou determinada judicialmente a sua indisponibilização, o provedor deverá promover a suspensão, em caráter imediato e permanente, de toda e qualquer conta envolvida:

I - na produção do conteúdo vedado, valendo-se de suas ferramentas;

II - no compartilhamento reiterado ou exclusivamente desse tipo de conteúdo, proibindo que os responsáveis criem novas contas na plataforma no futuro, mediante medidas técnicas razoáveis e proporcionais; e

III - encaminhar semanalmente à Justiça Eleitoral relatório com as métricas de implementação do disposto neste parágrafo, em formato agregado e sem identificação de usuários, contendo, no mínimo:

- a) número de contas suspensas nos termos dos incisos I e II;
- b) número de tentativas de recriação de contas impedidas ou mitigadas por medidas técnicas;
- c) tempo médio de resposta entre reporte/ordem e a adoção de medidas; e
- d) número de contestações, revisões e reversões das medidas adotadas.

§ 1º-E Na hipótese do § 1º-C, o provedor deverá preservar registro mínimo de evidências necessárias à revisão e ao controle, observada a proteção de dados pessoais.

§ 1º-F A decisão judicial deverá indicar objetivamente o conteúdo, o nexos entre a manipulação e o risco eleitoral e, quando aplicável, a inadequação de medidas menos restritivas.

§ 2º O descumprimento do previsto no caput e no § 1º deste artigo configura abuso do poder político e uso indevido dos meios de comunicação social, acarretando a cassação do registro ou do mandato, e impõe apuração das responsabilidades nos termos do § 1º do art. 323 do Código Eleitoral, sem prejuízo de aplicação de outras medidas cabíveis quanto à irregularidade da propaganda e à ilicitude do conteúdo. (Incluído pela Resolução nº 23.732/2024)

§3º Para fins de análise célere e instrução técnica relativa a conteúdos vedados neste artigo, o provedor de aplicação deverá, quando requisitado pela Justiça Eleitoral, disponibilizar acesso a dados e informações necessários e proporcionais, inclusive por meio de interfaces dedicadas (API) ou outros meios adequados.

§4º Poderão ser credenciadas instituições acadêmicas, científicas, tecnológicas, de inovação ou jornalísticas, conforme critérios e requisitos definidos em regulamento, para acessar dados necessários para à realização de pesquisas sobre os impactos de sistemas de inteligência artificial sobre a integridade do processo eleitoral, vedada a utilização desses dados para quaisquer finalidades comerciais e assegurado o cumprimento dos princípios da finalidade, da necessidade, da segurança e da confidencialidade das informações.

Justificativa

A evolução recente das tecnologias de geração e manipulação de mídia torna mais provável a circulação de conteúdos sintéticos com capacidade de causar danos graves e, muitas vezes, irreversíveis à integridade do processo eleitoral. Nesses cenários, medidas reativas e pontuais (conteúdo a conteúdo) tendem a ser insuficientes, especialmente quando a própria infraestrutura técnica do provedor facilita a criação e a rápida replicação do material ilícito. Por isso, é necessário explicitar obrigações de prevenção e mitigação proporcionais ao risco, alinhadas ao estado da arte de governança.

A inclusão de referência a deepfake e variações funcionalmente equivalentes, como deepnude, responde ao uso de sistemas generativos para produzir representações fraudulentas em contextos sexualizados, inclusive com potencial de dano grave a direitos fundamentais. Em linha, a recomendação conjunta relativa ao caso Grok³ reforça que respostas eficazes passam por medidas técnicas e operacionais e pela aplicação consequente de políticas de plataforma, inclusive com suspensão imediata e permanente de contas envolvidas e medidas para impedir a recriação de novas contas com mesma finalidade.

Nesse sentido, os §§ 1º-B e 1º-C propõem deveres mínimos de governança para provedores que disponibilizam ferramentas de IA capazes de gerar ou manipular áudio, vídeo ou imagem, com foco em prevenir e mitigar a produção e a circulação do conteúdo vedado, bem como interromper o vetor de abuso. A medida reconhece o dever de providências imediatas e eficazes, bem como a apuração de perfis e contas envolvidos para impedir nova circulação e inibir comportamentos ilícitos.

Além disso, o § 1º-C explicita que a governança desses modelos e sistemas deve incorporar práticas compatíveis com o estado da arte de gestão de riscos conhecidos e razoavelmente previsíveis, incluindo avaliações com participação de avaliadores independentes e exercícios de red-teaming, de modo a medir desempenho e identificar vulnerabilidades antes e durante

3 Objeto da Nota Técnica nº 1/2026/FIS/CGF/ANPD, no Processo SEI nº 00261.000178/2026-27 (Representação nº 01-2026, envolvendo X Corp. e X Brasil Internet Ltda., com petição complementar apresentada pela Deputada Federal Erika Hilton). Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnica-no-1-2026-fis-cgf-anpd.pdf>. Acesso em 5 de fev. 2026.

a oferta das ferramentas. Essa previsão reforça uma abordagem preventiva baseada em risco, adequada à escala e à velocidade de disseminação típica de conteúdos sintéticos.

D

Os §§ 1-D e 1-E equilibram a efetividade e garantias: (i) exigem preservação de registro mínimo de evidências, para viabilizar revisão, controle e contraditório, em linha com modelo já previsto de armazenamento de conteúdo e metadados pertinentes em repositório, com regras de sigilo e acesso restrito; e (ii) reforçam o dever de fundamentação objetiva, com indicação do conteúdo e do nexó entre manipulação e o risco eleitoral, evitando medidas excessivas e aumentando a segurança jurídica. Adicionalmente, o inciso III do § 1º-D introduz um dever de reporte mensal de métricas à Justiça Eleitoral, em formato agregado e sem identificação de usuários, permitindo aferir o grau de implementação das medidas, a capacidade de resposta a reportes e ordens, a eficácia de mecanismos anti-reincidência, como a mitigação de recriação de contas, e a existência de salvaguardas procedimentais por meio de dados sobre contestações, revisões e reversões, o que contribui simultaneamente para a efetividade e para a redução de riscos de remoções indevidas.

Ademais, o § 3º consolida um arranjo institucional voltado à análise célere, identificação, atribuição e mitigação de conteúdos sintéticos vedados, mediante força-tarefa técnica e credenciamento prévio de especialistas, centros de pesquisa universitários e organizações da sociedade civil, com inspiração no modelo de vetted-access do Digital Services Act (vetted-access é um acesso supervisionado e controlado a dados de plataformas digitais, concedido apenas a pesquisadores que passaram por um processo de seleção e validação pelas autoridades competentes)⁴.

D

Nesse mesmo sentido, a proposta incorpora mecanismos de transparência e produção de evidências compatíveis com uma abordagem preventiva e baseada em risco, em linha com experiências recentes como o ECA Digital e o Digital Services Act (DSA). À semelhança do modelo adotado no último pleito, a previsão de versões públicas das avaliações e dos relatórios de impacto em formato compatível com a proteção de dados pessoais e segredos comerciais permite uma melhor análise sobre a tolerabilidade dos riscos e a efetividade das medidas de mitigação, complementando os deveres técnicos impostos aos provedores. Essa diretriz articula-se com a proposta, no art. 9-C, de credenciamento, pela Justiça Eleitoral, de pesquisadores e universidades para acesso supervisionado a dados, convergindo com o regime de vetted researchers do DSA e fortalecendo a accountability regulatória diante de riscos sistêmicos associados à circulação de conteúdos sintéticos no processo eleitoral.

—
—

Por fim, nota-se que a previsão viabiliza, quando necessário e proporcional, acesso a dados e informações estritamente indispensáveis ao desempenho dessas atividades. Ao exigir transparência e publicidade dos critérios de credenciamento, do escopo do acesso e de mecanismos adequados de acompanhamento e controle, a medida busca compatibilizar celeridade e integridade eleitoral com proteção de dados pessoais, segurança da informação e preservação de segredos comerciais e industriais.

4 Ver European Commission, 'Commission adopts delegated act on data access under the Digital Services Act', Julho de 2025: <https://digital-strategy.ec.europa.eu/en/news/commission-adopts-delegated-act-data-access-under-digital-services-act>

Proposta minuta	Sugestão da Data Privacy Brasil
<p>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 nº 23.732/2024)</p>	<p>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 nº 23.732/2024)</p>
<p>I - a elaboração e a aplicação de termos de uso e de políticas de conteúdo compatíveis com esse objetivo; (Incluído pela Resolução nº 23.732/2024)</p>	<p>I - a elaboração e a aplicação de termos de uso e de políticas de conteúdo compatíveis com esse objetivo; (Incluído pela Resolução nº 23.732/2024)</p>
<p>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 nº 23.732/2024)</p>	<p>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;</p>
<p>III - o planejamento e a execução de ações corretivas e preventivas, incluindo o aprimoramento de seus sistemas de recomendação de conteúdo; (Incluído pela Resolução nº 23.732/2024)</p>	<p>III - o planejamento e a execução de ações corretivas e preventivas, incluindo o aprimoramento de seus sistemas de recomendação de conteúdo; (Incluído pela Resolução nº 23.732/2024)</p>
<p>IV - a transparência dos resultados alcançados pelas ações mencionadas no inciso III do caput deste artigo; (Incluído pela Resolução nº 23.732/2024)</p>	<p>IV - a transparência dos resultados alcançados pelas ações mencionadas no inciso III do caput deste artigo; (Incluído pela Resolução nº 23.732/2024)</p>
<p>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. (Incluído pela Resolução nº 23.732/2024)</p>	<p>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; (Incluído pela Resolução nº 23.732/2024)</p>

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. (Incluído pela Resolução nº 23.732/2024)

§ 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. (Incluído pela Resolução nº 23.732/2024)

§ 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. (Incluído pela Resolução nº 23.732/2024)

§ 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. (Incluído pela Resolução nº 23.732/2024)

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, mediante a apresentação de relatórios públicos sobre a eficácia de seus sistemas de recomendação na avaliação e mitigação de impactos à integridade do processo eleitoral.. (Incluído pela Resolução nº 23.732/2024)

VII – Exigir que os provedores de aplicação apresentem versão pública dos relatórios, mencionados no inciso VI, sobre a eficácia de seus sistemas de recomendação na mitigação de processos que atinjam a integridade do processo eleitoral.

§ 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. (Incluído pela Resolução nº 23.732/2024)

§ 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. (Incluído pela Resolução nº 23.732/2024)

<p>§ 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. (Incluído pela Resolução nº 23.732/2024)</p> <p>§ 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 nº 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. (Incluído pela Resolução nº 23.732/2024)</p>	<p>§ 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. (Incluído pela Resolução nº 23.732/2024)</p> <p>§ 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. (Incluído pela Resolução nº 23.732/2024)</p> <p>§ 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 nº 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. (Incluído pela Resolução nº 23.732/2024).</p>
--	---

Justificativa

Casos recentes, como do Grok — objetivo de manifestações técnicas conjuntas da Agência Nacional de Proteção de Dados (ANPD) da Secretaria Nacional do Consumidor (Senacon) e do Ministério Público Federal (MPF) — revelam a necessidade de que sistemas de IAs e algoritmos sejam concebidos e operados através da segurança por design. Ainda que o comando normativo busque tal objetivo, sua linguagem normativa pode ser mais forte e sintonizada com ferramentas de governança e processos representativas do estado da arte, notadamente como proposto “mecanismos de bloqueio ou redução de funcionalidade em cenários de abuso, medidas de identificação e rastreabilidade do conteúdo gerado e canal efetivo de reporte e correção”, bem como a adoção de avaliações independentes, como auditorias técnicas e exercícios de red-teaming, voltados à aferição de desempenho e à identificação de vulnerabilidades sistêmicas.

Ainda, a literatura nacional (Bioni, 2022) e estrangeira (Black e Murray, 2019) destaca que instrumentos de gestão de riscos, como as avaliações de impacto previstas na própria resolução, devem ser submetidos a algum grau de escrutínio público, como condição para uma governança em rede que ultrapasse modelos restritos de diálogo regulatório entre agentes econômicos e reguladores. Nesse sentido, a documentação de accountability relacionada à identificação, avaliação e mitigação de riscos deve contar com mecanismos mínimos de publicidade, de modo a torná-la cognoscível por um conjunto mais amplo de atores. Essa abertura permite o engajamento de partidos políticos, sociedade civil e demais interessados em processos de deliberação pública sobre quais riscos são toleráveis e quais demandam mitigação reforçada, à semelhança do que ocorre na seara ambiental.

Em matéria eleitoral, esses riscos são agravados pela velocidade de circulação da informação, pela elevada sensibilidade institucional do processo e pela potencial irreversibilidade dos danos à integridade democrática. É neste contexto que a gestão de riscos deve ser orientada pelo princípio da precaução, compreendido não apenas como a adoção de medidas preventivas, mas como a promoção de debate público qualificado sobre a cognição, a avaliação e a mitigação dos riscos associados ao uso de sistemas automatizados (Bioni & Luciano, 2020), o que reforça a necessidade de salvaguardas técnicas e organizacionais incorporadas desde a fase de desenvolvimento dos sistemas, capazes de prevenir usos abusivos, permitir rastreabilidade, viabilizar correções rápidas e reduzir danos antes que se tornem irreversíveis.

Proposta minuta	Sugestão da Data Privacy Brasil
<p>“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.</p> <p>§ 9º Não correspondente</p>	<p>Art. 9º G (...) § 9º O repositório de decisões será estruturado de forma interoperável com os sistemas dos provedores de aplicação, de forma que a ordem de remoção ou indisponibilidade de conteúdo inclua automaticamente peças substancialmente idênticas à removida, mesmo quando editados ou alteradas para contornar mecanismos de detecção.</p>

Justificativa

A inserção do § 9º ao art. 9º-G, determinando que o repositório de decisões seja estruturado de forma interoperável com os sistemas dos provedores de aplicação, de modo que ordens de remoção incluam automaticamente peças substancialmente idênticas, mesmo quando editadas para contornar mecanismos de detecção, é medida essencial para aumentar a efetividade das decisões do TSE. Evita que conteúdos sabidamente falsos ou gravemente descontextualizados se proliferem por meio de pequenas variações após a remoção, garantindo maior controle sobre a circulação de informações que possam comprometer o processo eleitoral.

A exigência de inclusão automática de conteúdos substancialmente idênticos encontra respaldo na prática do TSE, que já estendeu ordens de remoção para materiais replicados em múltiplos canais e formatos, prevenindo a disseminação contínua de conteúdos enganosos e protegendo a formação da opinião do eleitorado. Além de reforçar o próprio art. 9º-G, sem esse dispositivo as medidas de remoção perdem eficácia diante de edições simples de texto ou mídia, criando lacunas exploráveis por agentes enganosos e dificultando o cumprimento das ordens judiciais.

Proposta minuta	Sugestão da Data Privacy Brasil
<p>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: (Incluído pela Resolução nº 23.732/2024)</p> <p>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; (Incluído pela Resolução nº 23.732/2024)</p> <p>II - disponibilizar ferramenta de consulta, acessível e de fácil manejo, que permita realizar busca avançada nos dados do repositório que contenha, no mínimo: (Incluído pela Resolução nº 23.732/2024)</p> <p>a) buscas de anúncios a partir de palavras-chave, termos de interesse e nomes de anunciantes; (Incluído pela Resolução nº 23.732/2024)</p> <p>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; (Incluído pela Resolução nº 23.732/2024)</p> <p>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. (Incluído pela Resolução nº 23.732/2024)</p>	<p>Art. 27-A. (...)</p> <p>c) coletas sistemáticas, por meio de interface dedicada (application programming interface – API), de dados de anúncios, incluindo seu conteúdo, gasto, alcance, público atingido, identificação do anunciante e responsáveis pelo pagamento. (Incluído pela Resolução nº 23.732/2024)</p> <p>§ 1º Para os fins desse artigo, caracteriza conteúdo político-eleitoral, independente da classificação feita pela plataforma, aquele que versar sobre eleições, partidos políticos, federações e coligações, cargos eletivos, pessoas detentoras de cargos eletivos, pessoas candidatas, propostas de governo, projetos de lei, exercício do direito ao voto e de outros direitos políticos ou matérias relacionadas ao processo eleitoral. (Incluído pela Resolução nº 23.732/2024)</p> <p>§ 4º Os provedores de aplicações que realizem impulsionamento ou direcionamento de publicidade com base no tratamento de dados pessoais por meio de perfilamento ou microdirecionamento deverão elaborar relatório de impacto à proteção de dados, o qual deverá ser encaminhado ao Tribunal Superior Eleitoral (TSE) e à Agência Nacional de Proteção de Dados (ANPD), bem como disponibilizado em versão pública em repositório acessível.</p>

§ 1º Para os fins desse artigo, caracteriza conteúdo político-eleitoral, independente da classificação feita pela plataforma, aquele que versar sobre eleições, partidos políticos, federações e coligações, cargos eletivos, pessoas detentoras de cargos eletivos, pessoas candidatas, propostas de governo, projetos de lei, exercício do direito ao voto e de outros direitos políticos ou matérias relacionadas ao processo eleitoral. (Incluído pela Resolução nº 23.732/2024)

§ 2º As medidas previstas nos incisos do caput deste artigo deverão ser implementadas: (Incluído pela Resolução nº 23.732/2024)

I - em até 60 (sessenta) dias, a contar da entrada em vigor desta norma, no caso de provedor de aplicação que já ofereça serviço de impulsionamento no Brasil; (Incluído pela Resolução nº 23.732/2024)

II – a partir do início da prestação do serviço de impulsionamento no Brasil, no caso de provedor de aplicação que passe a oferecê-lo após a entrada em vigor desta norma. (Incluído pela Resolução nº 23.732/2024)

§ 3º As medidas previstas no caput deste artigo são de cumprimento permanente, inclusive em anos não eleitorais e períodos pré e pós-eleições. (Incluído pela Resolução nº 23.732/2024)

§ 4º O cumprimento do disposto neste artigo é requisito para o credenciamento, na Justiça Eleitoral, do provedor de aplicação que pretenda, nos termos dos §§ 3º e 9º do art. 29 desta Resolução, prestar serviço de impulsionamento de propaganda eleitoral. (Incluído pela Resolução nº 23.732/2024)

§ 4º Não correspondente

Justificativa

A manutenção do art. 27-A, inciso c, bem como de seu § 1º, na Resolução mostra-se necessária, adequada e proporcional para assegurar a transparência, a fiscalização e a integridade do processo eleitoral, especialmente no contexto da crescente utilização de plataformas digitais para a veiculação de propaganda político-eleitoral. A previsão de coletas sistemáticas de dados de anúncios por meio de interfaces dedicadas (APIs) viabiliza o monitoramento contínuo, padronizado e verificável, permitindo o efetivo controle sobre o conteúdo veiculado, os valores despendidos, o alcance, o público atingido, a identificação do anunciante e os responsáveis pelo pagamento, reduzindo, assim, as assimetrias informacionais entre plataformas, autoridades eleitorais, pesquisadores e sociedade civil.

O art. 27-A, inciso c, fortalece a coerência sistêmica da regulação eleitoral e a aplicação do conceito de tratamento de dados pessoais, nos termos do art. 5º, inciso X, da LGPD, ao disciplinar o acesso e a coleta de informações de interesse público no contexto da propaganda político-eleitoral digital. Além disso, o § 1º do art. 27-A cumpre papel essencial ao uniformizar o conceito de conteúdo político-eleitoral, afastando a possibilidade de enquadramentos restritivos ou discricionários realizados unilateralmente pelas plataformas digitais. Ao estabelecer que a caracterização independe da classificação atribuída pela própria plataforma, o dispositivo reforça a autoridade normativa da Justiça Eleitoral, evita lacunas regulatórias e dificulta práticas de ocultação ou subnotificação de anúncios relevantes para o processo democrático.

Nesse sentido, o acréscimo do § 4º revela-se medida complementar e necessária para o adequado enfrentamento dos riscos associados ao impulsionamento e ao direcionamento de publicidade eleitoral baseados em perfis comportamentais ou em técnicas de microdirecionamento. Ao exigir dos provedores de aplicações a elaboração de relatório de impacto à proteção de dados pessoais, com encaminhamento ao Tribunal Superior Eleitoral (TSE) e à Agência Nacional de Proteção de Dados (ANPD), além de versão pública em repositório acessível, o dispositivo reforça a transparência, a responsabilização e o controle institucional sobre práticas que envolvem tratamento intensivo de dados pessoais. A medida também viabiliza atuação coordenada e cooperativa com a ANPD, no âmbito de suas competências legais, para avaliação de riscos, harmonização interpretativa e adoção de medidas corretivas ou orientativas, especialmente diante de tratamentos capazes de afetar simultaneamente direitos fundamentais e a integridade do processo eleitoral.

Essa caracterização do impulsionamento e do microdirecionamento de propaganda político-eleitoral como tratamento de alto risco pode ser analisada a partir do que a própria ANPD entende como tal. No [guia orientativo de tratamento de dados pessoais de alto risco](#), a Autoridade indica que o tratamento que possa afetar significativamente interesses e direitos dos titulares, inclusive quando envolve tecnologias emergentes ou inovadoras, pode ser considerado de alto risco. A ANPD também reforça que essa caracterização depende de fatores contextuais e deve ser avaliada à luz das circunstâncias concretas de cada operação de tratamento.

Nessa mesma linha, Kloza et al. (2019) explicam que alguns gatilhos típicos de alto risco podem ser observados a partir da combinação entre perfilização sistemática, definição automatizada

de perfis e a produção de efeitos relevantes sobre indivíduos ou grupos sociais, inclusive para além da esfera estritamente individual. Conforme os autores, a avaliação de risco em DPIAs deve considerar não apenas danos individualizáveis, mas impactos sociais e sistêmicos, avaliados à luz da natureza, do contexto, da finalidade e do alcance do tratamento. No caso em tela, impõe-se considerar que essas práticas podem influenciar processos decisórios coletivos e direitos fundamentais como a liberdade de pensamento, a liberdade de expressão e a própria participação democrática.

Por fim, a articulação entre a coleta sistemática via API com maior granularidade e rastreabilidade, incluindo identificação do anunciante e dos responsáveis pelo pagamento, à definição normativa de conteúdo político-eleitoral que independe da classificação unilateral das plataformas e a exigência de relatório de impacto à proteção de dados em hipóteses de perfilamento e microdirecionamento consolida um núcleo coerente de transparência e responsabilização aplicável ao impulsionamento político-eleitoral. Esse conjunto reduz assimetrias informacionais, viabiliza fiscalização contínua e verificável e fortalece a atuação coordenada entre TSE e ANPD para antecipar e mitigar riscos típicos de tratamentos intensivos e potencialmente discriminatórios, preservando direitos fundamentais e a integridade do processo eleitoral por meio de medidas proporcionais, publicizáveis e orientadas a evidências.

Proposta minuta	Sugestão da Data Privacy Brasil
Não correspondente.	Art. 33-E. Para os fins previstos nesta Resolução, os partidos políticos, as federações, as coligações, as candidatas e os candidatos devem formular regras de boas práticas e de governança, previsto no art. 50 da Lei nº 13.709/2018, em especial ações educativas, bem como mecanismos, técnico, administrativos e internos de supervisão e de mitigação de riscos e outros aspectos relacionados desde a concepção do tratamento de dados pessoais.

Justificativa

A inclusão do art. 33-E busca consolidar e aprofundar os avanços introduzidos pela Justiça Eleitoral nas eleições de 2024 em matéria de proteção de dados pessoais, reconhecendo a centralidade da governança como eixo estruturante da integridade informacional do processo eleitoral. As alterações recentes da Resolução nº 23.610/2019 já incorporaram instrumentos relevantes de accountability, como o registro das operações de tratamento, a previsão de encarregados e a possibilidade de elaboração de relatórios de impacto à proteção de dados, especialmente em cenários de alto risco. Esses mecanismos, contudo, não se esgotam em si mesmos e pressupõem a existência de um programa de governança mais amplo, nos termos do art. 50 da Lei nº 13.709/2018, que funcione como instância integradora e orientadora dessas medidas.

Nesse sentido, a proposta visa suprir lacuna normativa ainda existente, ao explicitar o dever de partidos políticos, federações, coligações, candidatas e candidatos de formular regras de boas práticas e de governança em proteção de dados, compreendidas como o conjunto articulado de ações educativas, mecanismos técnicos, administrativos e internos de supervisão e mitigação de riscos. Trata-se de alinhar a regulação eleitoral à lógica já consagrada na LGPD, segundo a qual instrumentos como registros, relatórios de impacto e designação de responsáveis integram um programa de governança contínuo, e não medidas isoladas ou meramente formais.

A ênfase conferida à adoção de medidas desde a concepção do tratamento de dados (“privacy by design”) mostra-se particularmente relevante no contexto eleitoral, no qual incidentes de segurança, usos indevidos de dados ou falhas sistêmicas tendem a produzir danos de difícil ou impossível reversão, com impactos diretos sobre a igualdade de chances entre candidaturas, a liberdade de escolha do eleitorado e a confiança no processo democrático. A lógica preventiva, portanto, deve prevalecer sobre abordagens meramente corretivas, reforçando a necessidade de planejamento, avaliação e mitigação de riscos desde as etapas iniciais das estratégias de comunicação e campanha.

Além disso, a previsão expressa de ações educativas e treinamentos contínuos responde a evidências empíricas amplamente documentadas na literatura especializada, que identificam o fator organizacional e cultural como um dos principais gargalos para a efetividade da proteção de dados e da governança informacional. Programas de governança que não incorporam capacitação permanente tendem a falhar na internalização de boas práticas, mesmo quando dispõem de instrumentos formais adequados. Ao explicitar esse dever, a norma contribui para a construção de uma cultura de proteção de dados no âmbito eleitoral, compatível com a complexidade tecnológica e informacional das campanhas contemporâneas.

Com isso, o art. 33-E fortalece a coerência sistêmica da regulação eleitoral, densifica a aplicação do art. 50 da LGPD no contexto das eleições e contribui para uma abordagem mais preventiva, estruturada e sustentável da proteção de dados pessoais, em benefício da integridade do processo eleitoral e da tutela dos direitos fundamentais.

Proposta minuta	Sugestão da Data Privacy Brasil
Art. 33-D. Nas eleições para os cargos de Presidente da República, Governador, Senador e Prefeito das capitais dos Estados, a Justiça Eleitoral poderá determinar a elaboração de relatório de impacto à proteção de dados nos casos em que o tratamento representa alto risco. (Incluído pela Resolução nº 23.732/2024).	Art. 33-D. Nas eleições para os cargos de Presidente da República, Governador, Senador e Prefeito das capitais dos Estados, a Justiça Eleitoral poderá determinar a elaboração de relatório de impacto à proteção de dados nos casos em que o tratamento representa alto risco. (Incluído pela Resolução nº 23.732/2024).
§ 1º Considera-se de alto risco o tratamento de dados pessoais que, cumulativamente: (Incluído pela Resolução nº 23.732/2024)	§ 1º Considera-se de alto risco o tratamento de dados pessoais que, cumulativamente: (Incluído pela Resolução nº 23.732/2024)

I - seja realizado em larga escala, assim caracterizado quando abranger número de titulares equivalente a, no mínimo, 10% (dez por cento) do eleitorado apto da circunscrição; (Incluído pela Resolução nº 23.732/2024).

II - envolva o uso de dados pessoais sensíveis ou de tecnologias inovadoras ou emergentes para perfilamento de eleitoras e eleitores com vistas ao microdirecionamento da propaganda eleitoral e da comunicação da campanha. (Incluído pela Resolução nº 23.732/2024).

§ 2º A autoridade eleitoral que concluir necessários os relatórios de impacto na circunscrição expedirá, até o dia 16 de agosto do ano das eleições, ofício dirigido a todos os partidos políticos, federações e coligações que registrarem candidaturas para os cargos mencionados no caput deste artigo, informando o prazo em que deverá ser atendida a requisição. (Incluído pela Resolução nº 23.732/2024).

§ 3º Nas eleições gerais, a análise de necessidade do relatório de impacto e a expedição de ofício caberá à(ao) presidente do Tribunal da circunscrição. (Incluído pela Resolução nº 23.732/2024).

§ 4º O relatório de impacto será elaborado sob responsabilidade conjunta da candidata ou do candidato e do partido político, da federação ou da coligação pela qual concorre, devendo conter, no mínimo: (Incluído pela Resolução nº 23.732/2024).

I - a descrição dos tipos de dados pessoais coletados e tratados; (Incluído pela Resolução nº 23.732/2024).

II - os riscos identificados; (Incluído pela Resolução nº 23.732/2024).

III - a metodologia usada para o tratamento e para a garantia de segurança das informações; (Incluído pela Resolução nº 23.732/2024).

I - seja realizado em larga escala, assim caracterizado quando abranger número de titulares equivalente a, no mínimo, 10% (dez por cento) do eleitorado apto da circunscrição; (Incluído pela Resolução nº 23.732/2024).

II - envolva o uso de dados pessoais sensíveis ou de tecnologias inovadoras ou emergentes para perfilamento de eleitoras e eleitores com vistas ao microdirecionamento da propaganda eleitoral e da comunicação da campanha. (Incluído pela Resolução nº 23.732/2024).

§ 2º Caberá aos partidos políticos, federações, coligações e candidatos justificarem, até o dia 06 de agosto, a (des)necessidade de elaboração de relatório de impacto à proteção de dados pessoais junto ao presidente do Tribunal da circunscrição que poderá consultar a Autoridade Nacional de Proteção de Dados;

§ 3º A autoridade eleitoral e/ou a ANPD que concluir necessários os relatórios de impacto na circunscrição expedirá, até o dia 16 de agosto do ano das eleições, ofício dirigido a todos os partidos políticos, federações e coligações que registrarem candidaturas para os cargos mencionados no caput deste artigo, informando o prazo em que deverá ser atendida a requisição. (Incluído pela Resolução nº 23.732/2024).

§ 4º O relatório de impacto será elaborado sob responsabilidade conjunta da candidata ou do candidato e do partido político, da federação ou da coligação pela qual concorre, devendo conter, no mínimo: (Incluído pela Resolução nº 23.732/2024).

I - a descrição dos tipos de dados pessoais coletados e tratados; (Incluído pela Resolução nº 23.732/2024).

II - os riscos identificados; (Incluído pela Resolução nº 23.732/2024).

III - a metodologia usada para o tratamento e para a garantia de segurança das informações; (Incluído pela Resolução nº 23.732/2024).

<p>IV - as medidas, salvaguardas e instrumentos adotados para mitigação de riscos. (Incluído pela Resolução nº 23.732/2024).</p> <p>§ 5º As campanhas que não realizarem tratamento de alto risco deverão informar, no prazo de resposta ao ofício, o(s) requisito(s) do § 1º deste artigo que não preenchem. (Incluído pela Resolução nº 23.732/2024).</p> <p>§ 6º Os relatórios recebidos e as informações prestadas nos termos do § 5º deste artigo serão disponibilizados no site da Justiça Eleitoral para consulta pública. (Incluído pela Resolução nº 23.732/2024).</p> <p>§ 7º O disposto neste artigo não exclui o exercício simultâneo da competência da Autoridade Nacional de Proteção de Dados prevista no art. 38 da Lei nº 13.709/2018. (Incluído pela Resolução nº 23.732/2024)</p>	<p>IV - as medidas, salvaguardas e instrumentos adotados para mitigação de riscos. (Incluído pela Resolução nº 23.732/2024).</p> <p>§ 5º As campanhas que realizarem relatórios de impacto à proteção de dados pessoais, deverão apresentar sumário público das medidas de cognição, avaliação e mitigação do alto risco das suas atividades de tratamento de dados.</p> <p>§ 6º O disposto neste artigo não exclui o exercício simultâneo da competência da Autoridade Nacional de Proteção de Dados prevista no art. 38 da Lei nº 13.709/2018. (Incluído pela Resolução nº 23.732/2024)</p>
--	--

Justificativa

A disciplina do relatório de impacto à proteção de dados no âmbito eleitoral deve ser compreendida à luz da lógica mais ampla das avaliações de impacto, tal como consolidada no direito ambiental, na proteção de dados pessoais e, mais recentemente, na governança de sistemas de inteligência artificial. Em todas essas esferas, a função primordial do instrumento não é substituir a atuação do regulador, mas induzir à reflexão estruturada, ex ante, por parte do agente regulado sobre riscos, finalidades, proporcionalidade e medidas de mitigação associadas às suas próprias práticas.

Essa racionalidade parte do reconhecimento de que quem detém conhecimento efetivo sobre fluxos informacionais, bases de dados, finalidades de tratamento, arranjos contratuais e o ciclo de vida da informação é o próprio controlador. No contexto eleitoral, são os partidos políticos, federações, coligações, candidatas e candidatos que concentram essa visão sistêmica, estando, portanto, em melhor posição institucional para avaliar, de forma inicial, a desnecessidade de elaboração de relatório de impacto à proteção de dados, bem como para identificar riscos concretos associados a práticas de perfilamento, microdirecionamento e uso de tecnologias emergentes.

Sob essa perspectiva, a dinâmica regulatória associada ao relatório de impacto à proteção de dados deve ser concebida como um processo essencialmente procedimental e conversacional, que se inicia com uma manifestação técnica e fundamentada dos próprios controladores acerca da existência ou não de tratamento de dados de alto risco. Tal abordagem alinha-se à literatura especializada sobre data protection impact assessments, que compreende o RIPD não como um

□ mecanismo meramente reativo ou acionado de forma episódica pela autoridade pública, mas como um instrumento estruturante da gestão de riscos e da governança de dados. Nesse sentido, Gomes (2022, p. 3) sustenta que o relatório de impacto constitui o resultado de um processo contínuo de avaliação, devendo ser entendido não apenas como um documento produzido ao final de um exercício formal de conformidade, mas como ferramenta de suporte às atividades de tratamento, capaz de orientar decisões organizacionais, qualificar práticas de governança e viabilizar a demonstração de conformidade com as obrigações legais aplicáveis.

Isso não implica, contudo, colocar a Justiça Eleitoral ou a Autoridade Nacional de Proteção de Dados em uma posição de mera expectadora. Ao contrário, a institucionalização de um fluxo procedimental claro de colheita, organização e publicização de informações sobre a desnecessidade de RIPD contribui diretamente para a redução de assimetrias informacionais, qualificando a atuação fiscalizatória e decisória da Justiça Eleitoral e viabilizando uma atuação mais informada, dialética e proporcional, inclusive em articulação com a ANPD, nos termos do art. 38 da LGPD.

Nesse sentido, o cruzamento entre o calendário eleitoral e as etapas de avaliação e eventual requisição de relatórios de impacto revela-se especialmente relevante. A definição de marcos temporais claros permite alinhar o dever de reflexão e justificativa dos controladores com momentos em que as estratégias de comunicação e tratamento de dados tendem a ser estruturadas e intensificadas. Tal desenho favorece a atuação preventiva, em consonância com os princípios do privacy by design e da precaução, especialmente em um contexto no qual danos à integridade eleitoral e à autodeterminação informacional tendem a ser irreversíveis ou de difícil reparação. □

Ao deslocar o eixo inicial da avaliação para os próprios agentes que realizam o tratamento, sem abdicar do controle institucional e da possibilidade de requisição fundamentada de RIPD pela Justiça Eleitoral, o modelo proposto fortalece a accountability, promove maior aderência às práticas de governança previstas no art. 50 da LGPD e contribui para uma regulação eleitoral mais consistente, transparente e orientada à gestão efetiva de riscos.

Visando operacionalizar a compreensão do RIPD, propomos um fluxograma estruturado em fases, iniciando-se com as convenções partidárias para que partidos, federações, coligações e candidaturas avaliem, de forma fundamentada, a existência ou não de tratamento de dados de alto risco. Em seguida, busca-se estabelecer um diálogo regulatório no qual a Justiça Eleitoral exerce função de validação, orientação e eventual requisição motivada de RIPD antes do início oficial da campanha, preservando a efetividade do controle sem comprometer a previsibilidade, a segurança jurídica e a integridade do calendário eleitoral. Por fim, o estágio de monitoramento contínuo permite acomodar ajustes, impugnações e revisões ao longo da campanha, reconhecendo o caráter dinâmico das práticas de tratamento de dados e reforçando uma abordagem de fiscalização orientada à prevenção de danos, à accountability e à gestão contínua de riscos: —

<p>Fase 01: Preparação ex ante 20/07 a 05/08 - Convenções partidárias (escolha oficial dos candidatos)</p>
<p>Fase 02: Envio de informações e início dos diálogos regulatórios Até dia 10/08 (5 dia úteis após o final das convenções partidárias) para envio de informações sobre o tratamento de dados pessoais ou de justificativa da desnecessidade de RIPD (se for o caso)</p>
<p>Fase 03: Análise institucional e devolutiva ao TSE e ANPD Entre 10/08 - 15/08 - Aqui o TSE pode: (i) confirmar a inexistência de tratamento de alto risco ou (ii) entender pela requisição fundamentada de elaboração de RIPD (§§ 2º e 3º do art. 33-D)</p>
<p>Fase 04: Início da campanha, monitoramento e acompanhamento Momento em que pode haver resposta a eventos supervenientes, impugnações impugnações (5 dias após publicização, então até o dia 20/08) e eventual requisição superveniente de RIPD, mediante motivação.</p>

Proposta minuta	Sugestão da Data Privacy Brasil
<p>Art. 33-C. Para os fins previstos nesta Resolução, os partidos políticos, as federações, as coligações, as candidatas e os candidatos devem manter o registro das operações de tratamento de dados pessoais, nele contendo, ao menos: (Incluído pela Resolução nº 23.732/2024)</p> <p>I - o tipo do dado e a sua origem; (Incluído pela Resolução nº 23.732/2024)</p> <p>II - as categorias de titulares; (Incluído pela Resolução nº 23.732/2024)</p> <p>III - a descrição do processo e da finalidade; (Incluído pela Resolução nº 23.732/2024)</p> <p>IV - o fundamento legal; (Incluído pela Resolução nº 23.732/2024)</p> <p>V - a duração prevista para o tratamento, nos termos da Lei nº 13.709/2018; (Incluído pela Resolução nº 23.732/2024)</p> <p>VI - o período de armazenamento dos dados pessoais; (Incluído pela Resolução nº 23.732/2024)</p>	<p>Art. 33 - C. (...)</p> <p>§ 1º Para os fins do inciso VIII, o registro das operações de tratamento deverá abranger todas as pessoas naturais ou jurídicas contratadas por partidos políticos, federações, coligações, candidatas ou candidatos que participem, direta ou indiretamente, do tratamento de dados pessoais para fins de propaganda eleitoral, com a indicação de seus respectivos papéis como controladores, controladores conjuntos ou operadores.</p> <p>§ 2º A Justiça Eleitoral disponibilizará modelo para o registro de operações simplificado de que trata o caput deste artigo. (Incluído pela Resolução nº 23.732/2024)</p> <p>§ 3º O registro de operações deverá ser conservado pelas pessoas mencionadas no caput deste artigo durante o período eleitoral, permanecendo a obrigação em caso de</p>

<p>VII - a descrição do fluxo de compartilhamento de dados pessoais, se couber; (Incluído pela Resolução nº 23.732/2024)</p> <p>VIII - os instrumentos contratuais que especifiquem o papel e as responsabilidades de controladores e operadores; (Incluído pela Resolução nº 23.732/2024).</p> <p>§ 1º A Justiça Eleitoral disponibilizará modelo para o registro de operações simplificado de que trata o caput deste artigo. (Incluído pela Resolução nº 23.732/2024)</p> <p>§ 2º O registro de operações deverá ser conservado pelas pessoas mencionadas no caput deste artigo durante o período eleitoral, permanecendo a obrigação em caso de ajuizamento de ação na qual se apure irregularidade ou ilicitude no tratamento de dados pelas campanhas. (Incluído pela Resolução nº 23.732/2024)</p> <p>§ 3º Nas ações mencionadas no § 2º deste artigo, a autoridade eleitoral poderá determinar a exibição do registro de operações e de documentos que o corroborem. (Incluído pela Resolução nº 23.732/2024)</p>	<p>ajuizamento de ação na qual se apure irregularidade ou ilicitude no tratamento de dados pelas campanhas. (Incluído pela Resolução nº 23.732/2024)</p> <p>§ 4º Nas ações mencionadas no § 2º deste artigo, a autoridade eleitoral poderá determinar a exibição do registro de operações e de documentos que o corroborem. (Incluído pela Resolução nº 23.732/2024)</p>
---	--

Justificativa

A alteração proposta pelo art. 33-C busca conferir maior efetividade ao dever de registro de operações de tratamento de dados pessoais, esclarecendo o alcance do inciso VIII. Na prática, campanhas e partidos frequentemente contratam múltiplos fornecedores e consultorias que participam direta ou indiretamente do tratamento de dados para fins de propaganda eleitoral. Sem a explicitação de que essas pessoas naturais e jurídicas devem constar do registro, com a indicação de seus papéis como controladores, controladores conjuntos ou operadores, cria-se uma lacuna que dificulta a rastreabilidade das operações, a verificação de responsabilidades e a instrução de eventuais ações eleitorais sobre irregularidades ou ilicitudes.

A previsão proposta também melhora a padronização e a fiscalização do cumprimento da norma, pois permite que a Justiça Eleitoral identifique, de forma organizada, a cadeia de tratamento e os instrumentos contratuais correspondentes, reduzindo assimetrias informacionais e fortalecendo a transparência e a prestação de contas no uso de dados pessoais em campanhas, em consonância com as obrigações da Lei nº 13.709/2018.

Proposta minuta	Sugestão da Data Privacy Brasil
Art. 37. Para o fim desta Resolução, considere-se: (...)	(...) XXXVI - marca d'água: ato de incorporar informações, que normalmente são difíceis de remover, em resultados criados artificialmente por tecnologias digitais, como pela IA, inclusive em resultados como fotos, vídeos, áudio ou texto - para fins de verificação da autenticidade do resultado ou da identidade ou características de sua proveniência, modificação ou transporte.

Justificativa

A incorporação do inciso XXXVI no art. 37 confere clareza e segurança jurídica ao definir, de forma funcional, o que se entende por “marca d'água” no contexto de conteúdos gerados ou manipulados por tecnologias digitais, inclusive por sistemas de IA. Sem esse conceito mínimo, há risco de interpretações divergentes sobre o que constitui marcação, por exemplo, marca visível, marca invisível/robusta, metadados de proveniência, o que dificulta a fiscalização, a padronização de procedimentos e o cumprimento consistente de obrigações de transparência e mitigação.

Um dos resultados do [relatório sobre as eleições municipais de 2024](#), elaborado pelo Observatório IA nas Eleições, reforça a necessidade de positivação desse conceito. A análise dos casos mapeados evidencia que a prática decisória dos magistrados tem variado conforme o grau de sofisticação da manipulação do conteúdo, o que, na ausência de parâmetros técnicos minimamente definidos, tende a produzir respostas desiguais diante de situações funcionalmente semelhantes.

Além disso, marcas d'água, especialmente quando combinadas com mecanismos de registro de proveniência, são instrumento técnico relevante para verificação de autenticidade, identificação de alterações e rastreabilidade de conteúdo sintético, contribuindo para reduzir danos associados a manipulações como deepfakes em ambiente eleitoral. A definição proposta evita engessar soluções específicas, mantendo abertura para evolução conforme o estado da arte, e favorece a interoperabilidade entre plataformas, auditorias e autoridades, com observância da proteção de dados pessoais e da proporcionalidade.

Referências

AGÊNCIA BRASIL. Caso Banco Master. Disponível em: <https://agenciabrasil.ebc.com.br/politica/noticia/2026-02/senado-instala-comissao-para-apurar-fraudes-do-banco-master>. Acesso em: 5 fev. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Coordenação-Geral de Fiscalização; Coordenação de Fiscalização. Nota Técnica nº 1/2026/FIS/CGF/ANPD: sistema de inteligência artificial Grok. Possíveis violações à Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD). Brasília: ANPD, 2026. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnica-no-1-2026-fis-cgf-anpd.pdf>. Acesso em: 4 fev. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Coordenação-Geral de Fiscalização; Coordenação de Fiscalização. Objeto da Nota Técnica nº 1/2026/FIS/CGF/ANPD, no Processo SEI nº 00261.000178/2026-27 (Representação nº 01-2026, envolvendo X Corp. e X Brasil Internet Ltda., com petição complementar apresentada pela Deputada Federal Erika Hilton). Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnica-no-1-2026-fis-cgf-anpd.pdf>. Acesso em: 5 fev. 2026.

BIONI, Bruno Ricardo. Regulação e Proteção de Dados Pessoais: o princípio da accountability. Rio de Janeiro: Forense, 2022.

BIONI, B.; LUCIANO, M. O princípio da precaução na regulação de Inteligência Artificial: seriam as leis de proteção de dados o seu portal de entrada? In: FRAZÃO, A.; MULHOLLAND, C. (coords.). Inteligência artificial e direito: ética, regulação e responsabilidade. [livro eletrônico]. 2. ed. rev. São Paulo: Thomson Reuters Brasil, 2020.

BLACK, Julia; MURRAY, Andrew Douglas. Regulating AI and Machine Learning: setting the regulatory agenda. European Journal of Law and Technology, [s. l.], v. 10, n. 3, 30 dez. 2019. Disponível em: <https://www.ejlt.org/index.php/ejlt/article/view/722>. Acesso em: 25 nov. 2021.

BRASIL. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia orientativo sobre tratamento de dados pessoais de alto risco. Brasília: ANPD, 2024. Disponível em: <https://share.google/GRtKD4quMjkjzdgk>. Acesso em 06. Fev. 2026.

BRASIL. Lei nº 9.504, de 30 de setembro de 1997. Estabelece normas para as eleições. Diário Oficial da União: Brasília, 30 set. 1997. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/1997/lei-9504-30-setembro-1997-365408-norma-pl.html>. Acesso em: 22 jan. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: Poder Executivo, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 5 fev. 2026.

DATA PRIVACY BRASIL; ALÁFIA LAB. OBSERVATÓRIO IA NAS ELEIÇÕES. Relatório: balanço do Observatório IA nas Eleições. [S. l.], 2025. Disponível em: <https://observatorioianaseleicoes.com.br/wp-content/uploads/2025/08/RELATORIO-Balanco-OBservatorio-IA-nas-Eleicoes.pdf>. Acesso em: 22 jan. 2026.

DIAS, Jefferson Aparecido; DOCA, Heloisa Helou; SILVA, Fabiano Fernando da. Bots, fake news, fake faces and deepfakes: automation, under the bias of dromology, as a sophisticated form of biopower to influence the democratic election process. *Pensar – Revista de Ciências Jurídicas*, Fortaleza, v. 26, n. 3, p. 1-14, jul./set. 2021. DOI: 10.5020/2317-2150.2021.11840. Disponível em: <https://doi.org/10.5020/2317-2150.2021.11840>. Acesso em: 22 jan. 2026.

ESTADÃO CONTEÚDO. Eleições: Gilmar sugere força-tarefa sobre conteúdo sintético e acordo com empresas de IA. UOL Notícias, Brasília, 3 fev. 2026. Disponível em: <https://noticias.uol.com.br/ultimas-noticias/agencia-estado/2026/02/03/eleicoes-gilmar-sugere-forca-tarefa-sobre-conteudo-sintetico-e-acordo-com-empresas-de-ia.htm>. Acesso em: 4 fev. 2026.

EUROPEAN COMMISSION. Commission adopts delegated act on data access under the Digital Services Act. Julho 2025. Disponível em: <https://digital-strategy.ec.europa.eu/en/news/commission-adopts-delegated-act-data-access-under-digital-services-act>. Acesso em: 5 fev. 2026.

GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados. *Revista do Advogado*, São Paulo, 2022. Disponível em: https://mariaceciliagomes.com.br/wp-content/uploads/2022/01/Relatorio_de_Impacto_a_Protecao_de_Dados.pdf. Acesso em: 3 fev. 2026.

INTERNATIONAL INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE (International IDEA); FORUM ON INFORMATION & DEMOCRACY; DEMOCRACY REPORTING INTERNATIONAL. Protecting democratic elections through safeguarding information integrity: top 10 recommendations for platforms and states. Stockholm: International IDEA, 2024. 6 p. DOI: 10.31752/idea.2024.1. Disponível em: <https://www.idea.int/sites/default/files/2024-01/protecting-democratic-elections-through-safeguarding-information-integrity.pdf>. Acesso em: 22 jan. 2026.

KIRA, Beatriz et al. Current challenges in digital elections: lessons from electoral regulation and digital campaigning in Brazil. Berlin: Weizenbaum-Institut e.V., nov. 2025. (Weizenbaum Discussion Paper, n. 52). DOI: 10.34669/WI.DP/52. Disponível em: https://www.weizenbaum-institut.de/media/Publikationen/Weizenbaum_Discussion_Paper/Weizenbaum_Discussion_Paper_52.pdf. Acesso em: 22 jan. 2026.

Kloza, Dariusz. et al. (TRANS.). Em direção a um método para avaliações de impacto sobre a proteção de dados: entendendo as exigências do RGPD. d.pia.lab Policy Brief, 1/2019, 1-12, 2020. Disponível em: https://cris.vub.be/ws/portalfiles/portal/51221989/dpialab_pb2019_1_final_PT.pdf. Acesso em 04. fev. 2026.

LEMOS, André. Erros, falhas e perturbações digitais em alucinações das IA generativas: tipologia, premissas e epistemologia da comunicação. *Revista MATRIZES – USP*, 2024.

MANSELL, Robin et al. Information ecosystems and troubled democracy: a global synthesis of the state of knowledge on news media, AI and data governance. Paris: International Observa-

tory on Information and Democracy, jan. 2025. Disponível em: https://observatory.information-democracy.org/wp-content/uploads/2025/06/rapport_forum_information_democracy_2025-1.pdf. Acesso em: 21 jan. 2026.

D

SANTOS, João Guilherme Bastos dos et al. Das milícias digitais ao comportamento coordenado: métodos interdisciplinares de análise e identificação de bots nas eleições brasileiras. In: BRAZILIAN WORKSHOP ON SOCIAL NETWORK ANALYSIS AND MINING (BRASNAM), 10., 2021, evento online. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2021. p. 187-192. ISSN 2595-6094. DOI: 10.5753/brasnam.2021.16138. Acesso em: 22 jan. 2026.

SILBERSCHNEIDER, Cora. Caracterização e análise de propagandas políticas microdirecionadas no Brasil: um estudo de caso do Facebook e Instagram. Dissertação (mestrado) — Universidade Federal de Minas Gerais (UFMG), Ciência da Computação, 2023.

SULLIVAN, Arthur. Chatbots de IA confundem fatos com opinião, revela estudo. Deutsche Welle (DW), 22 out. 2025. Disponível em: <https://www.dw.com/pt-br/chatbots-de-ia-confundem-fatos-com-opini%C3%A3o-revela-estudo/a-74455677>. Acesso em: 5 fev. 2026.

SZPORER, Maurício et al. Democracia digital e fiscalização no âmbito das redes sociais: o PL 2330/20 e a (im)possibilidade de responsabilização dos provedores de conteúdo sobre o teor das informações compartilhadas. Revista Direito Unifacs, n. 285, p. 8-16, 2024.

D

TRIBUNAL REGIONAL ELEITORAL DE SÃO PAULO. Marçal é condenado a multa de R\$ 15 mil por vídeo contra Nunes na campanha eleitoral. Comunicação TRE-SP, 14 mar. 2025. Disponível em: <https://www.tre-sp.jus.br/comunicacao/noticias/2025/Marco/marcal-e-condenado-a-multa-de-r-15-mil-por-video-contr-nunes>. Acesso em: 5 fev. 2026.

—
—

Anexo I – Audiência Pública [Síntese das contribuições]

Bom dia,

Cumprimento Senhor Ministro Vice-Presidente Nunes Marques, na pessoa de quem cumprimento todas as autoridades presentes.

As contribuições da Associação Data Privacy Brasil, organização suprapartidária cuja missão é promover direitos fundamentais diante de tecnologias contemporâneas, estão todas centradas na **premissa** de que provedores de aplicações e de sistemas de IA, partidos, confederações e demais atores de um **ecossistema informacional** cada vez mais complexo, e estruturado por algoritmos de recomendação, modelos de monetização por engajamento e técnicas avançadas de segmentação de direcionamento da propaganda política, **devem ter obrigações e deveres mais bem delimitados e reforçados para a construção de uma ordem informacional democrática**. Em especial, sob uma vertente **precaucionária - e não apenas preventiva - de cognição, avaliação e gerenciamento multidimensional dos riscos e danos** de natureza irreversível, típicos do processo eleitoral.

Para tanto, dentre outras sugestões, propomos que:

- a. primeiro: adição de parágrafos no art. 9-C para melhor articulação do que se chama deveres de **“segurança by design”** por parte de fornecedores de IA. Além de serem obrigatórias as avaliações de impacto, sugerimos que, a exemplo do que foi determinado recentemente no caso Grok, haja **relatórios com periodicidade semanal** sobre o volume de **suspensão de contas e as soluções adotadas de bloqueio ou redução de funcionalidades para contenção de conteúdos com potencial impacto à integridade do processo eleitoral e outros ilícitos**;
- b. segundo: o pleito de que **haja versões públicas dessas avaliações e dos relatórios de impacto**, para que a sociedade possa se engajar sob o quão **toleráveis são esses riscos e quão eficientes são suas respectivas medidas de mitigação**. Essa medida, **conjugada com outro parágrafo que propomos no mesmo art. 9-C**, acerca da necessidade de a **justiça eleitoral credenciar pesquisadores e universidades para acesso a dados** para fins de realização de pesquisas sobre os impactos de produtos e serviços no processo eleitoral. Assim, a exemplo do que fez o ECA digital, **forja-se uma rede de governança pública e mais democrática**.
- c. terceiro: propomos, ainda, que provedores de aplicações que direcionam propaganda política valendo-se de técnicas de perfilhamento ou micro direcionamento devam, obrigatoriamente, elaborar relatórios de impacto à proteção de dados e fornecê-los ao TSE e ANPD (artigo 27-A);
- d. quarto: que, no **artigo 33-D**, seja alterada a lógica para que, ao invés de partidos políticos e demais atores sejam notificados acerca da necessidade de elaboração de relatórios de

impacto por parte da jurisdição eleitoral, **estes sejam proativos**, uma vez que são os controladores dos bancos de dados. Estes é que devem, **proativamente, notificar a jurisdição eleitoral e a ANPD acerca do alto risco das suas atividades de tratamento de dados** e, a seu turno, tais reguladores se manifestem. Essa nova **dinâmica-procedimentalização** gera, ao menos, mais coleta de dados e evidências, sobretudo para uma atuação ainda mais efetiva, sobretudo no período crítico eleitoral;

- e. quinto, por fim, propomos um novo dispositivo para que, **a exemplo do artigo 50 da LGPD**, a resolução obrigue que haja **programas de governança de privacidade com ênfase em treinamentos e medidas educativas, para que haja uma cultura de integridade nas estruturas partidárias**. Os recursos vultosos do fundo partidário devem ser canalizados para tanto. Um dos principais gargalos não é apenas o tecnológico, de capacidade forense ou normativo, mas também, e principalmente, cultural e humano dessas estruturas.

