

A relação entre a integridade do processo eleitoral e a privacidade

A proteção da integridade do processo eleitoral diante do uso da internet e das redes sociais representa um desafio que muitos formuladores de políticas estão abordando ou estão dispostos a abordar. Na internet, conteúdos que podem afetar a integridade do processo eleitoral são cada vez mais personalizados. Este fenômeno é tão preocupante [que foi identificado como um dos principais riscos globais de curto e médio prazo](#).

Em tempos de IA generativa, em que o custo econômico e a dificuldade técnica para a produção e disseminação de conteúdo falso ou sintético para enganar, manipular ou simular autenticidade foram consideravelmente reduzidos, a preocupação com a integridade do processo eleitoral se intensifica. Enquanto isso, a privacidade online e a proteção de dados pessoais são uma agenda inacabada na América Latina.

Existe uma conexão intrínseca entre a capacidade de coletar e processar grandes quantidades de dados pessoais e a forma como conteúdos falsos ou manipulativos são criados e divulgados em redes sociais e aplicativos de mensagens em particular, e na internet em geral. Por essa razão, a aplicação de leis e políticas rigorosas em matéria de proteção de dados pessoais e privacidade permite reduzir o impacto que o conteúdo falso ou manipulativo tem. Isso é especialmente importante em contextos eleitorais, em que estes conteúdos impactam e empobrecem o debate público, afetando diretamente os direitos políticos e eleitorais e a integridade do processo eleitoral.

[Este fenômeno é anterior ao surgimento da internet](#). No entanto, é graças ao surgimento das novas tecnologias que se ampliam a geração e propagação de conteúdos falsos e manipulativos. Isso é apoiado pelo próprio modelo econômico que sustenta as plataformas, ampliando sua eficácia e alcance. Por um lado, as redes sociais possuem algoritmos de recomendação de conteúdo que utilizam dados pessoais para gerar perfis aos quais podem depois apresentar conteúdos publicitários segmentados, incluindo propaganda explicitamente política. Esta técnica é conhecida como “microtargeting” ou “microdirecionamento”.

O [microtargeting político busca impactar direta ou indiretamente na democracia](#). É utilizado para convencer eleitores, incentivar ou desincentivar a participação nas urnas ou para arrecadar fundos com informações deliberadamente tiradas de contexto, imprecisas ou errôneas.

O controle exercido por essas empresas levanta sérias preocupações sobre os direitos das pessoas. Ao terem acesso a quantidades massivas de informações pessoais, essas empresas têm a capacidade de moldar o conteúdo que os usuários veem e com o qual interagem. Através da construção de perfis que podem revelar hábitos, relações sociais, preferências políticas e opiniões, para mencionar alguns exemplos. Os dados pessoais são o combustível

que potencializa riscos à integridade do processo eleitoral, seja tendo sido fornecidos pelo próprio usuário ou gerados pelas plataformas a partir de suas interações na internet.

Para os atores da desinformação, o acesso a ferramentas sofisticadas, como as utilizadas para criar “deepfakes” por meio de IA generativa ou “bots” programados para disseminar conteúdo e buscar manipular a opinião pública, [potencializa a efetividade](#) quanto à qualidade e escalabilidade deste microtargeting, dificultando sua detecção como conteúdo falso ou manipulativo. [Avatares gerados por IA e personagens sintéticos que simulam eleitores](#), influenciadores, apresentadores, comentaristas ou lideranças populares podem produzir aparência de espontaneidade, fabricar vozes de atores políticos artificiais e dificultar a identificação, pelos usuários, de que determinada manifestação pública foi criada ou mediada por tecnologia.

Neste contexto, impulsionamento com nanosegmentação [busca atingir](#) perfis cada vez mais específicos com conteúdos customizados e ferramentas baseadas em IA são usadas para avaliar e mapear seu impacto nas redes. A partir de dados pessoais de grupos de eleitores, perfis de “eleitores sintéticos” são criados para testar mensagens ou estratégias visando a maneira mais eficiente de influenciar eleitores reais.

Esta rápida expansão das IAs e a hiper-personalização com dados pode levar a um problema de “erosão epistêmica” para sociedades democráticas, como apontado pelo Painel Científico Independente de Governança de IA da ONU em 2026.

Desde a Access Now, Data Privacy Brasil e Electronic Frontier Foundation apontamos a aplicação de leis de proteção de dados pessoais e políticas públicas de privacidade como um mecanismo eficiente para melhorar a qualidade de nossas democracias e reduzir a manipulação do discurso público em ambientes digitais e seu impacto em contextos eleitorais. Medidas de ampliação do acesso à informação para a tomada de decisões eleitorais e de transparência do uso, pelas campanhas e partidos políticos, de tecnologias digitais assentadas no tratamento massivo de dados pessoais também cumprem papel relevante na garantia da integridade do processo eleitoral.

Recomendações para garantia da integridade dos processos eleitorais no Brasil diante das novas tecnologias

A preocupação com os efeitos da disseminação de conteúdos falsos, manipulativos ou deliberadamente descontextualizados se acentua particularmente em contextos eleitorais. Da Argentina ao México, passando pelo Brasil, muitos países da América Latina estão tendo ou terão processos eleitorais relevantes no próximo período.

Fornecer à cidadania informações de qualidade e de diferentes fontes é um elemento essencial para o exercício dos direitos políticos. Para fins de resguardar o processo eleitoral, esses

países devem fazer valer suas leis de privacidade e de proteção de dados pessoais através de suas autoridades competentes, em sintonia com seus poderes judiciários e tribunais eleitorais.

A Access Now, Data Privacy Brasil e Electronic Frontier Foundation propõem as seguintes recomendações para proteger a integridade do processo eleitoral a partir da garantia da privacidade e da proteção de dados durante os contextos eleitorais:

1. Potencializar as garantias e políticas de proteção de dados pessoais como elemento chave para a integridade do processo eleitoral, em particular os princípios da necessidade, finalidade e proporcionalidade:
 - a. Proibir o tratamento de dados pessoais sensíveis (como crenças filosóficas e rotulagem de orientações ideológicas), incluindo os inferidos, que revelem ou possam revelar a preferência política das pessoas para fins de segmentação de conteúdo político. Em contextos eleitorais, o tratamento de dados pessoais sensíveis só é legítimo quando a pessoa tenha dado seu consentimento de forma prévia, explícita e com propósitos de uso e transferências estritamente limitados e claramente informados.
 - b. O tratamento deve ser realizado somente sobre dados pessoais estritamente necessários para a finalidade que se persegue.
 - c. Proibir adicionar usuários a grupos de mensagens instantâneas com fins de divulgação política, salvo em casos excepcionais em listas de membros de partidos políticos ou tendo consentimento prévio e informado por parte do titular.
 - d. O consentimento livre, específico e informado implica que a pessoa seja capaz de fazer uma escolha real, destacada das demais e não correr nenhum risco de engano, intimidação, coação, negação de acesso a produtos ou serviços ou outras consequências negativas significativas caso não dê o seu consentimento.
2. Os partidos políticos, federações e coligações devem aprimorar a disponibilização de informação ao público em geral sobre suas atividades de tratamento de dados pessoais em contexto eleitoral, incluindo:
 - a. Política de tratamento de dados pessoais adotada, em observância à legislação de proteção de dados e à legislação eleitoral, incluindo as medidas adotadas para prevenir o descumprimento dos princípios gerais de proteção, para registrar as operações de tratamento de dados pessoais, para obter o consentimento de forma adequada e para garantir a segurança técnica e administrativa no tratamento de dados;
 - b. Canais de comunicação em que o titular de dados possa obter informações sobre o tratamento de seus dados pessoais, exercer os direitos previstos em lei e requerer o descadastramento no recebimento de mensagens eletrônicas e instantâneas;
 - c. Informações sobre perfilamento que realizam para fins eleitorais e sobre a contratação e utilização de tecnologias digitais baseadas em dados neste contexto, incluindo para fins de impulsionamento, microtargeting, análise de redes e predição de reação ou comportamento de eleitores.

3. Fortalecer mecanismos de cooperação entre a Agência Nacional de Proteção de Dados (ANPD) e o Tribunal Superior Eleitoral para:
 - a. Aprimorar canais de comunicação e robustecer iniciativas conjuntas para a supervisão do cumprimento de garantias associadas à proteção de dados no contexto eleitoral com a publicação de relatórios periódicos de fiscalização.
 - b. Identificar e desarticular estratégias coordenadas que comprometem a integridade do processo eleitoral e realizam atividades online que simulam ser “orgânicas” de base cidadã quando na realidade estão financiadas ou coordenadas por um partido, governo ou empresa, como as fazendas de bots, contas pessoais falsas gerenciadas por uma entidade, avatares de IA e personagens sintéticos que simulam eleitores reais para fins de manipulação da opinião pública, entre outras.
 - c. No âmbito de suas competências, determinar a elaboração e divulgação de relatório de impacto à proteção de dados nos casos de uso de dados pessoais sensíveis ou de tecnologias emergentes para perfilamento de eleitoras e eleitores.
4. As autoridades, partidos políticos, comunicadores e plataformas de redes sociais deverão garantir, na medida do possível, que a população tenha acesso a informações adequadas e relevantes para a tomada de decisões eleitorais.
 - a. Os partidos políticos, autoridades eleitorais e autoridades de proteção de dados deverão destinar uma porcentagem de seu orçamento em comunicação para alertar sobre as consequências do microtargeting em contextos eleitorais e sobre o uso de avatares de IA ou eleitores sintéticos para simular apoio, rejeição, indignação ou mobilização política espontânea.
 - b. Reforçar alianças com os verificadores de fatos e outros comunicadores relevantes, como organizações da sociedade civil, influenciadores e outros, para identificar campanhas que comprometam a integridade do processo eleitoral e comunicar à população sobre tais alianças por diferentes canais, incluindo canais oficiais do poder público.
 - c. Sistematizar as propostas eleitorais desenvolvidas pelos candidatos e suas plataformas eleitorais segundo eixos temáticos para facilitar a comparação entre partidos políticos.
 - d. Acordar estratégias entre autoridades e empresas de plataformas online, incluídas redes sociais e chatbots, no início dos períodos eleitorais, para que seja dada prioridade ao conteúdo desenvolvido pelas autoridades eleitorais.
 - e. Toda instância, protocolo ou política criada que envolva autoridades ou entes públicos deve ser comunicada seguindo os padrões da transparência ativa.
5. As plataformas deverão desabilitar ferramentas de microtargeting para conteúdo político eleitoral durante períodos previamente estabelecidos.
6. As autoridades, atores técnicos, acadêmicos, sociedade civil e/ou plataformas de redes sociais deverão colaborar na criação de um laboratório de análise de impacto algorítmico que permita supervisionar o cumprimento destas recomendações.

- a. Elaborar relatórios sobre os resultados alcançados, em especial aqueles que deem conta da existência de microtargeting, da utilização de dados pessoais para segmentação, e a exposição a conteúdo variado em contextos eleitorais.
 - b. Estabelecer protocolos estritos de cibersegurança para que os laboratórios impeçam o acesso à informação privada das pessoas usuárias reais.
7. As autoridades responsáveis por supervisionar a proteção de dados pessoais e em matéria eleitoral devem contar com autonomia e independência funcional, econômica e técnica suficientes para garantir o adequado exercício de suas competências.