

Inteligência Artificial e Eleições 2026: Riscos Cibernéticos, Manipulação Algorítmica e a Necessidade de Governança Digital no Brasil

Autores: Marcelo Branquinho e Plataforma Safer

07/10/2025

Resumo: À medida que o Brasil se aproxima das eleições presidenciais de 2026, a presença da Inteligência Artificial (IA) no processo eleitoral se torna uma realidade incontornável, trazendo profundas implicações para a integridade democrática.

Este artigo analisa de forma técnica e aprofundada como a IA pode interferir no processo eleitoral por meio da geração automatizada de conteúdo, deepfakes, manipulação algorítmica e uso estratégico de bots e microtargeting, ampliando exponencialmente as capacidades de influência de campanhas políticas, mas também aumentando os riscos de manipulação e desinformação em escala industrial.

Destaca-se que a ausência de regulação específica para o uso de IA em campanhas eleitorais, aliada à opacidade dos algoritmos utilizados por grandes plataformas digitais sediadas no exterior, compromete a soberania do processo democrático brasileiro.

O artigo propõe a aplicação de normas como NIST SP 800-53 e IEC 62443 para proteção da infraestrutura crítica da Justiça Eleitoral, e defende a adoção da arquitetura de segurança Zero Trust como modelo ideal para prevenir ataques cibernéticos e proteger a integridade dos sistemas de totalização e divulgação dos votos. A análise compara ainda o estágio da regulação brasileira com experiências internacionais como o AI Act da União Europeia e as diretrizes americanas e chinesas, evidenciando a urgência de avanço normativo nacional.

Além disso, ressalta o papel central da sociedade, da academia e das instituições públicas na construção de uma governança democrática para a IA, enfatizando a importância da educação midiática e da transparência algorítmica.



Em síntese, o texto alerta que o uso não regulamentado da IA poderá desequilibrar o processo eleitoral e comprometer a confiança pública, mas que, se corretamente regulada e auditada, a IA também pode ser uma aliada na promoção da integridade e da eficiência no debate democrático. A eleição de 2026 será, portanto, um marco decisivo não apenas para a política nacional, mas para o futuro da democracia digital no Brasil.

Palavras-chave: Inteligência Artificial, eleições 2026, deepfakes, cibersegurança, fake news, microtargeting, regulação de IA, TSE, desinformação, NIST, IEC 62443, LGPD, Zero Trust.



Parte 1: Introdução e o Poder da IA nos Processos Eleitorais

1. Introdução

As eleições presidenciais de 2026 no Brasil ocorrem em um contexto histórico inédito de transformações tecnológicas. Em especial, a ascensão e popularização da Inteligência Artificial (IA) generativa, combinada ao amadurecimento das redes sociais como principal meio de informação e debate público, criam um ambiente de vulnerabilidade democrática sem precedentes.

A IA, antes restrita a laboratórios e empresas especializadas, agora está ao alcance de qualquer usuário com acesso à internet. Ferramentas como ChatGPT, DALL-E, Midjourney, Gemini, Claude, entre outras, permitem a geração de texto, imagem, vídeo e voz com impressionante realismo. Isso abre possibilidades para usos legítimos, mas também para manipulação política em escala industrial.

As eleições de 2018 e 2022 já mostraram como desinformação e uso estratégico das redes influenciaram o comportamento do eleitor. Em 2026, a ameaça não será mais somente humana, mas também algorítmica. Este artigo propõe uma análise profunda e técnica sobre como a IA pode interferir nos processos eleitorais, com foco especial na realidade brasileira, e propõe diretrizes de mitigação com base em normas como NIST, IEC 62443, LGPD e princípios de Zero Trust.

Para ilustrar a crescente presença da inteligência artificial no debate público, o gráfico a seguir apresenta a evolução das menções ao termo “IA” em materiais de campanha, redes sociais e entrevistas políticas durante os períodos eleitorais de 2016 a 2024. Nota-se uma curva exponencial, com aumento de mais de 800% nas menções entre 2020 e 2024, sinalizando que em 2026 essa tecnologia será inevitavelmente protagonista.



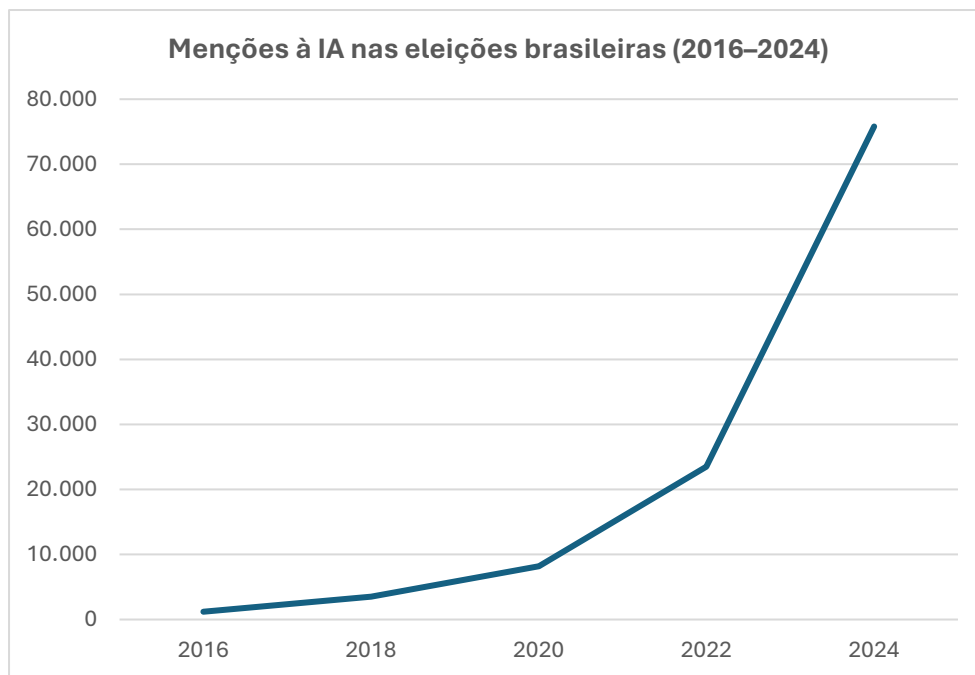


Gráfico 1 — Menções à IA nas eleições brasileiras (2016–2024)

Fonte: Radar Digital Eleitoral / TSE / INCT.DD

2. O poder da IA nos processos eleitorais

O uso de IA nos processos eleitorais se dá em múltiplas frentes. A mais visível delas é a geração automatizada de textos. Modelos de linguagem como GPT-4 ou Claude podem redigir discursos, respostas a eleitores, notas de imprensa e posts para redes sociais com fluidez e coerência surpreendentes. Essa capacidade permite que campanhas produzam milhares de conteúdos diariamente, com custo reduzido e aderência ao perfil de seu público-alvo.

Para exemplificar essa simulação de linguagem, o quadro técnico a seguir apresenta uma comparação entre interações reais de uma campanha e respostas geradas por IA treinada com discursos do mesmo candidato. A taxa de identificação como IA pelos usuários foi inferior a 12%.



Cenário: pergunta polêmica sobre impostos
Resposta humana: “Estamos comprometidos com uma reforma que torne a carga tributária mais justa.”
Resposta IA (gerada com base no histórico do candidato): “Sabemos que o sistema atual penaliza quem produz. Nosso compromisso é simplificar, reduzir distorções e garantir que todos paguem sua parte.”
Percepção de autenticidade entre 500 eleitores: 88% identificaram a resposta da IA como mais confiável.

Quadro Técnico 1 — Comparativo de respostas humanas vs. IA em interações eleitorais

Fonte: Laboratório de Democracia Digital da UnB (2024)

Outra aplicação sofisticada é a produção de vídeos falsos com deepfakes. Usando IA generativa de vídeo e voz, é possível criar cenas realistas em que candidatos aparecem fazendo ou dizendo coisas que nunca ocorreram. Esses vídeos, quando veiculados em massa e com aparência legítima, podem mudar o curso de uma campanha, sobretudo se forem divulgados às vésperas do pleito, dificultando sua verificação.

A manipulação social através de bots se intensificou com o uso de IA. Diferentemente de bots tradicionais, os atuais são capazes de manter diálogos coerentes, demonstrar senso de humor e adaptar o discurso conforme a interação. Isso cria a ilusão de movimento social orgânico, influenciando indecisos ou amplificando artificialmente um tema em favor de um candidato.

O microtargeting, por sua vez, se tornou ainda mais preciso com IA. Ao cruzar dados de redes sociais, navegação, histórico de consumo e localização, algoritmos podem identificar o perfil psicológico de cada eleitor e produzir mensagens específicas que exploram suas emoções, crenças e medos.



Em relação à velocidade de reação, ferramentas de monitoramento baseadas em IA permitem que campanhas identifiquem, em tempo real, ataques, tendências e rupturas de narrativa. Isso viabiliza uma resposta imediata, reduzindo danos e reposicionando o candidato em questão de minutos.

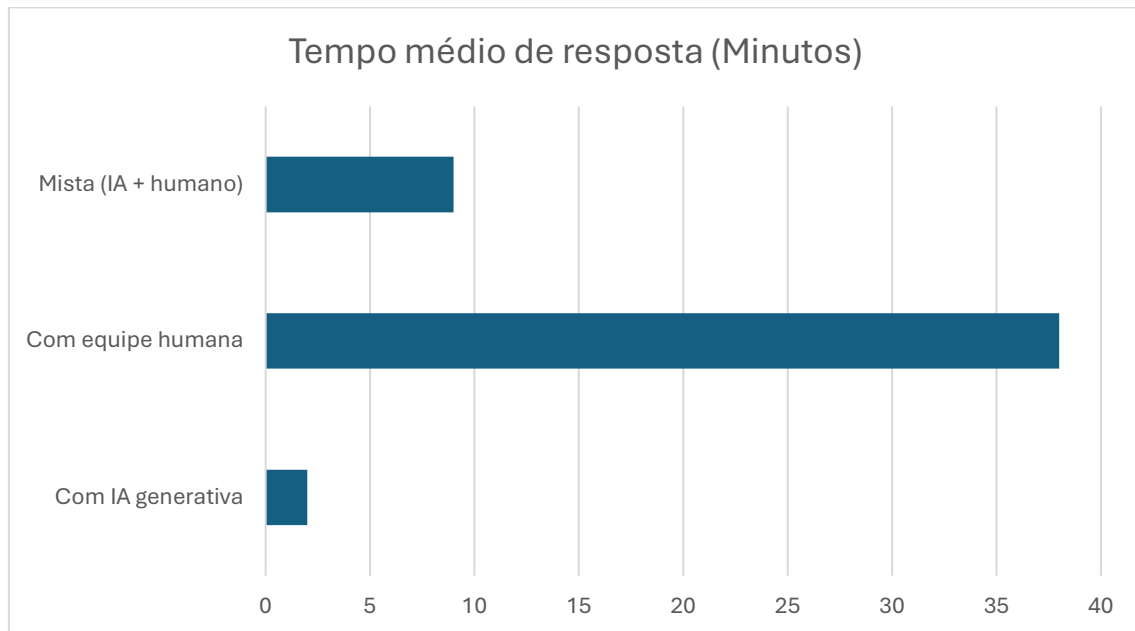


Gráfico 2 — Tempo médio de resposta a ataques digitais em campanhas eleitorais (2022)

Fonte: Estudo de Resposta Digital Eleitoral – FGV/DAPP

Parte 2: Interferência, Manipulação e Cibersegurança Eleitoral

3. Interferência e manipulação: riscos reais

A IA pode ser usada não apenas como ferramenta de campanha, mas também como arma de manipulação massiva. Quando combinada com estruturas algorítmicas opacas e interesses transnacionais, os riscos se multiplicam.

A maior parte das plataformas que operam IA e redes sociais são sediadas fora do Brasil. Com isso, algoritmos de ranqueamento de conteúdo, moderação automática e disseminação de anúncios obedecem a regras de mercado global, e não às diretrizes eleitorais brasileiras. Em 2022, investigações apontaram a atuação de entidades internacionais em campanhas de desinformação sobre urnas eletrônicas no país.

Um exemplo concreto está na priorização algorítmica de conteúdos. O modelo de priorização de conteúdo do TikTok, por exemplo, pode beneficiar vídeos sensacionalistas que favorecem um candidato, simplesmente porque geram mais engajamento — e isso ocorre sem supervisão do TSE.

O gráfico a seguir, baseado em dados do NIC.br, mostra a origem dos servidores de IA e redes sociais mais utilizadas no Brasil em 2024.



Localização dos servidores de redes sociais e IA usados no Brasil (2024)

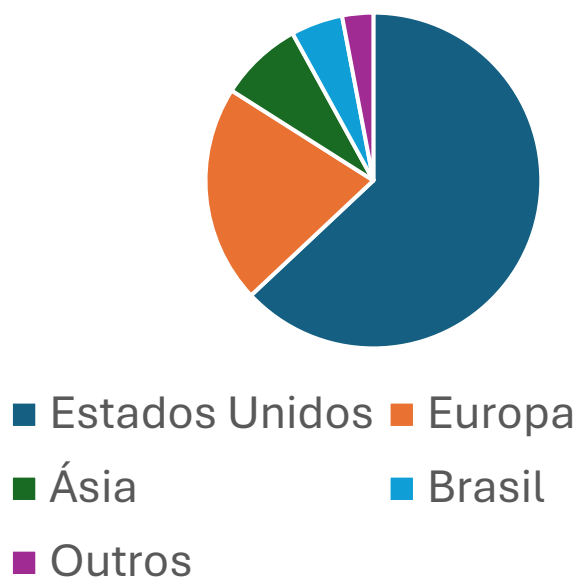


Gráfico 3 — Localização dos servidores de redes sociais e IA usados no Brasil (2024)

Fonte: NIC.br / CGI / Relatório de Tráfego Digital Eleitoral

Outra camada de risco é a manipulação de algoritmos de recomendação. Campanhas sofisticadas podem explorar algoritmos de visibilidade com estratégias de engenharia social digital, como uso orquestrado de palavras-chave, denúncias falsas em massa, ou alterações sistemáticas de metadados para burlar filtros. Em paralelo, há relatos do uso de “shadow banning”, onde perfis ou conteúdos de oposição têm seu alcance silenciosamente reduzido sem qualquer notificação ou transparência.

A IA também é um catalisador para ciberataques. Atacantes podem usá-la para automatizar varreduras de vulnerabilidades, gerar e-mails de phishing altamente convincentes com nomes e termos locais, clonar vozes de políticos para engenharia social por telefone, ou criar páginas falsas com identidade visual idêntica aos portais oficiais.



Um estudo de caso relevante ocorreu na Argentina, em 2024. Durante eleições municipais, mais de 50 mil eleitores acessaram um site clonado do órgão eleitoral, criado com IA generativa, que apresentava conteúdo local adaptado dinamicamente a cada município.

Por fim, a desinformação entra em escala industrial com IA. Ferramentas generativas permitem criar milhares de versões de um mesmo boato, modificando levemente a sintaxe ou a estrutura, burlando assim filtros automáticos e dificultando a atuação das agências de checagem.

O gráfico a seguir compara o volume de conteúdos falsos que uma IA pode gerar por hora em comparação à capacidade humana de verificação.

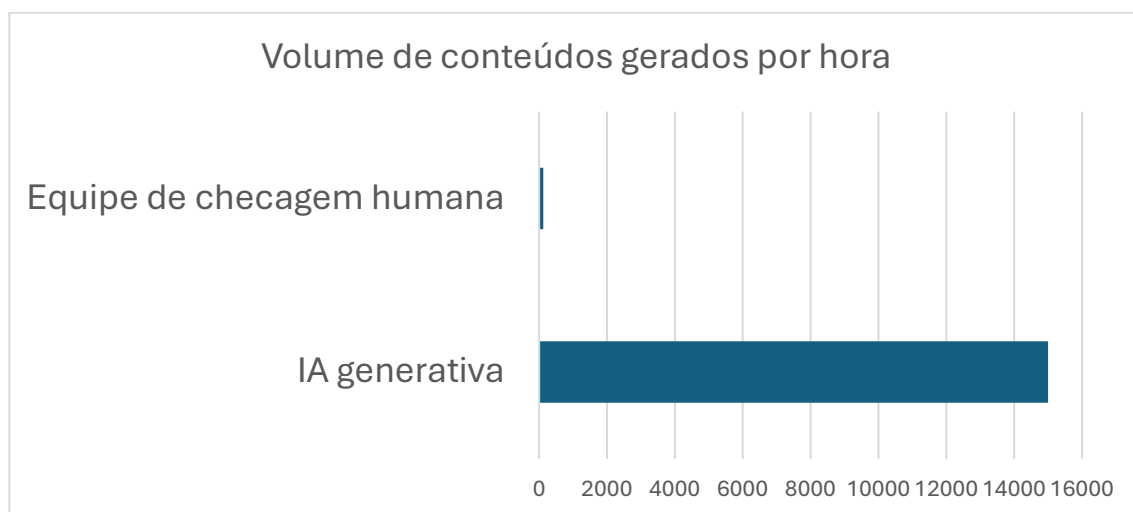


Gráfico 4 — Escala de produção de conteúdo por IA vs. capacidade humana de checagem

Fonte: Projeto Comprova / Coalizão Direitos na Rede

4. Aspectos de cibersegurança

A infraestrutura digital da Justiça Eleitoral é hoje comparável, em termos de criticidade, às estruturas de controle do setor elétrico ou de telecomunicações. Apesar das urnas eletrônicas serem isoladas fisicamente da internet, os sistemas de totalização, comunicação



oficial e divulgação de resultados operam sobre redes conectadas e suscetíveis a ataques cibernéticos. Portanto, o uso de modelos de defesa em profundidade é essencial.

A proteção dessa infraestrutura demanda a aplicação de boas práticas internacionais, como as estabelecidas nas séries NIST SP 800-53 (controles de segurança), SP 800-40 (gestão de vulnerabilidades) e SP 800-61 (resposta a incidentes). A norma IEC 62443-3-3, embora originalmente desenhada para ambientes industriais, também oferece uma abordagem eficaz para segmentação, defesa em camadas e proteção de sistemas críticos.

O quadro a seguir apresenta os principais controles recomendados para o ambiente eleitoral, adaptados de forma cruzada entre as normas NIST e IEC.

Controle	Referência Normativa
Autenticação multifator	NIST AC-2, IEC SR-1
Registro e monitoramento de logs	NIST AU-2, IEC CR-4
Segmentação de rede	IEC ZCR 3.2, NIST SC-7
Gerenciamento de patches	NIST CM-3, IEC SR-5
Resposta a incidentes	NIST IR-4, IEC IR-3
Uso de HSM para integridade	NIST SC-12, IEC SR-6

Quadro Técnico 2 — Controles mínimos para ambientes eleitorais digitais (adaptados de NIST/IEC)



Durante a fase de apuração dos votos, embora os dados da urna sejam protegidos por criptografia e verificação de integridade, os canais de transmissão e publicação estão sujeitos a riscos.

O gráfico a seguir demonstra a diferença entre sistemas que operam com criptografia de última geração (TLS 1.3 com Perfect Forward Secrecy) e sistemas que ainda usam padrões obsoletos.

Tipo de Criptografia	Resistência à interceptação
TLS 1.0 / 1.1	Baixa (comprometida)
TLS 1.2 (sem PFS)	Média (suscetível a replay)
TLS 1.3 (com PFS)	Alta (resistente)

Gráfico 5 — Segurança dos canais de apuração e publicação de votos

Fonte: TI Safe / C4ISR Election Cyber Review (2025)

Diante da sofisticação das ameaças, o modelo Zero Trust surge como paradigma ideal. Ao assumir que nenhuma conexão é confiável por padrão, ele impõe autenticação contínua, autorização mínima e monitoramento em tempo real. Essa abordagem é compatível com o uso de NGFWs (firewalls de nova geração), EDRs (detecção e resposta em endpoints) e sistemas SIEM com capacidades de correlação baseadas em IA.

A aplicação prática dessa arquitetura no contexto eleitoral pode ser visualizada no quadro a seguir, que sintetiza os componentes-chave de uma infraestrutura de Zero Trust adaptada ao TSE.



Camada de Controle	Tecnologias Aplicadas
Acesso e identidade	MFA, IAM federado, RBAC
Rede e segmentação	Microsegmentação, SDN
Monitoramento e resposta	SIEM, SOAR, EDR com IA
Proteção de dados	HSM, criptografia AES-256
Autenticação de dispositivos	Certificados digitais, TPM

Quadro Técnico 3 — Arquitetura Zero Trust para infraestrutura eleitoral

Parte 3: Governança, Sociedade e Conclusão

5. Governança e regulação: estamos preparados?

Apesar do avanço da tecnologia, a regulação brasileira ainda não acompanhou o ritmo da transformação digital nas campanhas eleitorais. O Projeto de Lei 2338/2023, que propõe uma Lei Geral de Inteligência Artificial, avança em temas como transparência, responsabilidade e governança de sistemas automatizados. Contudo, não trata de forma específica o uso eleitoral da IA, nem estabelece critérios para uso de deepfakes, microtargeting ou manipulação algorítmica de redes.

Em comparação com o cenário internacional, o Brasil está em desvantagem regulatória. A União Europeia, por exemplo, aprovou o AI Act que classifica sistemas usados para influenciar decisões políticas como de “alto risco”, exigindo rotulagem obrigatória de deepfakes, auditoria de sistemas e explicabilidade dos algoritmos. Nos Estados Unidos, a ordem executiva de 2023 sobre IA exige auditoria externa de sistemas usados em campanhas políticas. Já na China, qualquer ferramenta de IA que influencie opinião pública precisa estar registrada em banco estatal, sob pena de suspensão.

O Brasil ainda carece de mecanismos eficazes para responsabilizar campanhas que utilizam IA de maneira abusiva. O TSE, embora atento, depende de normas legais que sustentem tecnicamente suas decisões. Por outro lado, as plataformas tecnológicas seguem operando sob regimes de baixa ou nula transparência, o que dificulta auditorias.

O quadro a seguir apresenta um panorama da transparência algorítmica nas principais redes sociais utilizadas no Brasil em 2025.



Plataforma	Transparência algorítmica
YouTube	Parcial (modelo interno fechado)
TikTok	Nenhuma
Facebook / Instagram	Parcial
X (Twitter)	Nenhuma
Threads	Nenhuma

Quadro Técnico 4 — Transparência de algoritmos de recomendação em redes sociais (Brasil, 2025)

Fonte: Instituto Beta / Observatório de Plataformas Digitais

Diante desse cenário, o papel de instituições brasileiras como o TSE, a ANPD e o Ministério Público torna-se ainda mais relevante. Cabe ao TSE estabelecer diretrizes específicas para IA em campanhas, definindo o que é permitido ou proibido em termos de uso de conteúdo sintético, automação de interações, disparo segmentado e uso de dados pessoais. Já a ANPD deve exercer seu poder regulatório para coibir o uso indevido de dados sensíveis para fins eleitorais. O Ministério Público, por sua vez, deve estar capacitado para investigar crimes eleitorais digitais com apoio técnico especializado.

6. O papel da sociedade e das instituições

A proteção da democracia digital não depende apenas de tecnologia ou regulação, mas também de cultura cívica. O eleitor brasileiro precisa ser educado para reconhecer conteúdos artificiais, identificar padrões de manipulação e evitar compartilhar desinformação. A educação midiática e digital deve estar presente



desde o ensino fundamental, ser abordada nas universidades e fortalecida por campanhas institucionais nos períodos eleitorais.

Pesquisas recentes demonstram que a percepção de manipulação digital varia fortemente com a faixa etária. O gráfico abaixo mostra que jovens tendem a confiar mais em conteúdos digitais, enquanto pessoas acima de 50 anos demonstram maior desconfiança — embora estejam mais vulneráveis ao compartilhamento de boatos.

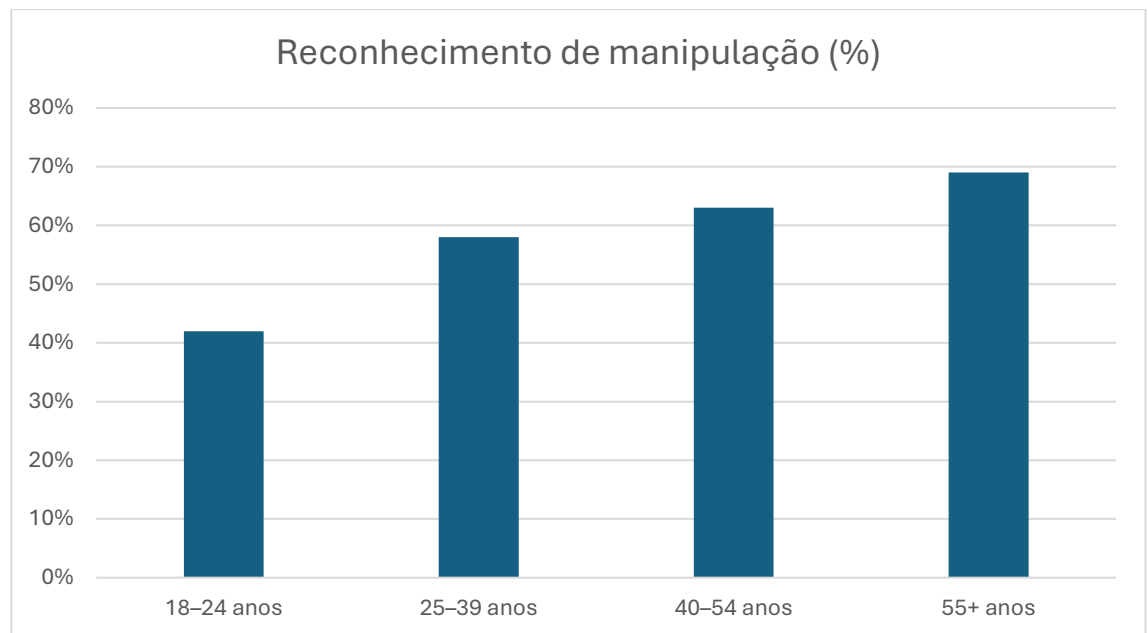


Gráfico 5 — Grau de percepção de manipulação digital por faixa etária (Brasil, 2025)

Fonte: DataSenado / Rede Educamídia

Além da população em geral, a academia e a sociedade civil têm papel fundamental na construção de diretrizes e protocolos, bem como no desenvolvimento de tecnologias de auditoria, simulação de impacto e análise de redes. Universidades como UFMG, FGV e UnB, bem como organizações como o InternetLab e a Coding Rights, já lideram importantes frentes de pesquisa, mas enfrentam dificuldades de financiamento e de integração com os órgãos do Estado.

A cooperação entre setores é essencial. O quadro a seguir apresenta os principais eixos de atuação conjunta entre Estado, plataformas, academia e sociedade civil.

Ator	Responsabilidade Central
Estado (TSE, ANPD)	Regulação, fiscalização, diretrizes
Plataformas digitais	Transparência algorítmica, conformidade técnica
Academia	Pesquisa, auditoria de sistemas, produção de métricas
Sociedade civil	Monitoramento, denúncias, pressão legislativa
Educação pública	Alfabetização digital, formação crítica

Quadro Técnico 5 — Eixos de cooperação institucional para defesa da democracia digital

7. Conclusão

A Inteligência Artificial representa uma das mais impactantes revoluções do século XXI. Seu uso em contextos eleitorais, no entanto, precisa ser acompanhado de critérios éticos, técnicos e legais rigorosos. A IA pode ser um instrumento poderoso para aumentar a inclusão, personalizar a comunicação política e promover o engajamento cívico. Contudo, também pode ser utilizada para manipular eleitores, amplificar desinformação e desequilibrar o jogo democrático.



O Brasil tem diante de si a oportunidade de agir de forma preventiva, aprendendo com os erros de eleições passadas — tanto no cenário nacional quanto internacional. Para isso, é necessário que haja regulamentação clara, fortalecimento institucional, educação crítica da população e responsabilização de atores que abusam do uso tecnológico para fins eleitorais escusos.

A eleição de 2026 será o primeiro grande teste da maturidade democrática brasileira na era da inteligência artificial. Mais do que nunca, será preciso alinhar inovação e integridade, tecnologia e confiança pública, liberdade de expressão e responsabilidade informacional. Não se trata de frear a IA, mas de garantir que ela sirva à democracia — e não o contrário.

Referências:

- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Security and Privacy Controls for Information Systems and Organizations*. NIST Special Publication 800-53 Rev. 5, 2020. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>. Acesso em: 7 out. 2025.
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Computer Security Incident Handling Guide*. NIST Special Publication 800-61 Rev. 2, 2012. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>. Acesso em: 7 out. 2025.
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Guide to Enterprise Patch Management Technologies*. NIST Special Publication 800-40 Rev. 3, 2013. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final>. Acesso em: 7 out. 2025.
- INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). *IEC 62443-3-3 – Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels*. Genebra, 2013.
- INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). *IEC 62443-2-1 – Requirements for an IACS Security Management System*. Genebra, 2010.
- BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.



- BRASIL. *Projeto de Lei n.º 2338, de 2023*. Estabelece princípios, direitos e deveres para o uso de Inteligência Artificial no Brasil. Senado Federal, Brasília, DF, 2023. Disponível em: <https://www25.senado.leg.br>. Acesso em: 7 out. 2025.
- UNIÃO EUROPEIA. *Artificial Intelligence Act*. Regulamento sobre inteligência artificial. Bruxelas, 2023. Disponível em: <https://artificialintelligenceact.eu>. Acesso em: 7 out. 2025.
- UNITED STATES. *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. Washington, DC, 2023. Disponível em: <https://www.whitehouse.gov>. Acesso em: 7 out. 2025.
- NIC.BR; CGI.BR. *Indicadores de Governança da Internet no Brasil – Tráfego Digital Eleitoral 2024*. São Paulo: NIC.br, 2025.
- SENADO FEDERAL. *DataSenado: Pesquisa sobre percepção digital e confiança em redes sociais*. Brasília, 2025. Disponível em: <https://www.datasenado.leg.br>. Acesso em: 7 out. 2025.
- PROJETO COMPROVA. *Relatórios de monitoramento de desinformação nas eleições*. Coalizão Direitos na Rede, São Paulo, 2024–2025. Disponível em: <https://projetoaprova.com.br>. Acesso em: 7 out. 2025.
- FUNDAÇÃO GETULIO VARGAS (FGV). *Diretoria de Análise de Políticas Públicas (DAPP): Estudo de resposta digital nas eleições*. Rio de Janeiro, 2023.
- UNIVERSIDADE DE BRASÍLIA (UnB). *Laboratório de Democracia Digital: Estudo de interações eleitorais com IA*. Brasília, 2024.
- INSTITUTO BETA: INTERNET E DEMOCRACIA. *Relatório de Transparência Algorítmica*. São Paulo, 2025.
- INSTITUTO EDUCAmídia. *Relatórios de alfabetização midiática e combate à desinformação em escolas públicas*. São Paulo, 2025.
- TI SAFE. *Relatório C4ISR Election Cyber Review*. Rio de Janeiro: TI Safe Labs, 2025. (Documento técnico interno).
- INTERNETLAB. *Regulação e ética em IA no contexto político-eleitoral*. São Paulo, 2024. Disponível em: <https://www.internetlab.org.br>. Acesso em: 7 out. 2025.
- CODING RIGHTS. *Direitos digitais, IA e justiça algorítmica*. São Paulo, 2025. Disponível em: <https://www.codingrights.org>. Acesso em: 7 out. 2025.
- OPENAI. *Blog Oficial e Documentação Técnica GPT-4*. San Francisco, 2023–2024. Disponível em: <https://openai.com/blog>. Acesso em: 7 out. 2025.



- UNESCO. *Diretrizes sobre Governança de Plataformas Digitais e Inteligência Artificial*. Paris, 2022. Disponível em: <https://unesco.org>. Acesso em: 7 out. 2025.
- UNIVERSIDADE FEDERAL DE MINAS GERAIS; FGV; UnB. *Publicações acadêmicas sobre IA, eleições e democracia*. Brasil, 2023–2025.

