

# Quando a IA Interfere nas Eleições

Quatro Ações para Proteger a Integridade Eleitoral e Preservar a Democracia<sup>1</sup>

Catherine Régis, Florian Martin-Bariteau,  
Jake Okechukwu Effoduh, Juan David Gutiérrez,  
Gina Neff, Carlos Affonso Souza e Célia Zolynski

## Por que IA e Eleições é um Tema Crítico?

As tecnologias há muito tempo influenciam as eleições, tanto positiva quanto negativamente, impactando seus resultados e a qualidade do debate público. Por exemplo, a Internet permite que os cidadãos se organizem de maneira mais eficaz do que nunca, capacitando-os a defender ideias e causas específicas. No entanto, também se tornou um canal poderoso para a desinformação.

O avanço da inteligência artificial (IA) apresenta novas ameaças significativas, incluindo a multiplicação de deepfakes, riscos elevados de cibersegurança, o surgimento de agentes manipuladores e a proliferação de dados sintéticos e contas falsas. Ao mesmo tempo, a IA oferece aos atores políticos uma ferramenta poderosa para se conectar com os eleitores e influenciar a opinião pública. Ao explorar tendências eleitorais já existentes, a IA tem o potencial de remodelar profundamente o processo democrático e influenciar os resultados das eleições. No entanto, sem medidas proativas, a IA pode agravar tendências preocupantes, como a polarização política e a queda da confiança na democracia.

Os governos devem tomar medidas decisivas com relação à IA, especialmente em um momento em que as democracias ao redor do mundo enfrentam desafios crescentes e ataques a seus processos eleitorais. Atuando em diversas frentes, será possível fortalecer os sistemas democráticos, melhorar a confiança na sociedade e garantir que a IA seja utilizada de forma responsável para aumentar a integridade das eleições.

## Principais Conclusões

- Exemplos recentes do Brasil, Romênia, Gabão, Estados Unidos e outros países revelam como o uso de inteligência artificial (IA) por atores políticos pode prejudicar a integridade eleitoral e a democracia.
- Os países usualmente não estão preparados para os desafios relacionados à IA: muitos não possuem regras que regulamentam o uso de IA em eleições, os partidos políticos ainda não chegaram a um consenso sobre práticas eleitorais justas na era da IA, e a maioria das jurisdições não consegue lidar de forma eficaz com ataques impulsionados por IA contra suas instituições democráticas.
- Recomendamos quatro ações: 1) os países devem atualizar as regras eleitorais (por exemplo, proibindo conteúdos enganosos gerados por IA); 2) os partidos políticos devem adotar um código de conduta com diretrizes claras para o uso responsável da IA na política; 3) as autoridades eleitorais devem estabelecer equipes independentes para prevenir e responder a incidentes envolvendo IA; e, 4) no âmbito internacional, os países devem criar um programa de Promotores da Integridade Eleitoral para IA e protocolos para lidar com interferências transfronteiriças.

## Como a IA representa uma ameaça para eleições e a democracia

Existem muitas formas pelas quais o uso de IA por atores políticos, tanto locais quanto estrangeiros, pode acabar prejudicando a integridade das eleições e da democracia.

Por exemplo, um estudo do Digital Forensic Research Lab descobriu que, durante as eleições brasileiras de 2024, nos seis meses antes da votação, políticos locais ou seus apoiadores usaram IA pelo menos 75 vezes para produzir imagens sintéticas, conteúdos de áudio ou vídeos com o objetivo de impulsionar suas candidaturas ou prejudicar seus adversários. Em particular, cinco candidatas foram vítimas de pornografia deepfake,<sup>2</sup> um fenômeno que frequentemente desestimula mulheres a assumirem cargos públicos.<sup>3</sup>

O Serviço de Inteligência Estrangeira da Romênia relatou, em dezembro de 2024, que a Rússia tentou influenciar as eleições presidenciais do país. Primeiramente, a Rússia teria utilizado propaganda de extrema-direita pró-Rússia e conteúdos gerados por IA disseminando-os por meio de uma ampla rede de canais de mídia social e contas automatizadas. Em segundo lugar, com a ajuda da IA (que pode ser usada para desenvolver malware capaz de burlar defesas de cibersegurança), a Rússia presumivelmente organizou cerca de 85.000 ataques contra a Autoridade Eleitoral Permanente da Romênia para obter acesso a seus bancos de dados. Como resultado da interferência russa, o Tribunal Constitucional da Romênia acabou anulando o primeiro turno das eleições presidenciais.<sup>4</sup>

Na campanha eleitoral do Gabão em 2023, uma controvérsia emergiu enquanto os eleitores se preparavam para um histórico triplo pleito—presidencial, legislativo e local. Perto do final da campanha, gravações de áudio surgiram nas redes, supostamente apresentando dois importantes líderes da oposição discutindo estratégias, alianças e apoio externo. O presidente em exercício acusou a oposição de “fomentar um levante popular”, enquanto a coalizão opositora denunciou as gravações como um “uso infame de IA”. O caso do Gabão destaca como o avanço da IA complica o debate público, tornando cada vez mais difícil para os eleitores distinguirem fato de ficção.<sup>5</sup>

Por fim, especialistas testaram os principais modelos de IA durante a campanha presidencial dos Estados Unidos em 2024 para avaliar sua capacidade de fornecer informações precisas sobre as eleições.

Os testes revelaram discrepâncias entre os conteúdos apresentados em diferentes idiomas e entre os compromissos públicos das empresas de IA com a precisão da informação eleitoral e o desempenho real de seus modelos.<sup>6</sup> Esses exemplos demonstram como diversos países frequentemente não estão preparados para enfrentar os desafios trazidos pelo crescimento da IA. Nossas recomendações sugerem formas de evitar ou mitigar os impactos negativos que as tecnologias emergentes têm sobre as eleições.

***Eleições locais são particularmente vulneráveis à influência da IA, uma vez que as autoridades locais muitas vezes carecem dos recursos e salvaguardas necessários para mitigar os riscos de forma eficaz.***

## Primeiro Desafio Muitos países ainda não adotaram regras para o uso de IA em eleições

A ausência de regras claras e específicas sobre o uso de IA em eleições gera incerteza jurídica, tornando difícil para as autoridades atribuírem responsabilidades ou tomarem medidas eficazes contra abusos.

Muitas regras eleitorais ao redor do mundo foram adotadas anos antes da IA generativa se tornar amplamente disponível e utilizada. Como resultado, elas frequentemente são muito genéricas para lidar com os riscos específicos que a IA apresenta. Por exemplo, muitas legislações não possuem definições de “mídia sintética” ou “conteúdo gerado por IA” e falham em estabelecer os limites do seu uso no contexto eleitoral.

Poucos legisladores aprovaram ou sequer discutiram propostas de regras eleitorais que abordem especificamente os desafios da IA nas eleições. No Reino Unido, por exemplo, as leis existentes sobre difamação focam na proteção de indivíduos contra declarações falsas, mas são ambíguas quando se trata de imagens ou vídeos falsos.<sup>7</sup>

Regras claras e harmonizadas são essenciais para garantir a responsabilização, aumentar a transparência e permitir intervenções oportunas. Ao preencher essas lacunas regulatórias, os formuladores de políticas podem oferecer salvaguardas robustas para preservar a integridade dos processos democráticos e reduzir a crescente insegurança em torno dos desafios eleitorais impulsionados pela IA.

## Ação 1 Os países devem atualizar as regras eleitorais

Os países devem atualizar as regras eleitorais para garantir que políticos, partidos políticos, empresas de tecnologia e eleitores saibam exatamente:

- como a mídia sintética pode ser usada em atividades eleitorais;
- quais usos dos sistemas de IA são proibidos ou limitados no contexto eleitoral; e
- como a responsabilidade deve ser atribuída quando as normas estabelecidas pelas regras eleitorais forem violadas.

Para garantir que a liberdade de comunicação política não seja excessivamente restringida, as novas regras eleitorais devem ser proporcionais ao risco que buscam prevenir. Autoridades independentes encarregadas de supervisionar o uso da IA em eleições precisarão de conhecimento técnico adequado e financiamento suficiente para fazer cumprir essas regras de forma eficaz.

Os países devem esclarecer as definições de termos-chave, como dados sintéticos, IA generativa, conteúdo gerado por IA e informação enganosa ou manipulada, além de avaliar a necessidade de modificar aspectos específicos de suas regras atuais. Além disso, eles devem considerar seriamente a adoção das seguintes normas obrigatórias:

- **Devem ser introduzidas proibições sobre o uso, publicação, exibição ou circulação de conteúdos enganosos gerados por IA com o objetivo de influenciar uma eleição. Por exemplo, as autoridades devem considerar a proibição do uso de imagens, vídeos ou áudios gerados por IA que retratem falsamente candidatos ou campanhas, ou que amplifiquem desinformação sobre um candidato, um referendo ou o processo eleitoral;**

- **Políticos e partidos políticos devem cumprir obrigações de transparência, como rotular imagens, clipes de áudio e vídeos gerados por IA utilizados, exibidos ou publicados em eleições. Para criar ou aprimorar esses rótulos, as autoridades devem realizar pesquisas científicas e coletar opiniões do público. Os rótulos devem ser facilmente reconhecidos pelos cidadãos, levando em consideração aspectos como design visual, redação, tamanho, duração, posição e momento de exibição;**
- **As autoridades devem obrigar as plataformas online a implementar políticas de rotulagem para anúncios políticos gerados por IA e a criar e aplicar rigorosamente regras de moderação de conteúdo para conter a disseminação de conteúdos prejudiciais gerados por IA.**

*As regras eleitorais devem abranger chatbots, que podem produzir informações enganosas sobre elementos-chave de uma eleição, como a localização das seções eleitorais, os documentos necessários para votar ou os antecedentes criminais dos candidatos.<sup>8</sup>*

## Segundo Desafio

# Os partidos políticos não chegaram a um consenso sobre o que constitui uma eleição livre e justa na era da IA

Los partidos políticos y los candidatos pueden. Atualmente, partidos políticos e candidatos podem utilizar ferramentas de IA para criar deepfakes sofisticados, gerar conteúdo enganoso em larga escala, microdirecionar eleitores com desinformação personalizada ou manipular o discurso público por meio de contas automatizadas.

Na ausência de regulamentação, diretrizes claras ou marcos éticos, há o risco de que partidos políticos utilizem a IA de maneira que prejudique a confiança dos eleitores, espalhe informações falsas e influencie de forma indevida os resultados das eleições.

Sem regras acordadas, os partidos políticos podem sentir-se pressionados a intensificar o uso de ferramentas de IA de maneira cada vez mais agressiva para não ficarem atrás de seus adversários. A pressão política pode criar uma espiral na qual os partidos priorizem o uso da IA para vencer a qualquer custo, em detrimento da integridade eleitoral.

## Ação 2

# Os partidos devem adotar um código de conduta como ponto de partida para assumir responsabilidade pelo comportamento político na era da IA

Códigos de conduta têm como objetivo fazer com que os atores políticos concordem em se comprometer com eleições livres e justas, adotando certos comportamentos ou evitando outros. Códigos de conduta sobre IA geralmente promovem a transparência e a honestidade no uso dessa tecnologia para fins eleitorais.

Códigos desse tipo já existem em algumas jurisdições. Por exemplo, em 2023, cinco partidos suíços se comprometeram a serem transparentes no uso da IA e a não a empregar para fins depreciativos. Para as eleições do Parlamento Europeu em 2024, os partidos endossaram conjuntamente um código de conduta com disposições específicas sobre o uso de IA. Países como o Reino Unido e algumas entidades subnacionais já iniciaram esforços para desenvolver códigos semelhantes.

Os códigos de conduta para o uso de IA em eleições devem comprometer os partidos a:

- **não usar ferramentas de IA para produzir conteúdo materialmente enganoso ou induzir os eleitores ao erro;**
- **rotular claramente os conteúdos quando recorrerem à IA de forma não trivial (dado o vácuo legislativo identificado anteriormente e a urgência da questão);**
- **não amplificar conteúdo sintético materialmente enganoso e denunciar comportamentos inadequados, tanto na publicação quanto na disseminação de conteúdo enganoso;**
- **fornecer diretrizes claras e treinamento adequado a funcionários do partido, membros, militantes e apoiadores sobre o uso de ferramentas de IA em campanhas eleitorais;**
- **abster-se de produzir, usar ou disseminar conteúdos enganosos, incluindo contas falsas, bots automáticos ou chatbots, para manipular a opinião dos eleitores;**
- **introduzir “camadas de moderação” em seus chatbots para direcionar os usuários da Internet a informações eleitorais oficiais; e**
- **comprometer-se a monitorar, auditar e revisar o uso de IA e ferramentas habilitadas por IA após as eleições.**

## Terceiro Desafio

# A maioria das jurisdições não está preparada para ataques impulsionados por IA contra suas eleições e instituições democráticas

Os países desenvolveram estratégias e mecanismos para enfrentar grandes crises, como desastres naturais, agitações civis ou pandemias. No entanto, muitos governos ainda não estão prontos para lidar com ataques impulsionados por IA contra a integridade de suas eleições e instituições democráticas.

Enfrentar com sucesso as ameaças da IA à integridade eleitoral é um desafio multifacetado. Aqui vão três pontos de atenção:

Em primeiro lugar, os países frequentemente carecem de sistemas abrangentes de monitoramento para detectar desinformação gerada por IA, deepfakes e outras campanhas automatizadas de influência direcionadas aos seus processos democráticos. Essa lacuna de conhecimento é agravada pela falta de mecanismos de colaboração entre as partes interessadas, como agências governamentais, plataformas de mídia social, veículos de imprensa e grupos da sociedade civil. Quando atividades suspeitas são detectadas, muitas vezes não há um protocolo claro para o compartilhamento de informações ou a coordenação de uma resposta.

Na sequência, vale destacar que muitas autoridades eleitorais não possuem o conhecimento necessário sobre IA para distinguir ameaças, deixando-as despreparadas para tomar medidas. Essa lacuna de capacitação se estende por todo o ecossistema democrático. Por exemplo, mesários e observadores eleitorais, que atuam como defensores da integridade eleitoral na linha de frente, geralmente recebem treinamento mínimo sobre ameaças digitais e podem ter dificuldades para responder a perguntas dos eleitores sobre conteúdo gerado por IA ou tentativas de manipulação.

Por fim, as autoridades eleitorais frequentemente não possuem a infraestrutura técnica, a expertise humana e a capacidade necessária para monitorar e combater ataques impulsionados por IA de

maneira eficaz. Sem esses recursos, as jurisdições são forçadas a reagir aos incidentes conforme eles ocorrem, em vez de implementar estratégias preventivas de defesa.

## Ação 3

# As autoridades eleitorais devem estabelecer uma equipe independente e multidisciplinar responsável por prevenir e responder a incidentes eleitorais causadas por IA

As autoridades eleitorais devem contar com uma equipe independente e multidisciplinar, operando sob supervisão judicial. Essa equipe deve ter o apoio de todas as partes interessadas no processo democrático e eleitoral da jurisdição. Ela deve estabelecer vínculos adequados com atores do ambiente midiático, plataformas online e outras entidades regionais ou internacionais relevantes. Além disso, deve incluir representantes dos partidos políticos para garantir que os protocolos de emergência e mitigação sejam considerados justos e equilibrados.

A equipe deve atuar tanto dentro quanto fora do ciclo eleitoral para manter a vigilância sobre ataques à democracia. Sua principal responsabilidade seria desenvolver um Plano de Resposta Eleitoral à IA, que defina estruturas claras de avaliação, responsabilidades, abordagens de comunicação, entre outros elementos. Essa abordagem se baseia em estratégias consolidadas de preparação para emergências em áreas como gestão de crises de saúde pública, resposta a desastres naturais e prontidão para incidentes de cibersegurança.

Essas estratégias já implementaram com sucesso sistemas de alerta precoce, protocolos de notificação, exigências obrigatórias de divulgação de incidentes, acordos de compartilhamento de recursos e equipes de resposta rápida.

Todos os atores do ecossistema midiático e da Internet devem participar da implementação do plano de resposta para limitar a disseminação de um ataque e alertar os cidadãos.

As autoridades eleitorais devem conduzir exercícios de simulação para permitir que os envolvidos compreendam como a IA pode ser usada, testem o plano de resposta e identifiquem possíveis vulnerabilidades que agentes mal-intencionados poderiam explorar.

O Plano de Resposta Eleitoral à IA deve levar em conta os direitos fundamentais dos cidadãos, protegendo contra ameaças de vigilância ou controle da expressão política.

*Para garantir que os incidentes eleitorais causados por IA sejam combatidos de forma eficaz, treinamentos adequados sobre IA e cibersegurança devem ser oferecidos a todos os atores do ecossistema democrático e eleitoral, incluindo mesários e observadores eleitorais.*

## Quarto Desafio

### A interferência eleitoral apoiada por IA frequentemente envolve atores ocultos operando em várias jurisdições

A natureza transnacional de muitos ataques eleitorais impulsionados por IA explica por que é difícil para jurisdições individuais enfrentá-los de maneira eficaz. Esse problema é agravado pela assimetria de recursos e conhecimento entre os governos, já que alguns não possuem a expertise, as ferramentas, os recursos ou a capacidade necessária para detectar e combater adequadamente as ameaças eleitorais impulsionadas por IA.

Sem protocolos internacionais alinhados, torna-se um desafio responsabilizar os perpetradores devido às diferenças entre sistemas legais, capacidades investigativas e limites jurisdicionais.

Os Estados democráticos devem reconhecer que um ataque contra uma democracia é um ataque contra os princípios que unem todas as democracias. A decisão por uma ação coletiva, portanto, é essencial para proteger valores democráticos compartilhados, aumentar a confiança dos cidadãos e garantir a integridade das eleições em todo o mundo.

## Ação 4

### Os países devem estabelecer uma iniciativa internacional de promotores da integridade eleitoral frente à IA e protocolos internacionais de assistência jurídica mútua em casos de interferência eleitoral relacionada à IA

Os Estados devem estabelecer uma iniciativa internacional centralizada para monitorar e reagir a casos de interferência eleitoral relacionados à IA: os Promotores Internacionais da Integridade Eleitoral para IA (International AI Electoral Trustkeepers).

Essa iniciativa reuniria especialistas multidisciplinares e instituições comprometidas com a detecção, mitigação e combate à interferência eleitoral impulsionada por IA. Ela serviria como um recurso técnico para países vulneráveis a tais interferências, oferecendo expertise, ferramentas e colaboração para lidar com ameaças eleitorais transnacionais. Os Promotores Internacionais da Integridade Eleitoral para IA também forneceriam suporte em crises, enviando equipes de resposta rápida para auxiliar durante eventos eleitorais críticos e monitorando situações de alto risco em tempo real.

A criação desses Promotores poderia surgir de iniciativas já existentes voltadas para a proteção eleitoral e mitigação de riscos da IA. Por exemplo, medidas poderiam ser tomadas para fornecer novos ou melhores recursos de IA (como especialistas temporários ou permanentes) e competências técnicas ou jurídicas à Divisão de Assistência Eleitoral da ONU (UN Electoral Assistance Division),<sup>9</sup> que apoia os Estados-membros na realização de eleições que expressem legitimamente a vontade do povo.

Além disso, a Rede Internacional de Institutos de Segurança da IA (International Network of AI Safety Institutes) poderia ser aproveitada para treinar e implantar esse programa ao redor do mundo.

Quando houver necessidade de expertise da indústria, os Promotores Internacionais poderiam ser apoiados por empresas do setor privado, como as companhias de IA e plataformas que integram o Acordo Tecnológico para Combater a Interferência Eleitoral com IA (Tech Accord to Combat AI-Generated Election Interference).<sup>10</sup>

Além disso, os mecanismos de assistência jurídica mútua serão essenciais para investigar e processar casos de interferência eleitoral impulsionada por IA, facilitando a cooperação entre jurisdições, a coleta e o compartilhamento de provas admissíveis provenientes de múltiplos países e garantindo que os perpetradores não explorem brechas legais para escapar da responsabilização. Esses mecanismos judiciais já foram eficazes na abordagem de outros desafios transnacionais, como o combate ao cibercrime, fraudes digitais, terrorismo, crime organizado, violações de direitos humanos e crimes de guerra.

***Esses mecanismos internacionais precisarão ser transparentes para garantir a proteção dos direitos fundamentais.***

## Conclusão

O impacto da IA na democracia ainda não está consolidado.

Embora este documento tenha se concentrado nos riscos, a IA também pode fortalecer as democracias. Autoridades eleitorais poderiam usar ferramentas de IA para lidar com tarefas complexas de maneira eficiente. Essas ferramentas poderiam tornar a votação mais acessível e incentivar a participação cívica.

Por exemplo, durante a contestada eleição de 2024 no Paquistão, a IA permitiu que o partido de um líder opositor preso enviasse mensagens de áudio para mobilizar eleitores, mesmo sob severas restrições.<sup>11</sup> No futuro, os defensores da democracia devem explorar como a IA pode aprimorar os sistemas democráticos.

Porém, a prioridade atual é proteger as democracias contra um perigo iminente: atores mal-intencionados, tanto nacionais quanto estrangeiros, que abusam da IA.

Isso exige ações em dois níveis.

Dentro dos países: os governos devem atualizar suas leis, os partidos políticos devem cooperar e as autoridades eleitorais devem se preparar para defender a integridade democrática contra abusos da IA.

Entre os países: a cooperação internacional é essencial. Nenhuma nação pode enfrentar os desafios da IA sozinha. Os países precisam alinhar suas leis sobre interferência eleitoral que use IA, fortalecendo tanto suas defesas individuais quanto sua resistência coletiva contra tentativas de enfraquecer a democracia globalmente.

Ao tomar essas medidas hoje, criaremos sistemas democráticos mais fortes, inclusivos e confiáveis para o futuro.

## Referências

1. A versão original deste texto foi produzida em inglês sob o título "AI in the Ballot Box". A tradução para o português foi realizada pelo professor Carlos Affonso Pereira de Souza, da Universidade do Estado do Rio de Janeiro (UERJ).
2. Farrugia, B. (2024, 26 de novembro). Brazil's electoral deepfake law tested as AI-generated content targeted local elections. DFRLab. <https://dfrlab.org/2024/11/26/brazil-election-ai-deepfakes>
3. Para mais informações sobre como a IA pode representar uma ameaça para a segurança de mulheres, vide: United Nations Educational, Scientific and Cultural Organization (2023). Technology-facilitated gender-based violence in an era of generative AI (World Trends in Freedom of Expression and Media Development Series). <https://unesdoc.unesco.org/ark:/48223/pf0000387483>
4. Harward, C. (2024, 6 de dezembro). Likely Kremlin-backed election interference against Romania threatens Bucharest's continued support for Ukraine and NATO. Institute for the Study of War. <https://understandingwar.org/backgrounder/likely-kremlin-backed-election-interference-against-romania-threatens-bucharests>
5. RFI. (2023, 23 de agosto). Élections au Gabon: polémique après des enregistrements supposés de candidats de l'opposition. RFI. <https://www.rfi.fr/fr/afrique/20230823-%C3%A9lections-au-gabon-pol%C3%A9mique-apr%C3%A8s-des-enregistrements-suppos%C3%A9s-de-candidats-de-l-opposition>
6. Palta, R., Angwin, J., & Nelson, A. (2024, 27 de fevereiro). How we tested leading AI models performance on election queries. Proof. <https://www.proofnews.org/how-we-tested-leading-ai-models-performance-on-election-queries>; Impelli, M. (2024, 31 de outubro). Voting rights groups warn about AI generating unfounded claims in Spanish. Newsweek. <https://www.newsweek.com/2024-election-spanish-latino-voters-artificial-intelligence-concerns-1978170>; Ott, H., & Lyons, E. (2024, 25 de junho). ChatGPT gave incorrect answers to questions about how to vote in battleground states. CBS News. <https://www.cbsnews.com/news/chatgpt-chatbot-ai-incorrect-answers-questions-how-to-vote-battleground-states>
7. Stockwell, S., Hughes, M., Swatton, P., & Bishop, K. (2024). AI-enabled influence operations: the threat to the UK general election. CETaS Briefing Papers. [https://cetas.turing.ac.uk/sites/default/files/2024-05/cetas\\_briefing\\_paper\\_-\\_ai-enabled\\_influence\\_operations\\_-\\_the\\_threat\\_to\\_the\\_uk\\_general\\_election.pdf](https://cetas.turing.ac.uk/sites/default/files/2024-05/cetas_briefing_paper_-_ai-enabled_influence_operations_-_the_threat_to_the_uk_general_election.pdf)
8. Kaye, R. (2023, 5 de abril). Australian mayor readies world's first defamation lawsuit over ChatGPT content. Reuters. <https://www.reuters.com/technology/australian-mayor-readies-worlds-first-defamation-lawsuit-over-chatgpt-content-2023-04-05>
9. United Nations Department of Political and Peacebuilding Affairs. (2023). 2023 factsheet: electoral assistance. [https://dppa.un.org/sites/default/files/electoral\\_assistance.pdf](https://dppa.un.org/sites/default/files/electoral_assistance.pdf)
10. AI Elections Accord (2024, 16 de fevereiro). A tech accord to combat deceptive use of AI in 2024 elections. [https://www.aielectionsaccord.com/uploads/2024/02/A-Tech-Accord-to-Combat-Deceptive-Use-of-AI-in-2024-Elections.FINAL\\_.pdf](https://www.aielectionsaccord.com/uploads/2024/02/A-Tech-Accord-to-Combat-Deceptive-Use-of-AI-in-2024-Elections.FINAL_.pdf)
11. Zhuang, Y. (2024, 11 de fevereiro). Imran Khan's 'Victory Speech' from jail shows A.I.'s peril and promise. The New York Times. <https://www.nytimes.com/2024/02/11/world/asia/imran-khan-artificial-intelligence-pakistan.html>

## Relatórios de Política Global sobre IA

Os Relatórios de Política Global sobre IA é uma iniciativa conjunta do IVADO, o principal consórcio de pesquisa e mobilização de conhecimento sobre IA do Canadá, sediado na Université de Montréal, e da l'initiative IA + Sociétés, da Université d'Ottawa. O objetivo é fornecer recomendações baseadas em evidências aos formuladores de políticas visando o enfrentamento de desafios globais emergentes relacionados à inteligência artificial.

Para esta primeira edição, os professores Catherine Régis e Florian Martin-Bariteau reuniram um grupo de especialistas internacionais em IA para desenvolver diretrizes políticas globais e práticas sobre o impacto da IA na democracia e na integridade eleitoral. O relatório foi produzido após um retiro de uma semana, realizado pela Società Italiana per l'Organizzazione Internazionale (SIOI), em Roma, Itália, em dezembro de 2024. O texto foi escrito com o apoio de Réjean Roy, diretor de Mobilização do Conhecimento do IVADO.

Este projeto foi viabilizado graças à contribuição do Fonds de recherche du Québec, do CEIMIA, da Chaire Canada-CIFAR em IA et droits de la personne del Mila, e da Chaire de recherche de l'Université d'Ottawa en technologie et société.

Além disso, contou com o apoio da Delegação de Quebec em Roma e da SIOI para a organização do retiro.

As opiniões expressas neste relatório de políticas são exclusivamente dos autores.



**Catherine Régis** é professora de direito na Université de Montréal e diretora de Inovação Social e Política Internacional do IVADO. Especialista em governança da IA, ela codirige o programa de pesquisa do Institut canadien de la sécurité de l'IA e é titular da Chaire Canada-CIFAR em IA et droits de la personne del Mila.



**Florian Martin-Bariteau** é titular da Chaire de recherche en technologie et société e professor associado de direito na Université d'Ottawa, onde lidera a l'initiative AI + Sociétés e o Centre de recherche en droit, technologie et société. Ele também é pesquisador associado do Berkman-Klein Center, da Harvard University.



**Jake Okechukwu Effoduh** é professor assistente na Lincoln Alexander School of Law, da Toronto Metropolitan University, especializado em direito da IA e direitos humanos internacionais. Ele contribui para o desenvolvimento de marcos regulatórios de IA em diversos países e lidera importantes projetos de pesquisa entre o Canadá e países africanos.



**Gina Neff** é professora de IA responsável na Queen Mary University of London e lidera o Minderoo Centre for Technology and Democracy, na University of Cambridge. Sua pesquisa analisa o impacto dos ambientes digitais no trabalho e na vida cotidiana.



**Juan David Gutiérrez**, professor associado na Universidad de Los Andes, em Bogotá, estuda as interseções entre políticas públicas e tecnologias. Como membro especialista da Parceria Global em Inteligência Artificial (GPAI), ele co-lidera o projeto de transparência algorítmica.



**Carlos Affonso Pereira de Souza** é professor da Universidade do Estado do Rio de Janeiro (UERJ) e dirige o Instituto de Tecnologia e Sociedade (ITS Rio). Como professor de direito e tecnologia, ele contribuiu para o desenvolvimento das leis brasileiras sobre Internet e proteção de dados.



**Célia Zolynski** é professora de direito privado na Université Paris 1 Panthéon-Sorbonne, especialista em direito digital e propriedade intelectual. Como coordenadora do Observatório da IA da Paris 1, ela se dedica à regulação da IA e aos direitos fundamentais.

Uma iniciativa conjunta de



Com o apoio de

