IVADO

Initiative IA + Société
AI + Society

AI in the Ballot Box

Four Actions to Safeguard Election Integrity and Uphold Democracy

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

Why AI and Elections Is a Critical Topic

Technologies have long influenced elections, both positively and negatively, shaping their outcomes and the quality of public debate surrounding them. For example, the Internet enables citizens to organize more effectively than ever, empowering them to advocate for specific ideas and causes, but it is also a formidable channel for disinformation.

The rise of artificial intelligence (AI) presents significant new threats, including the multiplication of deepfakes, heightened cybersecurity risks, the emergence of manipulative persuasive agents, and the proliferation of synthetic data and fake accounts. At the same time, AI offers political actors a powerful tool to connect with voters, influence public opinion, and shape the flow of information. By tapping into existing trends in elections, AI has the potential to profoundly reshape the democratic process and influence election outcomes. Without proactive measures, however, AI could exacerbate worrisome trends such as political polarization and declining trust in democracy.

Governments must take decisive action regarding AI, particularly at a time when democracies around the world are facing increasing challenges and attacks on their elections. By acting on various fronts, they will shore up democratic systems, improve trust in society, and ensure that AI is leveraged responsibly to enhance the integrity of elections.

Key Takeaways

- → Recent examples from Brazil, Romania, Gabon, the United States, and other countries show how AI use by political actors can damage electoral integrity and democracy.
- → Nations are often unprepared for AI-related challenges: many lack rules governing AI in elections, political parties haven't agreed on fair electoral practices in the AI age, and most jurisdictions can't effectively counter AI-driven attacks on their democratic institutions.
- → We recommend four actions: governments should update electoral rules (e.g., to prohibit misleading AI-generated content); political parties should adopt a code of conduct with clear guidelines on the responsible political use of AI; electoral authorities should establish independent teams to prevent and respond to AI-driven disruptions; and, at the international level, governments should establish International AI Electoral Trustkeepers and protocols for addressing cross-border interferences.

How AI Poses a Threat to Elections and Democracy

There are many ways in which the use of AI by political actors—both local and foreign—can end up damaging the integrity of elections and democracy.

For example, elections were held in Brazil in October 2024. A study by the Digital Forensic Research Lab found that in the six months before election day, local politicians or their supporters used AI at least 75 times to produce synthetic images, audio content, or videos to boost their candidacies or undermine their opponents. In particular, five female candidates were victims of deepfake pornography,[1] a phenomenon whose impact is often to discourage women from assuming public roles.[2]

Romania's Foreign Intelligence Service reported in December 2024 that Russia targeted that country in an attempt to influence its presidential elections. First, Russia used far-right, pro-Russian propaganda and AI-generated content that it disseminated through a large network of social media channels and AI-generated accounts. Second, with the help of AI (which can help develop malware that evades cybersecurity defences), Russia presumably organized some 85,000 attacks against the Romanian Permanent Electoral Authority to gain access to its databases. Russia's interference ultimately led Romania's Constitutional Court to annul the first round of the presidential elections.[3]

In Gabon's 2023 electoral campaign, a controversy erupted as voters prepared for a historic triple vote—presidential, legislative, and local. Near the campaign's end, audio recordings surfaced online, allegedly featuring two prominent opposition figures discussing strategies, alliances, and external support. The incumbent president accused the opposition of "fomenting a popular uprising," while the opposition coalition condemned the recordings as an "infamous use of AI." The Gabon case highlights how AI's rise complicates public debate, making it increasingly difficult for voters to distinguish fact from fiction.[4]

Finally, experts tested major AI models during the 2024 U.S. presidential election campaign on how well they performed on delivering accurate information about elections. These tests showed discrepancies with respect to information in different languages, and between AI companies' stated commitments to accurate electoral information and the performance of their models.[5]

These examples show how nations and governments often are not prepared to face the challenges posed by the rise of AI. Our recommendations suggest ways to avoid or mitigate the negative impacts that emerging technologies have on elections.

Local elections are especially vulnerable to AI's influence, since local democracies often lack the resources and safeguards to counter its risks effectively.

First challenge
Many governments have yet to adopt rules governing AI use in elections

The absence of clear and specific rules governing the use of AI in elections creates legal uncertainty, making it difficult for authorities to assign liability or take effective action against abuses.

Many electoral rules worldwide were adopted years before generative AI became publicly available and widely used. As a result, they are often too broad to address the unique risks posed by AI. For instance, many legislations lack definitions of "synthetic media" or "AI-generated content" and fail to define the limits of their use in the context of elections.

Few legislative bodies have adopted or even discussed proposals on electoral rules that would specifically address the challenges of AI in elections. In the United Kingdom, for example, existing defamation laws focus on protecting individuals from false statements but are ambiguous when it comes to fake images or videos.[6]

Clear and harmonized rules are essential to ensure accountability, enhance transparency, and enable timely interventions. By bridging these regulatory gaps, policymakers can provide robust safeguards to uphold the integrity of democratic processes and reduce the growing insecurity surrounding AI-driven electoral challenges.

Action 1
Governments should update electoral rules

Governments should update electoral rules to ensure that politicians, political parties, and tech companies, as well as voters, know precisely:

- → **how synthetic media can be used for electoral-related activities;**
- → **which uses of AI systems are prohibited or limited in the context of elections; and**
- → **how liability is to be allocated when the duties established by electoral rules are breached.**

To ensure that freedom of political communication is not significantly restricted, new electoral rules should be proportionate to the risk they seek to prevent. Independent authorities overseeing AI in elections will need adequate technical expertise and funding to effectively enforce these rules.

Jurisdictions should clarify definitions of key terms, such as synthetic data, generative AI, generative AI content, and misleading or deceptive information, and assess the necessity of amending particular aspects of their current rules. In addition, they should seriously consider adopting the following mandatory rules:

- → **Bans should be introduced on the use, publication, screening, or circulation of misleading AI-generated content to influence an election. For example, governments should consider prohibiting the use of AI-generated images, videos, or audio that portray candidates or referendum campaigns falsely or misleadingly, or that amplify misinformation about a candidate, a referendum campaign, or the electoral process.**
- → **Politicians and political parties should have to comply with transparency obligations such as labelling AI-generated images, audio clips, and videos used, published, screened, or circulated in elections. To create or improve these labels, governments should study scientific research and gather input from the public. Labels should be easy to recognize by citizens, with consideration of aspects such as visual design, wording, size, duration, position, and timing.**
- → **Governments should obligate online platforms to implement labelling policies for AI-generated political ads, and to create and strictly enforce content moderation rules to curb the dissemination of harmful AI-generated content.**

Electoral rules should cover chatbots, which can produce misleading information about key elements of an election, such as the location of polling stations, what documents are required to vote, or the criminal records of candidates.[7]

Second challenge
Political parties have not agreed on what constitutes free and fair elections in the age of AI

Political parties and candidates can now potentially leverage AI tools to create sophisticated deepfakes, generate misleading content at scale, micro-target voters with personalized disinformation, or manipulate public discourse through automated accounts.

In the absence of regulation, clear guidelines or ethical frameworks, there is a risk that political parties could use AI in a way that contributes to undermining voter trust, spreading false information, and unfairly influencing election outcomes.

Without agreed-upon rules, political parties might feel compelled to escalate their use of AI tools in increasingly aggressive ways to avoid falling behind their opponents. Political pressure could create a spiral where parties prioritize using AI to win at any cost over maintaining electoral integrity.

Action 2
Parties should adopt a code of conduct as a starting point for taking responsibility for political behaviour in the age of AI

Codes of conduct aim to have political actors agree to commit to free and fair elections by adopting certain behaviours or avoiding others. Codes of conduct on AI generally support transparency and honesty in using this technology for electoral purposes.

Such codes already exist in certain jurisdictions. For example, in 2023, five Swiss parties committed to being transparent in using AI and not using it for derogatory purposes. For the 2024 European Parliament elections, European parties jointly endorsed a code of conduct with specific provisions governing AI use. Countries like the U.K. and subnational entities have seen efforts to develop such codes.

Codes of conduct on the use of AI for electoral purposes should engage parties to:

- → **not use AI tools to produce materially misleading content or mislead voters;**
- → **clearly label content when parties resort to AI in a non-trivial way (given the legislative gaps identified earlier *and* the urgency of this question);**
- → **not amplify materially misleading synthetic content, and call out bad behaviour in either posting or amplification of misleading content;**
- → **give clear guidelines and proper training to party staff, members, campaigners, and supporters on the use of AI tools for campaigning;**
- → **abstain from producing, using, or disseminating misleading content, including fake accounts, automatic bots, or chatbots, to manipulate voter opinions;**
- → **introduce "moderation layers" to their chatbots so that they direct Internet users to official electoral information; and**
- → **commit to monitoring, auditing, and post-election review of their uses of AI and AI-enabled tools.**

Third challenge
Most jurisdictions are not prepared for AI-driven attacks on their elections and democratic institutions

Governments have developed strategies and mechanisms to face major crises like natural disasters, civil unrest, or pandemics. Many governments are not ready, however, to face AI-driven attacks against the integrity of their elections and democratic institutions.

Successfully facing AI-driven threats to electoral integrity is a multifaceted challenge.

First, governments often lack comprehensive monitoring systems to detect AI generated disinformation, deepfakes, and other automated influence campaigns targeting their democratic processes. This knowledge gap is compounded by insufficient collaboration mechanisms among stakeholders, such as government agencies, social media platforms, news organizations, and civil society groups. When suspicious activities are detected, there is often no clear protocol for sharing information or co-ordinating a response.

Second, many election officials lack the AI literacy required to distinguish threats, leaving them ill-equipped to take action. This capacity gap often extends throughout the whole democratic ecosystem. For example, poll workers and election observers, who serve as frontline defenders of electoral integrity, typically receive minimal training on digital threats and may struggle to handle voter questions about AI-generated content or manipulation attempts.

Third, government agencies often lack the technical infrastructure, human expertise, and capacity needed to monitor and counter AI-driven attacks effectively. Without these, jurisdictions are forced to react to incidents on an as-needed basis rather than implement proactive defence strategies.

Action 3
Electoral authorities should put an independent cross-functional team in charge of preventing and responding to electoral disruptions caused by AI

Electoral authorities should rely on an independent cross-functional team operating under judicial oversight. This team should be supported by all the stakeholders of a jurisdiction's democratic and electoral processes. It should have appropriate links with actors in the media environment, online platforms, and other pertinent regional or international entities. It should also include representatives from political parties to ensure emergency and mitigation protocols are considered fair and balanced.

The team should operate inside and outside the election cycle to maintain vigilance on attacks on democracy. It would be responsible for developing a comprehensive, public response plan for AI threats to elections. The AI Electoral Response Plan would define clear assessment frameworks, responsibilities, communications approaches, etc. This approach draws on established emergency preparedness strategies from fields like public health crisis management, natural disaster response, and cybersecurity incident readiness, which have successfully implemented early warning systems, reporting protocols, mandatory incident disclosure, resource sharing agreements, and rapid-response teams.

All actors of the media and Internet ecosystem should take part in the implementation of the response plan to limit the spread of an attack and alert citizens.

Electoral authorities should conduct table-top exercises or simulations to allow actors to understand how AI can be deployed and used, identify and test the response plan and concrete reactions to incidents, and identify possible vulnerabilities that rogue actors could exploit.

The AI Electoral Response Plan should take into account the fundamental rights of citizens to guard against threats of surveillance or control of political expression.

To ensure that electoral disruptions caused by AI are countered efficiently, adequate AI and cybersecurity training should be delivered to all actors of the democratic and electoral ecosystem, including polling station volunteers and observers.

Fourth challenge
Electoral interference supported by AI often involves covert actors operating across multiple jurisdictions

The transnational nature of many AI-driven electoral attacks explains why it is difficult for individual jurisdictions to address them on their own effectively. This problem is complicated by the asymmetry of resources and knowledge between governments, as some do not have the expertise, tools, resources, or capacity required to detect and counter AI-driven electoral threats adequately.

Without aligned international protocols, it is challenging to hold perpetrators to account due to differences in legal systems, investigative capabilities, and jurisdictional boundaries.

Democratic states should recognize that an attack on one democracy is an attack on the principles that unite all democracies. Collective action is therefore essential to protect shared democratic values, increase citizen trust, and ensure that the integrity of elections worldwide is upheld.

Action 4
Governments should establish International AI Electoral Trustkeepers and international protocols for mutual legal assistance in case of AI-related electoral interference

States should establish a centralized international platform and unit to learn about and react to instances of AI-related electoral interference: the International AI Electoral Trustkeepers.

These would comprise multidisciplinary experts and institutions committed to detecting, countering, and mitigating AI-driven electoral interference. They would serve as a technical resource for countries vulnerable to electoral interference using AI. They would offer expertise, tools, and collaboration for addressing transnational electoral threats. The International AI Electoral Trustkeepers would also offer crisis support by deploying rapid-response teams to assist during active electoral events and provide real-time monitoring and mitigation strategies in high-risk scenarios.

The creation of the International AI Electoral Trustkeepers could emerge from or be aligned with existing initiatives that aim to provide electoral assistance, or protect countries against the possible harms of AI. For example, measures could be taken to provide new or improved AI resources (e.g., ad hoc experts or permanent specialists) or competencies (e.g., technical or legal) to the UN's Electoral Assistance Division,[8] which helps member states to hold elections that legitimately express the will of the people and are deemed credible by national stakeholders. The nascent International Network of AI Safety Institutes could be leveraged for this initiative to train Electoral Trustkeepers and deploy them across the world on specific missions.

When industry expertise is required, the International AI Electoral Trustkeepers could be supported by private sector players, such as the AI and platform companies behind the Tech Accord to Combat AI-Generated Election Interference.[9]

Relying on mutual legal assistance mechanisms will also be essential for investigating and prosecuting cases of AI-driven electoral interference, as this will facilitate the seamless co-operation of players across jurisdictions, help collect and share admissible evidence originating from multiple countries, and ensure that perpetrators using AI to manipulate elections transnationally cannot exploit jurisdictional boundaries to evade accountability.

Such judicial mechanisms have already effectively addressed other transnational challenges requiring cross-border co-operation and evidence sharing, such as the fight against cybercrime, digital fraud, terrorism, organized crime, human rights violations, and war crimes.

These international mechanisms will need to be transparent to ensure the safeguarding of fundamental rights.

Conclusion

The impact of AI on democracy is not set in stone.

While this brief has focused on risks, AI could actually strengthen democracies. Election officials could use AI tools to handle complex tasks efficiently. These tools could make voting more accessible and boost civic participation. For example, during Pakistan's disputed 2024 election, AI enabled a jailed opposition leader's party to deliver audio messages to voters and mobilize them despite restrictions.[10] Looking ahead, democracy advocates should explore how AI can enhance democratic systems.

Now, though, the priority is protecting democracies from a pressing threat: rogue actors, both national and foreign, who misuse AI.

This requires action at two levels.

Within countries, governments must update their laws, political parties must work together, and electoral authorities must prepare to defend democratic integrity against those who would abuse AI.

Between countries, co-operation is essential. No nation can face AI challenges alone. Countries need to align their laws on AI-enabled election interference. This will both strengthen individual defences and build collective resistance against attempts to undermine democracy worldwide.

By taking these steps today, we will create stronger, more inclusive, and more trustworthy democratic systems for tomorrow.

Notes

1. Farrugia, B. (2024, November 26). Brazil's electoral deepfake law tested as AI-generated content targeted local elections. DFRLab. https://dfrlab.org/2024/11/26/brazil-election-ai-deepfakes
2. For more information on how AI presents serious concerns for the safety of women, see: 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
3. Harward, C. (2024, December 6). 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
4. RFI. (2023, August 23). 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
5. Palta, R., Angwin, J., & Nelson, A. (2024, February 27). 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, October 31). Voting rights groups warn about AI generating unfounded claims in Spanish. Newsweek. https://www.newsweek.com/2024-election-spanish-latino-voters-artifical-intelligence-concerns-1978170; Ott, H., & Lyons, E. (2024, June 25). 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
6. 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
7. Kaye, R. (2023, April 5). 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
8. United Nations Department of Political and Peacebuilding Affairs. (2023). 2023 factsheet: electoral assistance. https://dppa.un.org/sites/default/files/electoral_assistance.pdf
9. AI Elections Accord (2024, February 16). 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
10. Zhuang, Y. (2024, February 11). 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

The Global Policy Briefs on AI

The Global Policy Briefs on AI initiative is a joint endeavour of IVADO, Canada's premier AI research and knowledge mobilization consortium at Université de Montréal, and the AI + Society Initiative at the University of Ottawa, aiming to provide policymakers with policy recommendations to navigate key global current AI challenges.

For this first instalment, professors Catherine Régis and Florian Martin-Bariteau convened a group of leading AI experts from around the world to develop actionable globally oriented policy guidance on the impact of AI on democracy and electoral integrity. The brief was produced following a week-long retreat hosted by the Società Italiana per l'Organizzazione Internazionale (SIOI) in Rome, Italy, in December 2024. It was written with the support of Réjean Roy, director, Knowledge Mobilization, IVADO.

This project was undertaken thanks to the contribution of the Fonds de recherche du Québec, CEIMIA, the Canada CIFAR Chair in AI and Human Rights at Mila and the University of Ottawa Research Chair in Technology and Society, and with the help of the Délégation du Québec à Rome and SIOI for the organization of the retreat.

The views expressed in this policy brief are solely those of the authors.

Catherine Régis is a professor of law at Université de Montréal and director, Social Innovation and International Policy, IVADO. As an expert in AI governance, she co-directs the research program at the Canadian AI Safety Institute and holds the Canada CIFAR Chair in AI and Human Rights, Mila.

Florian Martin-Bariteau is the University Research Chair in Technology and Society and an associate professor of law at the University of Ottawa, where he leads the AI + Society Initiative and the Centre for Law, Technology and Society. He is a faculty associate of the Berkman-Klein Center at Harvard University.

An assistant professor at the Lincoln Alexander School of Law at Toronto Metropolitan University, **Jake Okechukwu Effoduh** specializes in AI law and international human rights. He contributes to the development of AI regulatory frameworks in several countries and leads major Canada-Africa research projects.

Juan David Gutiérrez, an associate professor at the University of the Andes in Bogotá, studies the intersections between public policies and technologies. As an expert member of the Global Partnership on Artificial Intelligence (GPAI), he co-leads the algorithmic transparency project.

Gina Neff is professor of responsible AI at Queen Mary University of London, and leads the Minderoo Centre for Technology and Democracy at the University of Cambridge. Her research analyzes the impact of digital environments on work and daily life.

A legal expert specializing in digital law, **Carlos Affonso Pereira de Souza** leads the Institute for Technology and Society in Rio de Janeiro. As a professor of law and technology, he has contributed to the development of Brazilian Internet and data protection laws.

A professor of private law at Université Paris 1 Panthéon-Sorbonne, **Célia Zolynski** is a specialist in digital law and intellectual property. As co-ordinator of the AI Observatory at Paris 1, she focuses on AI regulation and fundamental rights.

A joint endeavour of

IVADO

uOttawa | Initiative IA + Société AI + Society

With the support of

Fonds de recherche Québec

CIFAR

ceimia

This initiative was undertaken thanks in part to funding from the Canada First Research Excellence Fund.