



Brave New Ballot



Generative AI in Election Campaigns and Other Political Communication

FEBRUARY 2026

About IFES

At IFES, we envision a world where people are free, societies are democratic, and elections are fair. We collaborate with civil society, public institutions, and the private sector to build resilient democracies that deliver for everyone. As a global leader in the promotion and protection of democracy, our technical assistance and applied research develop trusted electoral bodies capable of conducting credible elections; effective and accountable governing stakeholders; civic and political processes in which all people can safely and equally participate; and innovative ways in which technology and data can positively serve elections and democracy. Since 1987, IFES has worked in more than 145 countries, from developing to mature democracies. IFES is a global, nonpartisan organization based in Arlington, Virginia, USA, and registered as a nonprofit organization [501(c)(3)] under the United States tax code.



**International Foundation
for Electoral Systems**

2000 M Street NW, Washington, DC, 20036, United States

www.IFES.org

 IFES1987

To request reprints or author engagement, please message Media@IFES.org

Brave New Ballot

Generative AI in Election Campaigns and Other Political Communication

Identifying Opportunities for Voter Engagement and Threats to Democratic Trust

AUTHOR

Dr. Fernanda Buriel

Deputy Director, IFES Center for Applied Research and Learning

PUBLISHED FEBRUARY 2026



International Foundation
for Electoral Systems



Sida

Brave New Ballot: Generative AI in Election Campaigns and Other Political Communication

Table of Contents

- Executive Summary.....3
 - Definitions, Scope, and Methodology3
 - Summary of Findings4
- Introduction5
- GenAI Applications in Election Campaigns and Other Political Communications: An Overview6
 - A multitude of actors6
 - A multitude of purposes6
 - Double-edged swords6
 - Promoting or benefiting particular political actors7
 - Damaging the reputation or electability of particular political actors.....9
 - Suppressing voters or otherwise manipulating voting patterns to affect results..... 11
 - Undermining trust in results, election authorities, and democratic systems 12
 - Manipulating public narratives 13
- Potential Factors Related to the Impact and Effectiveness of Synthetic Content in Elections 15
 - Impact versus Effectiveness 15
 - Content quality 16
 - Media environment: trust in media and prevalence of editorial media versus social media for news consumption 16
 - Citizens’ media literacy and resilience against disinformation..... 17
- Accountability Challenges 17
 - Establishing the responsibility burden: builders, creators, and disseminators 17
 - Determining consent of implicated actors 18
 - Establishing deception intent 19
 - Preventing accountability evasion through AI personas20

Ethical Challenges 21

- Unfairness of misrepresentation (negative or positive) of political actors’ characters and attributes 21
- Misappropriations and limits of consent in the use of a person’s image or likeness 21

Trust Challenges 22

- The liar’s dividend 22
- General distrust in media 23

Proposed Remedies and Associated Drawbacks 24

- Government regulatory challenges 24
 - Balancing the need for evidence and the need for timely rules before problems emerge 24
 - Balancing technology-focused and application-focused regulations 24
 - Harmonizing AI governance with existing laws and regulations, including on freedom of expression 25
- Tech company self-regulation, risk assessments, and ethical commitments 27
- Direct disclosure 28
- Indirect disclosure: provenance metadata, watermarking, and other forensic markers . 29

Conclusions and paths forward 30

Executive Summary

Following a global wave of prominent elections in 2024, several experts argued that the fears surrounding generative artificial intelligence (GenAI) in elections were overblown and that the evidence so far pointed to limited effectiveness of GenAI-driven efforts in swaying voters. But this early analysis of election data in the new artificial intelligence (AI) era should not justify letting down our guard, for two primary reasons. First, the volume and pervasiveness of synthetic content are likely to increase in the near future. Second, the misuse of GenAI in political communications can affect democratic processes in ways beyond influencing who wins an election.

This report provides an overview of recent GenAI applications in and around election campaigns and other forms of political communication around the globe, discusses factors likely to have an impact on their scale and success, and explores adverse ramifications for democracy. It also outlines key challenges in the strategies available to address these problems – from regulatory constraints to socio-technical solutions – and discusses initial implications and recommendations for election authorities and other decision-makers.

Definitions, Scope, and Methodology

GenAI refers to “a type of artificial intelligence that can learn from and mimic large amounts of data to create content such as text, images, music, videos, code, and more, based on inputs or prompts.”¹ Such AI-generated content is often referred to as **synthetic media**.

Although AI can be used for a number of purposes in election processes and operations, this report focuses largely on the uses of synthetic media in **political communication** generally and in **election campaigns** specifically. While political communication is broadly defined as “an interactive process concerning the transmission of information among politicians, the news media, and the public,”² most examples shared in this report concern the election campaign period – the time before an election during which political parties and candidates try to persuade voters and secure votes. Other political communication efforts discussed here might not be directly associated with elections but still aim to shape how stakeholders perceive political actors or their policies.

The typology and considerations offered in this report aim to facilitate the visualization of examples detected so far and to point out challenges and opportunities for the development or enhancement of legislation, regulatory mechanisms, and other socio-technical solutions to prevent or sanction abuse and hold different actors accountable. The report is based largely on extensive desk research covering academic, technical, and practitioner literature; analysis of news media; and some initial engagements with election authorities to understand their approaches and challenges in addressing the GenAI issue.

¹ Harvard University. (n.d.). Generative Artificial Intelligence (AI). <https://www.huit.harvard.edu/ai>

² Norris, P. In Smelser, N. J., & Baltes, P. B. (2001). International encyclopedia of the social and behavioural sciences. *Proceedings of US National Academy of Sciences*, 95(3), pp. 11631–11640. <https://www.sciencedirect.com/science/article/abs/pii/B0080430767043643?via%3Dihub>

Summary of Findings

1. Actors

 <p>Candidates & Parties</p> <p>Identifiable content produced directly by campaigns to benefit their own interests.</p>	 <p>Foreign Actors</p> <p>Malign influence operations targeting elections and information environments.</p>	 <p>Independent Groups</p> <p>Individuals, supporters, or anonymous entities with unknown affiliations.</p>
---	---	---


2. Purposes

 <p>Inform & Engage</p> <p>Leveling the playing field for smaller parties, engaging constituents at scale.</p>	 <p>Benefit Actors</p> <p>Enhancing appeal, relatability, and positive perception of candidates.</p>	 <p>Damage Reputation</p> <p>Attacking opponents through distortions, forgeries, and negative characterizations.</p>
 <p>Suppress & Manipulate</p> <p>Confusing voters about logistics or procedures to suppress turnout.</p>	 <p>Shape Narratives</p> <p>Astroturfing and flooding social media to create false impressions of public opinion.</p>	 <p>Undermine Trust</p> <p>Fabricating fraud to erode trust in election results, authorities, and institutions</p>

3. Applications

 <p>Imagery</p> <p>Positive: posters, depiction of desirable behavior. Negative: catastrophic scenarios, opponents in poor light</p>	 <p>Hyper-targeted Messaging</p> <p>Personalized messages based on individual data. Interactive avatars engaging with constituents</p>	 <p>Deepfakes</p> <p>Realistic video/audio of politicians doing/ saying things they didn't. Non-consensual intimate imagery.</p>
 <p>Fabricated Fraud</p> <p>Fake evidence of vote rigging or election interference. Doctored documents or news sites.</p>	 <p>Synthetic Personas</p> <p>AI-generated personas evading repression or justice.</p>	 <p>Chatbots</p> <p>Logistical election information. Guidance through political platforms.</p>

4. Challenges

 <p>Accountability</p> <ul style="list-style-type: none"> • Difficult tracing content to creators. • Dismissal of real evidence as fake. • Legal evasion via synthetic personas 	 <p>Ethics</p> <ul style="list-style-type: none"> • Unfair positive or negative misrepresentation. • Consent: Appropriating likeness of deceased figures. • Non-consensual use of private citizen data. 	 <p>Trust</p> <ul style="list-style-type: none"> • Erosion of faith in democratic systems. • Increased polarization. • Public retreating to less reliable information silos.
--	--	---

5. Remedies & Their Challenges

 <p>Gov Regulations</p> <p>Balancing the need for evidence-based policy with the speed of AI development. Ensuring regulations do not infringe on Free Speech or constitutional rights.</p>	 <p>Tech Self-Regulation</p> <p>Conflicts of interest when companies assess their own products. Lack of independent oversight in initiatives like the "AI Elections Accord." Potential "ethics washing."</p>	 <p>Direct Disclosure</p> <p>"Implied Authenticity Effect". Over-labeling causing user fatigue or numbness to warnings. Technical difficulties in enforcement across platforms.</p>
---	--	---

Introduction

Generative artificial intelligence (GenAI) is making it much easier to create sophisticated, deceptive content that is difficult to distinguish from reality, magnifying the scale and effectiveness of disinformation campaigns. Concerns arose as artificially generated content began to proliferate in online spaces, particularly about its potential impact on the information environment around elections. As an illustration of the level of concern, by the end of July 2024, about one quarter (151) of all bills introduced on artificial intelligence (AI) in state legislatures in the United States related to deepfakes and misleading media in political communications.³

Following a global wave of prominent elections in 2024, several experts argued that fears surrounding GenAI in elections were overblown and that evidence so far pointed to limited effectiveness of AI-driven efforts in swaying voters.⁴ But this early analysis of election data in the new AI era should not justify letting down our guard for two reasons: first, because the volume and pervasiveness of synthetic content are likely to increase in the near future; and second, because the misuse of GenAI in political communications can affect democratic processes in ways beyond influencing who wins an election.

As this report illustrates, in addition to enabling attacks against opponents with realistic but false content, GenAI technology is also helping political actors misrepresent themselves in a positive light to citizens, evade accountability for harmful or misleading content, and even misappropriate the likenesses of historical figures. Consequences of such applications can range from ill-informed voters to the normalization of radical ideologies. Given the novelty, complexity, and speed with which GenAI is being introduced into political communication, governments, election authorities, civil society, and even technology companies are struggling to limit its ill effects.

This report provides an overview of recent GenAI applications in and around election campaigns and other forms of political communication around the globe, discusses factors likely to have an impact on their scale and success, and explores adverse ramifications for democracy, including heightened election-related disinformation. It also outlines key challenges in the available strategies to address these problems – from regulatory constraints to socio-technical solutions – and discusses initial implications and recommendations for election authorities and other decision-makers.

³ Norden, L. Narang, L., & Protzmann, L. (2024, August 7). States Take the Lead in Regulating AI in Elections — Within Limits. *Brennan Center for Justice*. <https://www.brennancenter.org/our-work/research-reports/states-take-lead-regulating-ai-elections-within-limits>

⁴ See, e.g., Simon, F. M., & Altay, S. (2025). Don't panic (yet): Assessing the evidence and discourse around generative AI and elections. *Knight First Amendment Institute*. <https://knightcolumbia.org/content/dont-panic-yet-assessing-the-evidence-and-discourse-around-generative-ai-and-elections>

GenAI Applications in Election Campaigns and Other Political Communications: An Overview

A multitude of actors

One of the first observations that can be made about synthetic content portraying political actors during an election period is that it originates from several sources, both identifiable and anonymous. Some materials are clearly labeled and carry the approval of the candidate or political party they intend to benefit, but the origin of most synthetic content is difficult to pinpoint. The International Panel on the Information Environment has found that although 25 percent of GenAI content used globally in 2024 elections was produced by candidates or political parties, almost half of the content (46 percent) had no known source.⁵ There is also evidence that malign foreign actors are using synthetic content in their disinformation campaign efforts targeting elections⁶; these actors accounted for 20 percent of the synthetic election content produced in 2024, according to the same report. Finally, independent individuals and groups – driven by personal and political beliefs or by financial incentives – also engage in the production and dissemination of material.⁷

This multitude of actors, coupled with the legal, technical, and operational challenges in ascertaining authorship or ownership of online content (discussed in later sections), can make it harder to ensure accountability for harmful content.

A multitude of purposes

Double-edged swords

GenAI use in political communication can serve democratic principles as much as it can harm them. For instance, GenAI can help level the playing field, reducing the costs of high-quality media production and helping smaller parties and candidates increase the appeal of their campaign materials. This could promote pluralism by increasing their competitiveness against larger and better-resourced parties that can afford sophisticated media teams.

In other cases, synthetic media can cause direct harm. Partnership on AI, a multistakeholder collaboration aiming to harness AI for positive impact, notes that one of these potential threats is

[m]anipulating democratic and political processes, including deceiving a voter into voting for or against a candidate, damaging a candidate's reputation

⁵ *Generative AI in Electoral Campaigns: Mapping Global Patterns*. (2025). International Panel on the Information Environment. <https://www.ipie.info/research/sfp2025-1>

⁶ See, e.g., Osadchuk, R. and Acarvin, A. (2024). *Doppelganger: How Russia mimicked real news sites and created fake ones to target US audiences*. <https://dfrlab.org/2024/09/18/doppelganger-us-election/>

⁷ Spring, M. (2024). *How X users earn thousands from US election misinformation and AI images*, BBC News. <https://www.bbc.com/news/articles/cx2dpj485nno>.

by providing false statements or acts, influencing the outcome of an election via deception, or suppressing voters.⁸

The recent examples described below illustrate some of these uses, although the list is not exhaustive and the categorizations are not always clear-cut; such content often has several or overlapping goals that are not always explicit to media consumers.

Promoting or benefiting particular political actors

Whether commissioned or approved by candidates or developed independently by supporters without candidates' consent, synthetic media is often used to benefit particular actors. Content may try, for instance, to enhance candidates' physical attributes or appearance; increase their perceived appeal, friendliness, relatability, or trustworthiness; elevate their character; or simply extend their ability to reach broader audiences. Under this rubric, synthetic content might focus on positive imagery, hyper-targeted messaging or deepfakes.

Positive imagery: Synthetic content has been used in campaign material, social media posts, and even traditional media to directly promote specific candidates or parties and their ideas. Examples range from creative posters that mimic specific artistic styles to more realistic images that show political actors engaging in behavior that would ostensibly be seen as desirable by potential voters and supporters (see examples below). Positive representations, particularly realistic ones, could convince voters that certain candidates have attributes, skills, or experiences they do not, in fact, have.

In **Argentina (2023)**, candidate Sergio Massa made extensive use of AI-generated posters to bolster his campaign. The material was shared through Massa's official social media accounts.



In the **United States (2024)**, a synthetic image that circulated on social media without an explicit source showed then-candidate Donald Trump walking through floodwaters after Hurricane Helene.



Hyper-targeted messaging and avatars: Going beyond microtargeting that relies on demographics or social media activity, AI facilitates hyper-targeted messages personalized at the individual level, integrating high volumes of data from different sources and making predictions about the messages that are more likely to resonate with each user. The content can be tailored to individual voters' needs and interests and give the impression that

⁸ PAI's *Responsible Practices for Synthetic Media*. (2025, March 19). Partnership on AI: Synthetic Media. https://syntheticmedia.partnershiponai.org/#read_the_framework

candidates are truly responsive. Some officials and candidates have also been using AI to “talk” directly to constituents through interactive avatars of themselves, which may further enhance the sense that personal relationships are being built. Depending on how they are programmed, AI impersonation outputs may or may not be constrained to the political actor’s real positions on different issues, and the tools might become more focused on captivating the voter than on faithfully conveying candidates’ ideas. In addition to these more political concerns, hyper-targeted messaging also raises ethical and legal questions around data privacy and user consent.⁹

Deepfakes to overcome outreach challenges and increase inclusion:

Some candidates and parties have used synthetic content to overcome practical constraints and expand voter outreach. For instance, AI-powered software enables political actors to translate speeches and other political content into local languages in real time. Text-to-speech conversion tools are increasingly natural sounding,¹⁰ which can help people with low literacy or visual impairments access policy platforms and other written content. But

although text-to-speech conversion technology can promote inclusivity in political communication, it can become problematic if cloned voices and deepfakes are used without the consent of implicated individuals (as discussed in later sections) or if they convince audiences that the depicted political actors have a level of familiarity with their languages, cultures, or personal situations that they do not really have.

In **South Korea (2022)**, an AI-generated avatar of candidate Yoon Suk-yeol was employed to mimic his speech and behavior while offering more targeted engagement with voters, responding to users’ questions. The avatar was created and deployed by Yoon Suk-yeol’s campaign team.



In **India (2024)**, President Narendra Modi’s campaign used AI to interact with voters through WhatsApp, greeting them by their names and in their languages.



⁹ Watson, N. (2024, October 15). Protecting Voter Data Privacy in the Age of AI. *Corporate Compliance Insights*. <https://www.corporatecomplianceinsights.com/protecting-voter-data-privacy-in-the-age-of-ai/>

¹⁰ See, e.g., Microsoft’s VibeVoice tool: <https://microsoft.github.io/VibeVoice/>

Deepfakes to overcome political restrictions and repression: GenAI may also help individuals overcome political restrictions and repression. The ease of creating and manipulating videos with AI enabled former Pakistani Prime Minister Imran Khan, for instance, to campaign from prison. GenAI also enabled the opposition movement in Belarus to create a completely artificial “candidate” to help disseminate its ideas while shielding real opposition figures from Alexander Lukashenka’s repression. While these applications may serve democratic goals when they empower individuals who were unjustly incarcerated or are being politically persecuted, they can also undermine legitimate sanctions and sustain visibility of those who have received reasonable due process. Moreover, AI-generated “candidates” could be used to advance unlawful or extremist ideologies and promote hate speech while enabling the real people behind them to evade responsibility.

In **Pakistan (2024)**, former Prime Minister Imran Khan used a deepfake of himself to campaign for his party (PTI) and mobilize voters while he was still in prison.



In **Belarus (2024)**, amid intense repression by the Lukashenka regime, the opposition developed Yas Gaspadar, an AI-generated candidate, to interact with Belarusians and spread opposition ideas while protecting real opposition leaders from retaliation.



Damaging the reputation or electability of particular political actors

The use of synthetic media to damage the reputation of certain candidates or parties can be directed by political opponents, opponents’ supporters, and even malign actors trying to sway results or inflame the electorate. Synthetic media employed for this purpose may use some of the same tactics described above in addition to distortions or complete forgeries of candidates’ actions or speeches, generating false “evidence” of wrongdoing, and inciting suspicion, disapproval, or hatred. Under this rubric, synthetic content might focus on negative imagery, hyper-targeted messaging and deepfakes.

Negative imagery: Synthetic content has been used for campaign posters and social media outreach to degrade specific candidates or parties and their ideas, particularly by portraying what some would see as catastrophic scenarios in the event of their ascension to power.

During the **European Union Parliamentary Elections (2024)**, anti-EU parties and coalitions such as the Italian Lega party and France's Identity and Democracy (ID) Coalition deployed a series of AI-generated imagery portraying what they see as unwanted values advanced by the EU. The images were almost always unlabeled, in violation of a code of conduct the parties signed ahead of the elections.



Hyper-targeted messaging: As with positive campaigning, hyper-targeted messaging can leverage a wealth of personal data to tailor messages to individual voters, aiming to turn them against specific actors. Algorithms can be used to identify issues that citizens feel strongly about and increase the salience of dissonant ideas held by opponents to which users are exposed.

Deepfakes for reputational damage: In a step beyond negative depictions of political actors and their ideas, doctored videos, audio recordings, and text can be used to damage reputations or electoral chances, mainly by convincing media consumers that politicians have expressed or done things they have not. As Partnership on AI notes, down-ballot candidates and female politicians are targeted more frequently by this malicious use of synthetic content. “Deepnudes” and other nonconsensual intimate imagery not only harm their political aspirations, but also have a chilling effect on other women who are considering entering politics.¹¹ While more reputable GenAI platforms have policies against such content, some open-source companies have been used to develop synthetic pornographic content by exploiting real images of people, scraped without consent, and little has been done to stop the practice.¹²

¹¹ Khan, T. (2025, March 11). *Protecting Global Democracy in the Digital Age: Insights from PAI’s Community of Practice – Partnership on AI*. Partnership on AI. <https://partnershiponai.org/protecting-global-democracy-in-the-digital-age-insights-from-pais-community-of-practice/>

¹² Maiberg, E. (2023, October 19). *Inside the AI Porn Marketplace Where Everything and Everyone Is for Sale*. 404 Media. <https://www.404media.co/inside-the-ai-porn-marketplace-where-everything-and-everyone-is-for-sale/>

During regional elections in **Colombia (2023)**, candidate Alejandro Eder, running for mayor of Cali, was portrayed in a likely artificially generated audio supposedly discussing a “peace pilot” that involved dialogue with the guerrilla group National Liberation Army (*Ejército de Liberación Nacional*, or ELN).

Just weeks before the Legislative Assembly election in **Northern Ireland (2022)**, a deepfake video portrayed candidate Cara Hunter partaking in pornographic activities. The video was shared thousands of times, mainly through WhatsApp. As of January 2025, the police had not yet identified its creator.

In **Turkey (2023)**, President Recep Erdoğan shared a deepfake video depicting a member of the Kurdistan Workers’ Party (PKK) – a Turkish political militant group that the EU and several countries have designated as a terrorist organization – supporting presidential candidate Kemal Kılıçdaroğlu.

Deepfakes for misleading guidance: In addition to portraying politicians engaging in supposedly undesirable behavior to damage their reputations, synthetic content may also portray them providing supporters with advice or instructions that go against their electoral or political goals. For instance, voters might be exposed to deepfake audio or video in which their preferred candidates tell them they have withdrawn from the race or that voters should not turn out to vote.

On the eve of municipal elections in **Argentina (2025)**, an AI-generated video of opposition leader Mauricio Macri circulated on the internet. Macri was depicted saying the candidate he had endorsed was dropping out and, even though she would still be on the ballot, everybody should vote for President Milei’s candidate. Article 64 of Argentina’s Electoral Code prohibits any campaigning in the 48 hours preceding the election, hindering Macri’s response. Milei supported the content as “freedom of expression.”



In the **United States (2024)**, an AI-generated robocall impersonating then-President Joe Biden told voters not to vote in the primaries to “save their votes for the general elections.” Without the more visible flaws often noticed in deepfake videos (audio and image synchronization, unnatural movements), the veracity of audio recordings can be even harder to verify.

Just a few days before the presidential elections in **Ireland (2025)**, then-candidate Catherine Connolly was portrayed in a deepfake video in which she appeared to announce her withdrawal from the contest. Connolly filed a formal complaint with the Election Commission.



Suppressing voters or otherwise manipulating voting patterns to affect results

Synthetic media can also be used to target and confuse voters – for instance, about registration requirements, dates for registration and voting, or electoral procedures and options at the polls, suppressing votes or manipulating voting patterns. Unintentional confusion and misinformation may also result if GenAI-powered tools deliver flawed outputs. Under this rubric, synthetic content might focus on doctored information and flawed chatbots.

Doctored official documents, websites, news media headlines: By forging official communication channels, malicious actors may effectively disinform and lead voters to miss deadlines, go to the wrong registration or polling sites, or unintentionally invalidate their votes. If carried out in a targeted manner – such as in a candidate’s stronghold or among sectors of the population statistically more likely to vote for certain parties – these tactics can affect election results. Ahead of the 2024 elections in the United States, AI-generated websites mimicked official voter registration pages, collecting private data and leading people to believe they were registered when they were not, in fact, included in voter lists.¹³

Chatbots: Voter suppression and confusion might also occur unintentionally, as AI-powered chatbots can provide inaccurate outputs on election information. In early 2024, for instance, Democracy Reporting International noted that chatbots by Google, Microsoft, and OpenAI all shared inaccurate information about the European elections, including polling dates and how to cast a ballot.¹⁴

Undermining trust in results, election authorities, and democratic systems

Mixing features described above, some GenAI applications focus on distorting reality or forging “evidence” to undermine trust in the election process and results. Content could suggest significant fraud, instigate fear, and sow distrust in the process, fueling political apathy and disengagement or mobilizing people to fight against those they perceive to have wronged them.

Fabricating politician-led fraud: Some synthetic materials have featured politicians supposedly planning to commit electoral fraud or interference through, for instance, vote-buying or collusion with election officials. These have taken the shape of artificially generated videos or audio, supposedly recorded surreptitiously and then shared publicly to “unmask” portrayed politicians. In Slovakia, for instance, fake audio recordings in 2024 portrayed the West-friendly candidate

In **Nigeria (2023)**, AI-generated audio depicted candidate Atiku Abubakar and supporters discussing ways to work with the Election Commission to rig the elections. The Nigerian Centre for Democracy and Development’s Election War Room investigated the file and concluded that the audio was fake.

Meet Lydia (persian_queen) ✨
@LydiaTeeanalaja · Follow
Listen to how Atiku, Okowa and Tambuwal are planning to rig the 2023 presidential election tomorrow 🤪🤪🤪
May PDP never happen to us 🙏



5:02 AM · Feb 24, 2023

104 Reply Copy link

Read 23 replies

¹³ Knowles, J. Pistone, A. (2024, October 14). AI deepfakes, voting misinformation, fake fundraisers and other 2024 election scams ramp up. *ABC 7*. <https://abc7chicago.com/post/ai-deepfakes-voting-misinformation-fake-fundraisers-other-2024-election-scams-ramp-day-nears/15429430/>

¹⁴ Goujard, C. (2024, April 15). AI chatbots spread falsehoods about the EU election, report finds. *POLITICO*. <https://www.politico.eu/article/ai-chatbots-spread-falsehoods-about-the-eu-elections-report-finds/>

Michal Šimečka boasting about rigging the election by buying votes from Roma people and saying he would increase the price of beer. Although some AI detection tools are being used to assess the authenticity of such content, these tools are still largely unreliable, further complicating efforts to firmly debunk false and malicious content.

Fabricating fraud by election officials and other stakeholders: Other efforts to manufacture election fraud have targeted election officials, portraying them as driving or enabling interference. In other cases, civil society watchdogs, observers, and activists have been targeted. In the Philippines in 2025, for instance, synthetic content depicted progressive candidates, civil society watchdogs, and election monitors as associated with communist insurgents, enhancing “red-tagging” tactics often used in the country to instigate violence.

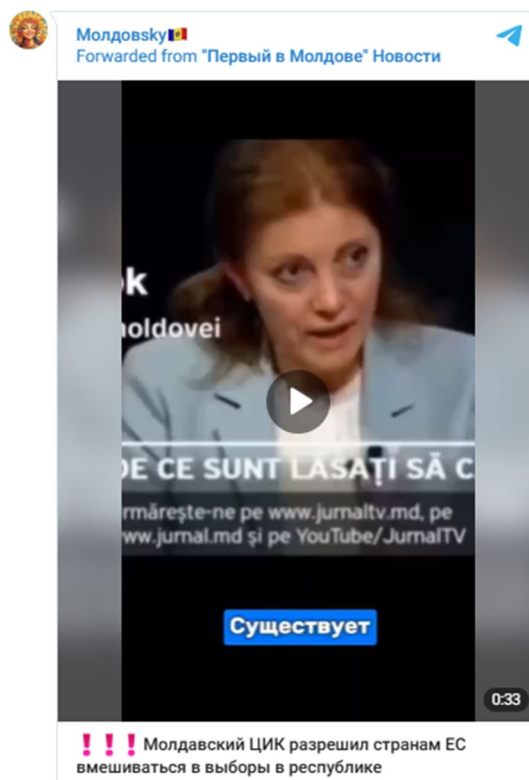
These types of efforts could instigate threats and violence against officials and civil society actors; such fabrications also undermine trust in the long term, portraying electoral institutions and authorities as untrustworthy orchestrators of fraud.

Manipulating public narratives

AI can be used to manipulate social and political narratives by imitating reputable news media outlets, tilting survey results with automated respondents, and flooding social media accounts with comments to create the impression that a larger sector of the population shares certain views – a practice known as *astroturfing*. These campaigns often aim to drown out dissenting voices and fracture solidarity among protesters. Concerningly, a recent study showed that people not only struggle to distinguish social media posts created by real users from those created by ChatGPT, but also find disinformation content created by AI to be more compelling.¹⁵

Synthetic personas and manufactured public comments: AI is being used to generate messages and automate publishing in coordinated ways through social media posts,

In **Moldova (2025)**, a deepfake portrayed the head of the Central Election Commission, Angelica Karaman, claiming that the EU had received official permission to interfere in the country’s elections. Russian Foreign Ministry spokeswoman Maria Zakharova further disseminated the video in her Telegram channel.



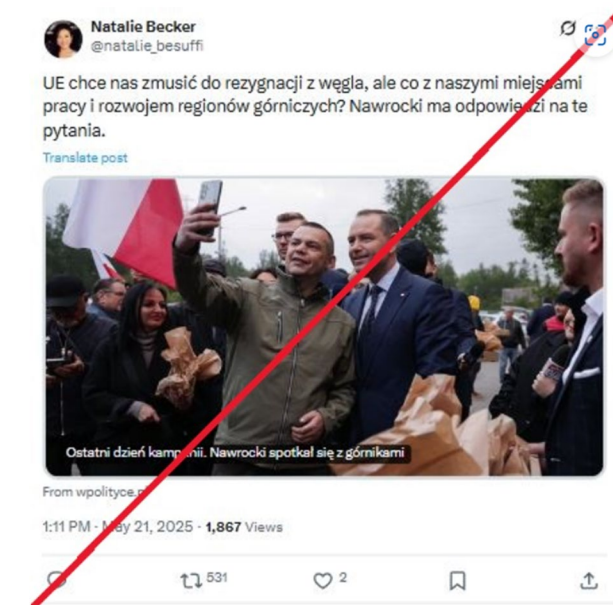
¹⁵ Spitale, G., Biller-Andorno, N., & Germani, F. (2023). AI model GPT-3 (dis)informs us better than humans. *Science Advances*, 9(26). <https://www.science.org/doi/10.1126/sciadv.adh1850>

comments on news articles and online forums. Real users exposed to these messages might believe that peers share an opinion, potentially influencing their own perceptions of an issue. In the Philippines in 2025, for instance, a likely AI-powered network of fake social media accounts proliferated to defend former President Rodrigo Duterte after he was sent to the International Criminal Court on charges of crimes against humanity. The fake accounts aimed to create the illusion that Duterte had overwhelming public support and shape the political debate just before the country's midterm elections in May 2025.

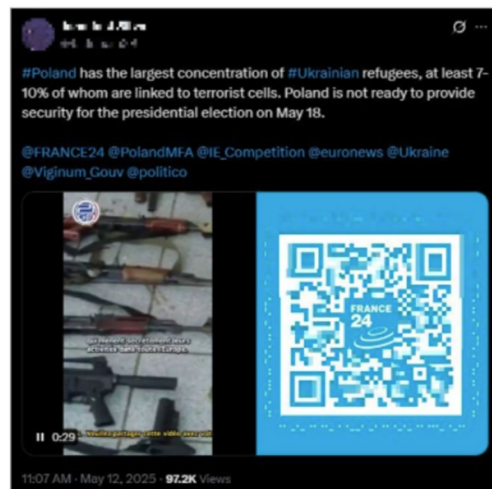
Doctored reputable news outlets:

Certain media outlets are largely trusted by consumers to provide credible information. Malicious actors have leveraged this trust and co-opted these outlets' logos, website layouts, or social media accounts to spread false or misleading information disguised as coming from trusted sources (e.g., Russia-aligned social media posts in Poland). Some synthetic content disseminated this way has aimed to instigate fear or hatred toward individuals or groups and to shape political views ahead of polls.

In **Poland (2025)**, Russia's Doppelganger operation used AI-generated personas and fake accounts to simulate Polish citizens posting opinions that aligned with Russian interests. Many synthetic users displayed "concerns" about Poland's military spending, criticized the EU or directly supported pro-Russian presidential candidate Karol Nawrocki.



In **Poland (2025)**, social media posts with headlines purporting to be from reputable international news media, such as *France 24* and *Deutsche Welle*, accused Ukrainians in Poland of planning terrorist attacks ahead of the 2025 presidential elections. The fake QR codes did not redirect users to news articles.



Potential Factors Related to the Impact and Effectiveness of Synthetic Content in Elections

Some experts have argued that GenAI has not – at least not yet – been as impactful in affecting election results as initial projections suggested. While this might be true, the illustrations presented in the previous section show that GenAI has already been used in ways that distort reality and potentially abuse people’s private data, personal values, and biases to advance political goals. As these applications proliferate, especially if no strategies are implemented to contain their misuse, it will become increasingly hard to measure their real impact on voters’ attitudes and election results. Acknowledging this intrinsic challenge, this section presents potential factors affecting the impact of artificially generated content, based on the limited data collected for this report.

It is also important to mention that the impact of synthetic content in election campaigns might be defined in ways broader than merely swaying voters’ immediate choices. By gaining attention and reaching larger audiences, synthetic content could shape debates, mobilize apathetic citizens and change perceptions across time in ways that are difficult to measure. And although this can also be said of authentic content or non-AI-driven disinformation, synthetic content has the advantage of being potentially more realistic and targeted.

Impact versus Effectiveness

Synthetic content can be *impactful* – having a significant effect on its audience – without being *effective* – meaning, achieving the creator’s or disseminator’s intended effect and goals. In fact, synthetic content can be impactful in a way that undermines the creator’s goals, as was the case with South African Democratic Alliance’s political advertising ahead of the 2024 national elections. The ad, which intended to criticize the ruling African National Congress party, backfired on the Democratic Alliance in the

In **South Africa (2024)**, the Democratic Alliance (the main opposition party) ran an AI-generated campaign video showing the country’s flag burning. The party claimed it was a symbolic depiction of what would happen if the country remained under the leadership of the ruling African National Congress. The ad garnered significant attention, but mostly negative toward Democratic Alliance, as many South Africans were outraged by seeing the flag in flames. The Democratic Alliance did not label the video as generated by AI, which, as argued by Code for Africa (a network of civic technology and data journalism organizations), could have minimized public outrage.



face of public outrage about the desacralization of the national flag.¹⁶

Content quality

As the examples throughout this report help illustrate, synthetic content used in political campaigns has varied significantly in quality, complexity, and realism. Many AI-generated videos show clear signs indicating they are not real (e.g., unnatural movements, lack of fluidity in speech). In this sense, such deepfakes are not too different from “cheapfakes” or “shallowfakes” – media manipulated with basic, non-AI editing tools. Although these videos can still garner attention and help convey a message, their ability to deceive might be reduced as voters can more easily detect that they are not real. As AI platforms become more sophisticated and users become more proficient in their use, the general quality of synthetic content is expected to increase, potentially increasing its effectiveness.

Media environment: trust in media and prevalence of editorial media versus social media for news consumption

In a 2025 report, an expert group on AI and elections appointed by the government of Norway pointed out that levels of citizen trust in traditional, editor-controlled media can lessen the impact of synthetic media. Citing data from the Norwegian Media Authority, the report notes that 73 percent of Norway’s population had fairly high or very high trust in Norwegian news media in general. Eight out of 10 Norwegians used editorial media such as newspapers (print and online) as a source of news.¹⁷ These patterns could help limit exposure to unlabeled, deceptive synthetic content, as news media outlets would have more resources to detect, verify, or filter potentially artificial content or to clearly inform their audiences of the content’s nature.

In the United States, on the other hand, Pew Research data suggest that trust in traditional news media is declining while trust in social media sites is increasing, and that these trends are particularly acute among Republicans. In 2024, Republicans trusted social media almost as much as they did national news media outlets. Interestingly, although also in decline, Republicans’ trust in local news media remains relatively high,¹⁸ which indicates that these outlets might be a more promising vehicle to debunk pernicious synthetic media gaining traction elsewhere.

¹⁶ How an AI-manipulated video caused harm during South African elections: An analysis by digital democracy nonprofit Code for Africa (2025, March 19). *Partnership on AI*.

<https://partnershiponai.org/codeforafrica-framework-case-study/>

¹⁷ Artificial Intelligence and Democratic Elections – International Experiences and National Recommendations Report by the Expert Group on Artificial Intelligence and Elections. (2025) *Norway Government*. <https://www.regjeringen.no/en/dokumenter/artificial-intelligence-and-democratic-elections-international-experiences-and-national-recommendations-report-by-the-expert-group-on-artificial-intelligence-and-elections/id3086085/>

¹⁸ Eddy, K. Shearer, E. (2025, October 29). How Americans’ trust in information from news organizations and social media sites has changed over time. *Pew Research Center*. <https://www.pewresearch.org/short-reads/2025/10/29/how-americans-trust-in-information-from-news-organizations-and-social-media-sites-has-changed-over-time/>

Trust in and reliance on reputable news media – assuming these organizations are, indeed, capable of and engaged in filtering or disclosing artificial content as such – can thus be an indicator of the level of exposure and vulnerability to potential deception by synthetic media.

Citizens’ media literacy and resilience against disinformation

Citizens are ultimately the main target of political campaigns – the audience whose attitudes and behaviors campaigners mean to influence. If citizens were perfectly equipped with the knowledge and skills to discern synthetic from authentic content – and, moreover, the extent to which its artificial manipulation affects content’s trustworthiness – then almost all other concerns would become obsolete. This is, of course, not the case. Moreover, the novelty of synthetic content means that different groups’ level of familiarity and expertise varies significantly, and it can be assumed that large demographics will remain vulnerable to GenAI deception, as they are to disinformation more generally.

Media literacy levels in a society more broadly could still help estimate the reach of deceptive synthetic content in political campaigning, as media-literate individuals are expected to be less likely to engage with the content – not being deceived by it or spreading it further. A flaw in this logic is that people do not share only content they believe to be true. Recent studies by Google’s incubator Jigsaw have suggested that knowing a piece of media is artificially generated is not enough to prevent consumers from sharing it.¹⁹ Individual media literacy might thus not be enough to address the spread of harmful synthetic content. Citizens must also consider the potential impact of certain media on others, even if they are not deceived themselves.

Accountability Challenges

As NDI’s *Guide to Monitoring Generative AI in Elections for Nonpartisan Citizen Observers*²⁰ explains, GenAI can interfere with several rights enshrined in international and regional instruments. These include the right to seek and receive information in order to make an informed choice on election day, the right to a level playing field, and the right to free expression. GenAI’s nature, however, makes it difficult to hold actors using GenAI accountable for breaching or undermining these rights.

Establishing the responsibility burden: builders, creators, and disseminators

One of the most obvious challenges in establishing effective and enforceable regulations on synthetic media use in political campaigns is the difficulty in tracing the content to responsible actors and establishing effective accountability mechanisms.

¹⁹ Jigsaw. (2021, August 31). The effect of warning labels on the perceptions of manipulated media. *Medium*. <https://medium.com/jigsaw/the-effect-of-warning-labels-on-the-perceptions-of-manipulated-media-c1de5ceb83e9>

²⁰ Synthetic Voices, Real Users: A Guide to Monitoring Generative AI in Elections for Nonpartisan Citizen Observers (2025). *National Democratic Institute*. <https://ndi.org/publications/synthetic-voices-real-voters-guide-monitoring-generative-ai-elections-nonpartisan>

Partnership on AI identifies three types of actors involved in the life cycle of synthetic media – *builders* (of the AI tools), *creators* (AI-tool users who create content), and *distributors* (social media and other outlets that spread the content) – all of which can contribute to a more ethical use of synthetic media. For instance, builders can embed disclosure mechanisms (either direct, as in visible labels and watermarking, or indirect, as in adding cryptographic provenance information to the file metadata that makes manipulation detectable). Creators can be transparent, disclosing any media manipulation and seeking the consent of those they portray in their content. Distributors can also play their part, for instance by making efforts to detect when third-party content is synthetic, disclose any manipulation, avoid distributing unattributed synthetic content, and be clear about their policy on publishing synthetic media.²¹

Unsurprisingly, this ethical guidance has limited practical effect, particularly when it is in the interest of builders, creators, and/or disseminators to *not* be transparent. For instance, builders might prioritize attracting more users interested in creating hard-to-detect deceptive content, creators might actually want to deceive, and disseminators might either want to avoid the costs of investing in safeguards or even welcome the traffic that synthetic media can bring to their platforms.

Identifying who is ultimately responsible for harmful content and establishing appropriate and proportionate sanctions and remedies in this intricate chain are still challenging tasks. Laws and other regulatory mechanisms in certain countries are evolving to mitigate this issue, and some reputable GenAI platforms have incorporated restrictions into their policies (e.g., prohibitions against impersonating candidates, using tools for campaigning, and misrepresenting the voting process).²² However, the proliferation of open-source AI platforms that do not impose strict content policies hinders regulators' and investigators' capacity to attribute responsibility for synthetic content.

In the context of political campaigns or messaging that affect voters' perceptions and behaviors, it is also important to understand the roles and responsibilities of candidates, political parties, and independent individuals with political goals – as well as those of AI developers, social media platforms, and traditional media – in the creation and dissemination of synthetic political content. Regulations, remedies, and sanctions must be tailored to these roles and responsibilities.

Determining consent of implicated actors

Related to the responsibility burden, it is practically very challenging to establish whether there was consent – and thus also responsibility – of the actors implicated in synthetic content creation and/or dissemination.

²¹ PAI's *Responsible Practices for Synthetic Media*. (2025b, March 19). Partnership on AI - Synthetic Media. https://syntheticmedia.partnershiponai.org/#read_the_framework

²² Democracy in the Age of Generative AI: Navigating Risks and Harnessing Opportunities (2024). *International Republican Institute*. <https://www.iri.org/wp-content/uploads/2024/08/GenAI-Democracy-White-Paper-Final.pdf>

Consensual use refers to instances of GenAI application that are driven or approved by the political actors they implicate and are often meant to benefit or add value to their campaigns. Non-consensual applications are those in which the implicated actors did not request or accept the use of their image, voice, or other personal identifiers, and are usually meant to damage a candidate's reputation or electability. It is also common, however, for supporters to engage in the creation or dissemination of synthetic media to promote or give an advantage to political actors without their direct consent.

Political actors' inability to completely control whether their images and likenesses are used – positively or negatively – and their ability to deny knowledge and/or responsibility for synthetic content that benefits them or harms opponents represent a serious accountability challenge.

Establishing deception intent

The capacity to determine synthetic media creators' or disseminators' intent to deceive (versus simply conveying a message in creative or satirical ways) is yet another obstacle. As the examples in the previous section show, some GenAI content is explicitly artificial, created in artistic or unrealistic formats. While this content conveys a message or intends to evoke certain feelings and perceptions in the audience, it might not be generally intended to deceive viewers into believing the content is real.

On the other hand, synthetic content that reproduces and distorts real images, text, audio, or video in realistic ways, without any disclosure or label to indicate it was generated by AI, can be understood to be intended to deceive. Based on this distinction, YouTube, for example, requires content creators to disclose manipulation only when they upload “meaningfully altered or synthetically generated content that seems realistic.”²³ This requirement exempts from disclosure manipulation

such as beauty filters and AI-generated animation and content deemed “not realistic,” such as someone riding a unicorn or floating in space. Since July 2024, Google Ads has also

In **Argentina (2023)**, candidate Sergio Massa used synthetic media to degrade or criticize his main opponent, Javier Milei. Most material, as in the example below, was not intended to be realistic; it also featured a link – albeit in very small type – to Massa's Instagram page of AI-generated campaign material.



²³ *Disclosing use of altered or synthetic content - Android - YouTube Help.* (n.d.).
<https://support.google.com/youtube/answer/14328491>

required certified election advertisers to disclose when ads “contain synthetic or digitally altered content that inauthentically depicts real or realistic-looking people or events.”²⁴

Intent to deceive, however, is not always easy or objective to determine. What some media creators might say is not realistic – and thus not intended to deceive – can still, in practice, deceive some media consumers.

Preventing accountability evasion through AI personas

As the case of the Belarusian AI-generated “candidate”²⁵ shows, AI can serve democratic principles by helping activists circumvent censorship and repression and recover, to an extent, their right to free speech. In authoritarian environments where traditional opposition movements are banned, exiled, or silenced, synthetic avatars and AI-generated spokespeople can maintain communication channels that help political figures who believe their prison sentences and other sanctions are driven by political persecution to continue expressing their views and cultivating supporters. These tools can also be used to sustain morale in political movements, maintain a visible presence in public discourse, and counter official narratives that opposition groups have been irreversibly defeated.

But the same tools that help circumvent repression can also undermine accountability. In a country with strong legislation

In **France (2024)**, ahead of the EU parliamentary elections, fake accounts pretending to be members of the Le Pen family gained attention on TikTok. “Amandine Le Pen” – a deepfake young “niece” of far-right leader Marine Le Pen – posted about her life, often with ambiguous or double-entendre statements that poked fun at immigrants and people of color. In the video screenshot below, “Amandine” says there is “nothing better than waking up to see that everything is snow white.” Le Pen’s party, National Rally (Rassemblement National, or RN), condemned the “malicious” use of AI and advocated for regulations, but the party also opposed an umbrella digital bill the country passed, claiming it was an authoritarian measure.



²⁴ Update to our policy on Disclosure requirements for synthetic content (July 2024) - Advertising Policies Help. (n.d.). <https://support.google.com/adspolicy/answer/15142358>

²⁵ The Belarusian opposition movement clarified it had no intention of formally nominating Yas Gaspadar as a candidate.

and enforcement mechanisms to prevent the spread of discriminatory narratives, for example, political actors might hide behind an AI candidate to disseminate racist, sexist, or xenophobic ideas without facing the law. The fact that it is not always feasible or easy to identify who is ultimately behind the content further enables bypassing accountability, as illustrated by the example from France (see text box).

Ethical Challenges

Unfairness of misrepresentation (negative or positive) of political actors' characters and attributes

As some of the examples in this report illustrate, synthetic content that misrepresents political actors' personalities, beliefs, attitudes, or behavior to deceive voters into thinking they are less worthy poses a clear problem to the fairness of election campaigns. By the time false or misleading content is exposed as such, the damage is often already done, and implicated candidates might have lost support based on unwarranted reactions from voters. Recent research has shown that disinformation not only can lead to poor judgment and decision-making but also has a lingering effect and influence on people's reasoning – even after it has been debunked.²⁶

While it is easier to pinpoint the unfairness of synthetic media that misrepresent political actors in a negative way, it is worth noting that AI-generated content employed to paint them in a positive light can be just as detrimental to voters' clear judgment. For instance, as discussed above, targeted messaging could convince voters that candidates espouse their exact ideas and beliefs, and deepfakes might convince voters that candidates speak their language or have other abilities and experiences that they do not really have. And although one might argue that lies have always been an integral part of political campaigns, it is clear that GenAI has made these lies more powerful – both in their volume and in their level of realism. As AI-enabled misrepresentation becomes a key component of political campaigns, elections might be won not by candidates whose genuine ideas resonate with the most people, but by those who can resonate with the most people by manipulating their beliefs and values.

Misappropriations and limits of consent in the use of a person's image or likeness

As discussed above, establishing whether a political actor was aware of or approved certain synthetic content is already challenging, but there is more to the issue of consent than just legal responsibility. Examples such as the case of Indonesia, where the late President Suharto's image has been used in AI-generated videos, raise another set of relevant questions, such as whether it is ethical to "resurrect" deceased figures for partisan purposes without explicit consent and whether there should be limits on the ability to attribute content to a deceased individual whose likeness is being used.

²⁶ Ecker, U. K., Lewandowsky, S., Cook, J., Schmid, P., Fazio, L. K., Brashier, N., ... & Amazeen, M. A. (2022). The psychological drivers of misinformation belief and its resistance to correction. *Nature Reviews Psychology*, 1(1), 13–29.

These questions are increasingly relevant in the U.S. media and entertainment industry, where AI-generated replicas or new products that use deceased celebrities' content can generate significant revenue. In California, a new law took effect in January 2025, expanding existing post-mortem rights related to AI-generated digital replicas.²⁷ In 2024, the state of Tennessee also passed legislation to protect the rights of musicians and other artists, including deceased artists, from AI.²⁸ In both states, consent and authorization to use a deceased person's likeness must be given by the person's estate.

In **Indonesia (2024)**, AI-generated videos of late President Suharto (who died in 2008) were used to boost his party's (Golkar) campaign.



When used for political purposes, synthetic content featuring deceased historical figures can be even more ethically controversial and facilitate attempts to reinterpret and manipulate historical facts. Decision-makers and electoral authorities may need to analyze legislation on post-mortem rights in other sectors to inform solutions to this GenAI application in political communication.

Trust Challenges

The liar's dividend

Even if GenAI-powered efforts do not have an immediate and significant effect on election results, they can still change how people interact with and perceive information. The “liar's dividend” is a term coined by Chesney and Citron²⁹ to explain the phenomenon in which people may dodge responsibility and accountability for things they have said or done by claiming that genuine video, audio, or textual evidence is fake or manipulated. Because the public is now aware that manipulated media is common, they might be primed to doubt even authentic content. An iconic example of this phenomenon is provided by U.S. President Donald Trump, caught in an *Access Hollywood* tape making vulgar comments about women.

²⁷California expands its Post-Mortem right of publicity law to cover AI digital replicas | Cowan, DeBaets, Abrahams & Sheppard LLP. (n.d.). Cowan, DeBaets, Abrahams & Sheppard LLP. <https://cdas.com/california-expands-its-post-mortem-right-of-publicity-law-to-cover-ai-digital-replicas/>

²⁸ Rosman, R. (2024, March 22). Tennessee becomes the first state to protect musicians and other artists against AI. *NPR*. <https://www.npr.org/2024/03/22/1240114159/tennessee-protect-musicians-artists-ai>

²⁹ Chesney, B. Citron, D. (2019). *Deep fakes: a looming challenge for privacy, democracy, and national security* — *California Law review*. California Law Review. <https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security>

Trump initially acknowledged the recording was authentic but later suggested that the voice was not actually his and even suggested that he wanted to investigate the recording.³⁰

The liar’s dividend is an important consideration when designing interventions focused on citizens’ increasing exposure to synthetic content. While this exposure can open media consumers’ eyes to the depth and breadth of AI-generated content, it can also prime them to think that anything can be manipulated and to neglect or refuse to trust authentic content that is potentially relevant to their decision-making.

General distrust in media

Although there is still no significant evidence that the proliferation of synthetic content is negatively affecting trust in traditional news media,³¹ this concern is already leading some media outlets to make more careful calculations about their approach to GenAI. For instance, Canada’s CBC News considered using an AI-generated persona to conceal the identity of a victim of online romance fraud who wanted to remain anonymous while speaking on the record. A synthetic persona was thought to be capable of preserving the best features of storytelling by conveying the same emotions as the real source – aspects that are usually lost with conventional face and voice alteration techniques. CBC News ultimately decided against this approach, determining that “even with public labels conveying that content is synthetic, there was not sufficiently broad public understanding of the technology to prevent some audience members from being misled or misinterpreting what they saw.”³² Furthermore, the media outlet was concerned about the software company’s use of private data and the possibility that the source’s true identity might be revealed or that the virtual persona might resemble another real person.

In some contexts, where political polarization is relatively low and trust in editorial media is high, citizens might be able to rely on media outlets to fact-check and filter out disinformation – with or without synthetic content. In highly polarized environments, however, where baseline distrust in media is already high, established news media’s decision not to use synthetic content likely will not be enough to restore trust. In fact, research shows that news consumers who distrust the veracity and honesty of traditional news media turn to alternative outlets,³³ such as online platforms, where they are exposed to a higher volume of inauthentic content.

³⁰ Haberman, M. Martin, J. (2017, November 28). *Trump Once Said the ‘Access Hollywood’ Tape Was Real. Now He’s Not Sure*. The New York Times. <https://www.nytimes.com/2017/11/28/us/politics/trump-access-hollywood-tape.html>

³¹ Newman, N. (2024, June 17). *Overview and key findings of the 2024 Digital News Report*. Reuters Institute. <https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024>

³² *How CBC News decided against using AI to conceal a news source’s identity*. (2024) Partnership on AI. <https://partnershiponai.org/wp-content/uploads/2024/03/pai-synthetic-media-case-study-cbcnews.pdf>

³³ Hameleers, M., Brosius, A., & De Vreese, C. H. (2022). Whom to trust? Media exposure patterns of citizens with perceptions of misinformation and disinformation related to the news media. *European Journal of Communication*, 37(3), 237–268. <https://doi.org/10.1177/02673231211072667>

Proposed Remedies and Associated Drawbacks

Government regulatory challenges

Balancing the need for evidence and the need for timely rules before problems emerge

The world is grappling with the difficulty of AI governance more broadly; its novelty, speed of development, and pervasiveness make effective and comprehensive rules all the more difficult. While some policymakers call for careful, “evidence-based” policy – which requires a period of waiting for the consequences of AI use to emerge so data can inform decisions – other experts argue that “holding regulatory action to too high an evidentiary standard can paradoxically make it harder to gather the information that we need for good governance.”³⁴ This paradox can be explained, among other factors, by the facts that the evidence is biased and that the AI industry is deeply entangled with research on the topic.

In the world of elections, waiting for the problem to occur before taking action can be particularly dangerous, as political actors could gain power illegitimately or unfairly by taking advantage of the regulatory vacuum. Furthermore, trying to sanction individuals and fix a tilted playing field after important electoral processes have concluded or election results are known can be extremely risky and raise claims of political interference, as Romania’s 2024–2025 presidential election has shown.³⁵ Clear, settled, widely known, and enforceable rules for political campaigns – and the use of AI in those campaigns – are crucial for election integrity and trust.

Balancing technology-focused and application-focused regulations

The current AI regulatory landscape is chaotic. As Alanoca and colleagues noted in a recent paper, the term “AI regulation” has been used for drastically different efforts. It covers non-binding guidelines, country strategies, and industry standards as well as binding laws and executive orders. It has also been used to describe regulation focused on the technology itself and its applications. This conceptual ambiguity and confusion, they explain, might hinder international cooperation, deter stakeholders from participating in the legislative process, and create a false sense of safety, because citizens might believe there are robust safeguards in place when the “regulations” are nothing more than voluntary commitments – a practice some describe as “ethics washing.”³⁶

Alanoca and co-authors also identify an important distinction in the nature of AI regulations worldwide – whether they target the technology itself (e.g., GenAI, dual-use foundation models, general-purpose systems) or its applications (e.g., deepfakes, biometric identification, recruitment). When considering regulatory frameworks, decision-makers and

³⁴ Casper, S., Krueger, D., & Hadfield-Menell, D. (2025). Pitfalls of Evidence-Based AI Policy. *ICLR*. <https://arxiv.org/abs/2502.09618>

³⁵ For an in-depth analysis of the Romanian case, see IFES’ analysis: The Romanian 2024 Election Annulment: Addressing Emerging Threats to Electoral Integrity (2024, December 20). <https://www.ifes.org/publications/romanian-2024-election-annulment-addressing-emerging-threats-electoral-integrity>

³⁶ Alanoca, S., Gur-Arieh, S., Zick, T., & Klyman, K. (2025). Comparing Apples to Oranges: A Taxonomy for Navigating the Global Landscape of AI Regulation. <https://arxiv.org/pdf/2505.13673>

stakeholders must analyze whether technology-focused and application-focused rules are compatible and whether they sufficiently address risks in political communication.

Harmonizing AI governance with existing laws and regulations, including on freedom of expression

One of the most critical challenges for legislators and stakeholders working on GenAI regulations in political campaigns is ensuring that any new restriction is in line with the country's overall legal framework and does not infringe on established rights and protections, including those related to freedom of expression. The variety of legal frameworks across countries might thus make "importing" regulations more complicated.

In September 2024, the U.S. state of California enacted a law targeting deceptive content and expanding the time frame to ban deceptive AI content targeting political candidates.³⁷ Two weeks after it went into effect, the law was blocked by a judge on the basis that "principles safeguarding the people's right to criticize government ... apply even in the new technological age."³⁸ Minnesota is facing similar challenges to its law on the "use of deep fake technology to influence election."³⁹ Enacted in 2023 and amended in 2024, the law aimed to prevent election deepfakes and punish those who create or disseminate them. X Corporation (formerly Twitter) filed a lawsuit against Minnesota, arguing that the law violated the First and Fourteenth Amendments of the U.S. Constitution and Section 230 of the Communications Decency Act (CDA) by imposing liability against online platforms.⁴⁰ Section 230 of the CDA has provided broad legal immunity to online platforms for user-generated content; while it encourages "good-faith moderation," the regulation shields tech giants from liability for such content. At the time of the writing of this report, the case was still open, and enforcement of the law was paused. Several other U.S. states have introduced similar bills on GenAI content use in elections,⁴¹ but they also seem likely to face challenges.

In Brazil, the debate seems to be going in a different direction. Resolution 23,610/2019 was recently modified by the country's Superior Electoral Court (*Tribunal Superior Eleitoral*, or TSE) to address the use of AI in elections. In addition to explicitly allowing the use of synthetic material in certain circumstances, the resolution imposes some restrictions and makes Big Tech companies liable for not acting immediately to remove irregular content during the electoral period. The resolution also forces these companies to adopt and make public the

³⁷ California Legislature. (2024). *Assembly Bill No. 2839: Elections: Deceptive Media in Advertisements* (Chapter 262, Statutes of 2024). Retrieved from https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB2839

³⁸ United States District Court for the Eastern District of California. (2024, October 2). *Order granting preliminary injunction in Kohls v. Bonta, No. 2:24-cv-02527* [Court order]. CourtListener. <https://storage.courtlistener.com/recap/gov.uscourts.caed.453046/gov.uscourts.caed.453046.14.0.pdf>

³⁹ Minn. Stat. § 609.771 (2024). *Use of deep fake technology to influence an election*. Retrieved from <https://www.revisor.mn.gov/statutes/cite/609.771>

⁴⁰ X Corp. v. Ellison, No. 0:25-cv-01649 (D. Minn. filed April 23, 2025) [Complaint]. Retrieved from <https://www.courthousenews.com/wp-content/uploads/2025/04/X-lawsuit-minnesota-deepfake.pdf>

⁴¹ Ballotpedia. (n.d.). *AI deepfake legislation tracker: Political communications (2025 session)*. Retrieved June 11, 2025, from <https://legislation.ballotpedia.org/ai-deepfakes/search?category=Political%20communications&session=2025&page=1>

measures they have taken to reduce dissemination of content that undermines electoral integrity.⁴² In June 2025, the Brazilian Supreme Court expanded Big Tech liability, making online platforms responsible for taking down certain third-party content even in the absence of a specific judicial order.⁴³

In several countries, election management bodies have the authority to issue and enforce regulations on the use of media during elections, but specifically regulating the use of AI is particularly complex. In the Philippines, for instance, the Commission of Elections (COMELEC) issued Resolution No. 11064⁴⁴ on September 26, 2024, ahead of May 2025 general elections. The resolution established guidelines for the use of AI, social media, and internet technologies, requiring the registration of all digital campaign platforms (social media accounts, websites, blogs, podcasts) and mandating disclosure of AI-generated content as well as facilitation of content verification by COMELEC. It explicitly prohibited the misuse of these technologies to create and disseminate deepfakes, use fake accounts or bots to artificially amplify narratives, or coordinate inauthentic behavior aimed at manipulating public opinion.

COMELEC's original resolution intended to apply the registration requirement (and sanctions for non-compliance) to *all* actors, including private individuals and entities using online platforms to support or oppose a political candidate. However, election watchdogs and human rights advocates argued that such broad obligations risked chilling legitimate political speech and could deter civil society groups, independent journalists, and ordinary citizens from participating in democratic discourse online. Critics also questioned whether COMELEC had the technical capacity to monitor media and consistently enforce the rules in an impartial manner, particularly given resource constraints and the volume of content generated during national campaigns – a concern that applies to most, if not all, election commissions. Following sustained advocacy, COMELEC eventually amended the resolution to remove sanctions on private individuals and influencers.⁴⁵

Similar debates have emerged in Indonesia and Brazil, where election authorities are testing new regulatory frameworks to address synthetic content, often amid significant controversy. Stakeholders must not only review existing frameworks carefully and ensure new regulations

⁴² TSE proíbe uso de inteligência artificial para criar e propagar conteúdos falsos nas eleições. (2025, February 22). Justiça Eleitoral. <https://www.tse.jus.br/comunicacao/noticias/2024/Fevereiro/tse-proibe-uso-de-inteligencia-artificial-para-criar-e-propagar-conteudos-falsos-nas-eleicoes>

⁴³ Pompeu, A., & Feitoza, C. (2025, June 12). STF Tem Maioria Para Ampliar Responsabilização de Big Techs. Diário da Manhã. <https://www.dm.com.br/brasil/stf-tem-maioria-para-ampliar-responsabilizacao-de-big-techs/>

⁴⁴ Commission on Elections, Republic of the Philippines (2024, September 17). *Resolution No. 11064: Guidelines on the use of social media, artificial intelligence, and internet technology for digital election campaigns, and the prohibition and punishment of its misuse for disinformation and misinformation, in connection with the 2025 national and local elections and the BARMM parliamentary elections.* https://comelec.gov.ph/php-tpls-attachments/2025NLE/Resolutions/com_res_11064.pdf

⁴⁵ Aning, J. (2025, February 17). *Comelec eyes shutdown of unregistered socmed campaigners.* Inquirer.net. <https://www.inquirer.net/429066/comelec-eyes-shutdown-of-unregistered-socmed-campaigners/>

are compatible but also be open to revoking or modifying rules that have become obsolete or no longer contribute to the greater good.

Tech company self-regulation, risk assessments, and ethical commitments

Technology companies involved in building AI platforms and creating and disseminating content have also initiated or participated in independent initiatives to establish safeguards for the ethical use of AI in political messaging. Among these initiatives is the AI Elections Accord, an agreement signed by 27 AI companies committing to combating deceptive use of AI in 2024 elections.⁴⁶ However, it is important to be vigilant about the actual behavior of these companies and whether commitments are being followed or simply used for public relations purposes. As an analysis by the Brennan Center for Justice notes, only about half of the signatory companies provided a progress report for the accord website,⁴⁷ and many failed to report on all eight core accord commitments.⁴⁸ The Brennan Center analysis also points out the lack of oversight by independent institutions and civil society in understanding these companies' compliance with their commitments, which hinders transparency and accountability.

Another initiative AI developers can subscribe to is the use of risk assessments for AI tools. Google, for instance, launched its Secure AI Framework (SAIF) and accompanying SAIF Risk Assessment to, as the company stated, “help secure AI systems across industry.”⁴⁹ The framework is designed to help companies analyze issues such as access controls to models and data sets, prevent adversarial attacks, and secure coding frameworks.

While potentially useful, these types of company-led risk assessments can also encounter roadblocks, particularly when findings trigger conflicts of interest. For example, companies may be reluctant to disclose risks publicly if doing so could expose them to liability, damage their reputation, or reduce their competitive advantage. In some cases, decision-makers might even underplay or ignore identified risks if they calculate that the commercial payoff outweighs potential harms. As Birhane and colleagues have found analyzing papers on machine learning, the values reflected in this literature overwhelmingly focus on system performance over users' rights and ethical principles.⁵⁰

As Casper, Krueger, and Hadfield-Menell note, this focus on performance – and the fact that, in many cases, the ones doing or funding AI research are also the tech companies profiting from the technology – suggests that the “AI community may be systematically predisposed

⁴⁶ A Tech Accord to Combat Deceptive Use of AI in 2024 Elections (2024, September 17). *AI elections accord*. <https://www.aielectionsaccord.com/>

⁴⁷ Ahmed, A. Doyle, O. Harris, D. E. Norden, L. (2025, February 13) Tech Companies Pledged to Protect Elections from AI — Here's How They Did. *Brennan Center for Justice*. <https://www.brennancenter.org/our-work/research-reports/tech-companies-pledged-protect-elections-ai-heres-how-they-did>

⁴⁸ For more details on the eight core commitments, see [Commitments - AI Elections Accord](#).

⁴⁹ Adkins, H. Venables, P. (2024, October 24). SAIF Risk Assessment: A new tool to help secure AI systems across industry. *Google*. <https://blog.google/technology/safety-security/google-ai-saif-risk-assessment/>

⁵⁰ Birhane, A., Kalluri, P., Card, D., Agnew, W., Dotan, R., & Bao, M. (2022). The values encoded in machine learning research. *2022 ACM Conference on Fairness, Accountability, and Transparency*, 173–184. <https://doi.org/10.1145/3531146.3533083>

to produce evidence that will disproportionately highlight the benefits of AI compared to its harms.”⁵¹ This dynamic is particularly problematic in the electoral context, where the consequences of poorly mitigated risks, such as the spread of targeted disinformation about a candidate or democratic institution, are severe and difficult to reverse once public confidence has been undermined.

Direct disclosure

In a recent guidance document, the U.S. National Institute of Standards and Technology (NIST) lists the following as the most common techniques used to directly disclose AI use in content:⁵²

- Content labels (visible tags and warnings within/on top of content)
- Visible watermarks (icons in various shades covering content to indicate AI usage)
- Disclosure fields (disclaimers and statements indicating AI use and providing more context on the content)

While disclosing AI use is a logical step in enhancing transparency and promoting better-informed media consumption, as a recent report by the International Republican Institute notes, such technical fixes do not always account for the sociopolitical nature of disinformation.⁵³ Google-led research has found that people often struggle to understand the nuance between labels such as “created by AI,” “not created by AI,” “edited with AI,” and “altered or synthetic content.” Recent experiments run by Google’s Jigsaw have also shown that a significant number of people might not believe warnings about inauthentic digital content, or simply disregard such warnings; as mentioned earlier in this report, they might also share this content, even knowing it conveys false information.⁵⁴

Furthermore, Google’s studies seem to corroborate the “implied authenticity effect”⁵⁵ – meaning that the fact that some content is labeled induces people to believe in the authenticity of unlabeled material. The body of evidence on the effects of labeling is still growing, and nuances are starting to emerge. For instance, another set of experiments by Sanderson, Zhong, and Tucker found that implied authenticity effects were zeroed out by an

⁵¹ Casper, S. Krueger, D. Hadfield-Menell, D. (2025). Pitfalls of Evidence-Based Policy. *ICLR*.
<https://arxiv.org/pdf/2502.09618>

⁵² Raimondo, G. M., Locascio, L. E., Chandra, B., Dunitz, J., Awad, G., Lee, Y., Fontana, P., Amironesei, R., Przybocki, M., Roberts, K., Heyman, M., & Tabassi, E. (2024). Reducing Risks posed by synthetic content: An Overview of Technical approaches to digital content transparency. In *NIST Trustworthy and Responsible AI*. National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-4.pdf>

⁵³ Ooi, H. H., Spittler, A., Zink, A., & International Republican Institute. (2024). Democracy in the age of Generative AI: Navigating risks and harnessing opportunities. In *International Republican Institute*. <https://www.iri.org/wp-content/uploads/2024/08/GenAI-Democracy-White-Paper-Final.pdf>

⁵⁴ Jigsaw. (2021, August 31). The effect of warning labels on the perceptions of manipulated media. *Medium*. <https://medium.com/jigsaw/the-effect-of-warning-labels-on-the-perceptions-of-manipulated-media-c1de5ceb83e9>

⁵⁵ Wittenberg, C. Epstein, Z. Berinsky, & A. Rand, D. (2023, November 28). Labeling AI-Generated Content: Promises, Perils, and Future Directions. *MIT*. <https://pdfs.semanticscholar.org/de8b/185841ad92b7502845ee344ae707931eb0e0.pdf>

increased skepticism toward unlabeled media caused by prior exposure to labeled content.⁵⁶

Google has also reported concerns about media consumers assuming that anything labeled as AI-generated is inherently untrustworthy, even when the digital alteration is minor or could help consumers visualize complex phenomena (e.g., quantum mechanics) that cannot be captured through “authentic” means.⁵⁷ Such cognitive shortcuts have been identified in other areas; for instance, several studies have shown that people tend to perceive genetically modified foods negatively and avoid products labeled as containing genetically modified parts even if they are safe and offer better nutritional content than non-genetically modified foods.⁵⁸ Given these insights, Google has decided to employ prominent direct disclosures sparingly, “only in cases with sensitive content in which there is high likelihood of harm from deception (e.g., an election ad).”⁵⁹

It is very important for technology companies such as Google to keep doing rigorous research and adapting their institutional policies and approaches toward AI and AI labeling in responsible ways, but it is also critical that the public does not rely exclusively on corporate goodwill and social responsibility. In its case study report published by Partnership on AI, Google states that “we determined that the benefits at this time of placing a prominent label on sensitive content such as election ads outweighed the downsides outlined above.”⁶⁰ It is worth questioning, however, whether it should be a company’s responsibility – or right – to establish risk or sensitivity thresholds when it comes to issues with clear implications for the public. It should also not be assumed that all companies will carefully consider the risks – and be transparent about them – or that they will prioritize the public good over profit without more formal legal and regulatory constraints and pressure from government and the public.

Indirect disclosure: provenance metadata, watermarking, and other forensic markers

A leading remedy proposed to fight misleading AI-generated content online is the establishment of technical standards to provide anyone – creators, publishers, and consumers – with the ability to trace the origin of media and detect manipulation, even if the content is not explicitly labeled as manipulated. This approach might include reviewing cryptographic signatures and metadata about the content’s origin and editing history.

⁵⁶ Sanderson, Z. Zhong, & W. Tucker, J. (2025). It Works When It Works: Measuring the Direct and Indirect Effects of AI Labels on Political Images (preprint). https://www.researchgate.net/publication/397026730_It_Works_When_It_Works_Measuring_the_Direct_and_Indirect_Effects_of_AI_Labels_on_Political_Images

⁵⁷ Hebbar, N. Wolf, C. (2024, December 3). Determining trustworthiness through provenance and context. Google. <https://publicpolicy.google/article/determining-trustworthiness-provenance-context/>

⁵⁸ Kim, Y., Kim, S., & Arora, N. (2022). GMO labeling policy and consumer choice. *Journal of Marketing*, 86(3), 21-39. <https://journals.sagepub.com/doi/abs/10.1177/00222429211064901>

⁵⁹ How Google’s research informed its approach to direct disclosure (2024). *Partnership on AI*. <https://partnershiponai.org/google-framework-case-study/>

⁶⁰ Ibid.

In addition to supporting transparency, provenance metadata can help investigative journalists, fact-checkers, and election authorities verify the authenticity of content more quickly during critical events, like elections or protests, when misinformation spreads rapidly. It can also help platforms automate the detection of manipulated media at scale by cross-referencing embedded signatures against trusted registries.

The Coalition for Content Provenance and Authenticity (C2PA)⁶¹ – a collaborative effort among major technology and media companies – has introduced new cryptographic techniques to enable this type of rapid review by embedding tamper-evident metadata into files, including images, videos, audio, and documents. Consumers would click on an icon somewhere in the file to see information such as when the content was created, by whom, and what types of edits have been made. Standards like C2PA can significantly increase transparency in digital content manipulation, but must rely on adoption across platforms that build and host synthetic content. Some companies are already integrating C2PA specifications into commercial tools, while others have announced pilot programs to evaluate their scalability and interoperability across diverse ecosystems. Their effectiveness also relies on creators to voluntarily disclose information or, at a minimum, not make efforts to remove provenance metadata that could reveal manipulation.

In its report explaining that overly frequent direct disclosure could overwhelm and confuse media consumers, Google suggests instead the consideration of clear “entry points” in the media – icons users can click to “learn more” about the content, including provenance data and more context about the extent of AI use.⁶² But in addition to the technical issues described above, indirect disclosure also faces *technical-social* challenges; it requires media consumers to both (1) have the ability to access and understand the context and provenance information and (2) be sufficiently interested in verifying the authenticity of content. Direct and indirect disclosure could also get more complicated and harder to enforce when content is shared through private person-to-person and group chats, as opposed to more public social media accounts.

Conclusions and paths forward

While some experts have quickly dismissed what they deem “overblown” concerns over the impact of GenAI in elections, the examples throughout this paper serve as a warning that there are, in fact, many reasons for concern. The question is not simply whether synthetic content can change voters’ choices on the ballot, but also how such content shapes voters’ relationships with information and with political representatives; their capacity and willingness to trust individuals, processes, and institutions; and their ability to make decisions outside of the echo chambers that not only do not challenge their strongest biases, but also reinforce those biases.

⁶¹ Advancing digital content transparency and authenticity (n.d.). C2PA <https://c2pa.org/>

⁶² How Google’s research informed its approach to direct disclosure (2024). *Partnership on AI*. <https://partnershiponai.org/google-framework-case-study/>

This report has also offered an overview of legal and regulatory, ethical, and socio-technical challenges stakeholders are facing in trying to address these issues. While no definitive or all-encompassing solutions are available, emerging evidence and lessons learned can help shape paths forward for decision-makers, election authorities, civil society, and other stakeholders. Below are some initial recommendations.⁶³

Engage independent experts in the search for evidence. As reflected in this report, a large volume of cutting-edge research on GenAI is being conducted or funded by technology companies. While this may be a sign of commitment to social responsibility, it may also undermine the impartiality of findings and conclusions. It is crucial for the transparency and integrity of the evidence-finding process to engage – and fund – independent experts who can build on, but not rely on, the research produced by those with attached financial interests. California recently did this, convening AI experts – mainly from academia – into the Joint California Policy Working Group on AI Frontier Models, which produced a report with recommendations for California legislators considering AI-related bills.⁶⁴ It is important to keep investing in such research, specifically its impact on political messaging.

Engage political actors and the public to enhance AI literacy and gather well-informed inputs. The novelty and technical complexity of AI might make the public hesitant to partake in the policy and regulation debate, but their perspectives and inputs are very much needed. The same goes for political actors, who are directly implicated in and affected by the use of AI in political campaigning. It is important to convey to these stakeholders that they do not need to be experts in the workings of AI to engage in conversations about its impact on their lives. The California initiative mentioned above, for instance, ensured there was a period for public input to the expert document. The opportunity allowed civil society and advocacy groups to not only provide their own thoughts but also to show support for certain recommendations.⁶⁵ As legislators consider AI regulations related to political campaigning, they should ensure those involved in campaigning also have opportunities to chime in.

Carefully consider labeling regulations, while being cautious of the negative effects of over-labeling. While transparency is critical, it is also critical to be aware of the unintended consequences of certain well-intentioned measures, such as labeling all content created, edited, or manipulated with AI. When facing an overload of information, people tend to use cognitive shortcuts to make judgments and could simply internalize that everything touched

⁶³ IFES is also developing a more comprehensive playbook on the safe use of AI in elections via its AI Advisory Group on Elections ([AI AGE](#)).

⁶⁴ Chayes, J. T., Cuéllar, M.-F., Fei-Fei, L., Bommasani, R., Singer, S., Appel, R. E., Cen, S., Cooper, A. F., Cryst, E., Gailmard, L. A., Gonzalez, J. E., Ho, D. E., Klaus, I., Lee, M. M., Liang, P., Reuel, A., Song, D., Spence, D., Weinstock, J. (2025b). *Joint California Policy Working Group on AI Frontier Models*. https://www.cafrontieraigov.org/wp-content/uploads/2025/03/Draft_Report_of_the_Joint_California_Policy_Working_Group_on_AI_Frontier_Models.pdf

⁶⁵ Barcott, B. (2025, April 13). California's AI Working Group Report is good. Here's how it could be better — Transparency Coalition. Legislation for Transparency in AI Now. Transparency Coalition. <https://www.transparencycoalition.ai/news/californias-ai-working-group-report-is-really-good-heres-how-it-could-be-better?>

by AI is untrustworthy – or that everything not manipulated by AI *is* trustworthy – when that is not the case. Media consumers could also become numb to the labels if they are in virtually every piece of media they consume, which might not be an unreasonable assumption as AI use expands.

Carefully balance any restrictions on the dissemination of information with safeguards on freedom of expression. Constraints on speech and content are not to be taken lightly, particularly given the power of controlling narratives on electoral and political outcomes. But decision-makers must consider the realities in their countries and work on longer-term, sustainable solutions, such as digital literacy, while also addressing the challenges of the day, which might require regulations restricting certain content. Decision-makers must carefully analyze their overall legislative frameworks and societal contexts to impose any necessary constraints while safeguarding freedom of expression.

Anticipate the need for legislative change and adaptation. People’s relationship with GenAI is changing rapidly; how they perceive synthetic content, how they use AI platforms to create their own content, and the political and societal effects of such content are also expected to change over time. Legislators should thus commit to periodically revisiting assumptions, updating data, and hearing from those most affected by GenAI to adjust legal frameworks.

Consider special legislation and exemptions to enable political actors to minimize damage caused by GenAI during electoral campaigns. Several countries have established “silent periods” (also known as “electoral silence” or “blackout periods”), usually 1 to 2 days before election day, during which political rallies and campaign messaging and activities are prohibited. Malign actors might take advantage of their anonymity and this legal impediment on candidates to spread harmful synthetic content in the period when targeted individuals and parties cannot properly respond. Legislators should consider ways to reduce incentives for or minimize the impact of this tactic, such as offering opportunities for victims of malicious synthetic content to respond and debunk it. In Brazil, for instance, the “right of reply” enables candidates affected by disinformation in the official campaign broadcast, print media, radio, television or the internet to make factual corrections – upon favorable court rulings – using the same medium where the disinformation was shared.⁶⁶ However, if actors violate the silent period, there is much less time for the courts to hear a case and concede space for replies ahead of election day.

Build hybrid regulatory frameworks of technology-focused and application-focused rules. Acknowledging that regulations that focus on GenAI technology broadly might not sufficiently address specific risks to the electoral process, decision-makers and stakeholders should ensure these are complemented by compatible application-focused regulations, such as GenAI use for political campaigns, lobbying, and voter engagement.

⁶⁶ Rollo, A. (2024, September 14). *O direito de resposta nas eleições municipais deste ano*. Consultor Jurídico. Retrieved 6/12/2025 from <https://www.conjur.com.br/2024-set-14/o-direito-de-resposta/>

Identify sanctions that more effectively address incentives (e.g., working with payment processors to prevent financial transactions to platforms that violate rules and regulations). The prospect of financial gains is usually a strong motivator for less-reputable AI platforms to violate standards and regulations. They provide users with capabilities that more reputable AI companies do not offer, such as using politicians' likenesses without their consent to create deepfakes and pornographic content. Regulators can work with e-commerce payment processing companies to halt financial transactions to platforms known to be in violation of rules and regulations. For example, in May 2025, after warnings and requests by credit card processors for CivitAI to review its policies, which had enabled users to make nonconsensual pornographic content, the companies decided to pause services to the AI platform.⁶⁷ This is not a foolproof measure, because platforms can resort to using cryptocurrency and other less transparent payment mechanisms – as CivitAI indicated it would do – but it would still be an obstacle to wrongdoing.

Require transparency and human oversight of AI systems. Regardless of whether countries where AI companies operate have already passed laws on the topic, companies should take a proactive approach to following the good practices and requirements established in existing global legislation, such as conducting thorough risk assessments on new products, ensuring system training data are of high quality, documenting technical and ethical decisions, facilitating human oversight, and clearly communicating with users and the public about the platform's features and operating issues.

Invest in institutional communication and collaborate with AI platforms to facilitate accurate outputs to questions and prompts on elections and other political processes. As more people rely on major AI platforms to get quick answers to their questions about elections, election management bodies can work with these companies to ensure outputs are informed by data from official channels and even to encourage users to check election management bodies' official websites and social media accounts for the latest information. Election management bodies and other public institutions should also invest in enhancing their official channels to provide clear and consistent messages and reduce the need for users to go to third parties for information.

Avoid harmful mass surveillance practices. While scraping social media content to identify mis- and disinformation narratives or abnormalities in voting locations can enable quicker responses by election authorities, they should weigh the reputational costs of such initiatives, which can be perceived as mass surveillance tactics and have an impact on people's participation.⁶⁸ Election management bodies should also make sure to incorporate ethical data management standards into scraping practices to preserve individual privacy.

Prioritize media literacy and critical thinking programs. GenAI capabilities are evolving at an incredible pace. Only a few months before this report's publication, experts were

⁶⁷ Maiberg, E. (2025, June 13). *Civitai, site used to generate AI porn, cut off by credit card processor*. 404 Media. <https://www.404media.co/civitai-site-used-to-generate-ai-porn-cut-off-by-credit-card-processor/>

⁶⁸ Juneja, P. (2024, April 29). Artificial intelligence for electoral management. *International IDEA*. <https://www.idea.int/publications/catalogue/artificial-intelligence-electoral-management>

instructing media users to look for clues that content was fake by looking at eye patterns⁶⁹ and the number of fingers or hand gestures.⁷⁰ Newer AI technology is quickly overcoming these issues; few to no flaws in synthetic content will be detectable to the human eye. Instead of investing in interventions that encourage people to look for visible signs, programs should focus instead on helping media consumers fact-check and use appropriate tools to gauge the likelihood of authenticity of content. Most importantly, investments should be made in developing people’s critical thinking skills to analyze, question, and investigate content before forming judgments. For elections, given the high profile of politicians and the high stakes of electoral processes, verifying information should be easier because mainstream media will most likely invest in investigating controversial reporting. However, partisanship can compromise critical thinking.

These preliminary recommendations are based on an understanding of people’s *current* relationship with GenAI content, which is largely shaped by their exposure to and familiarity with it at the moment. As exposure and familiarity deepen and expand, as seems to be the logical course, this relationship will certainly evolve – as should our strategies to address the emerging challenges.

⁶⁹ Tonkin, S. (2024, July 17). Want to spot a deepfake? Look for the stars in their eyes. *The Royal Astronomical Society*. <https://ras.ac.uk/news-and-press/research-highlights/want-spot-deepfake-look-stars-their-eyes>

⁷⁰ Chapman, P. (2024, December 17). Hands, eyes, voice — How to spot an AI Deepfake. *Firebrand*. <https://firebrand.training/uk/blog/hands-eyes-voice-how-to-spot-an-ai-deepfake>



2000 M Street NW, Washington, DC, 20036, United States

www.IFES.org