IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Preserving Electoral Integrity In The Age Of Artificial Intelligence: Legal And Ethical Challenges In Regulating Ai- Driven Campaign Practices.

- Lakshika Negi, LL.M, University Institute of Legal Studies, Chandigarh University

-Dr. Shailja Thakur, Assistant Professor, University Institute of Legal Studies, Chandigarh University

Abstract

This paper provides a comprehensive legal and ethical analysis of the integration of Artificial Intelligence (AI) into modern political campaigning. It examines the dualistic role of AI, which simultaneously offers unprecedented tools for voter engagement and campaign efficiency while posing significant threats to democratic integrity through the proliferation of disinformation, deepfakes, and invasive micro targeting. The paper conducts a comparative analysis of regulatory frameworks, contrasting the proactive, advisory-led approach of the Election Commission of India (ECI) with the comprehensive, rights-based EU AI Act and the fragmented, disclosure-focused legislation in the United States. Through an examination of key case laws, including the Cambridge Analytical scandal and incidents from the 2024 Indian general election, the paper identifies core challenges in regulation, such as the "pacing problem" of law versus technology and the tension between curbing harmful content and protecting free speech. The paper concludes by offering a multi-stakeholder framework of recommendations, advocating for amendments to existing Indian laws (the Representation of the People Act, 1951, and the Information Technology Act, 2000), mandating algorithmic and financial transparency, prohibiting specific malicious AI applications, and investing in public digital literacy to foster a resilient electorate.

Key words: Artificial intelligence, technology, election, deepfake, campaigns, politics

1. Introduction

The integration of technology into the electoral process is not a new phenomenon, but the recent advancements in Artificial Intelligence (AI) represent a categorical shift in its nature and impact.[1] The historical trajectory began with the systematic collection and analysis of voter data, which has long been the cornerstone of modern political campaigns.[1] This first wave of computational politics was epitomized by the Cambridge Analytica scandal, where the firm leveraged vast datasets harvested from social media to construct detailed psychographic profiles of voters. This analytical approach, while controversial, required significant capital, data science expertise, and access to proprietary data, creating a high barrier to

entry.[2]

The contemporary landscape has been fundamentally reshaped by the advent and widespread accessibility of generative AI. The public release of powerful models such as OpenAI's ChatGPT, Google's Bard, and image generators like Midjourney and DALL-E in 2022 marked a paradigm shift from analytical AI to creative AI.[4] These tools empower users to generate novel and hyper-realistic text, images, audio, and video content from simple text prompts, often at little to no cost and with minimal technical skill.[5] The 2024 global election year, with polls in over 50 countries including India and the United States, has been identified as the first to be conducted under the widespread influence of these potent new technologies.[8] This technological evolution has effectively democratized the tools of mass influence. While early AI applications in politics were the domain of well-funded entities, generative AI's low cost and user-friendliness have diffused sophisticated content creation capabilities to a vast array of actors, from less-resourced political campaigns to individual malicious actors.[6] This shift from a centralized, high-cost model of influence to a decentralized, low-cost one is the primary driver of the current regulatory and ethical crisis, fundamentally altering the threat model for electoral integrity.

The proliferation of AI in the political sphere presents a profound democratic dilemma. On one hand, AI offers a suite of tools that can potentially enhance and invigorate democratic discourse. It can be used to educate citizens by simplifying complex policy issues, help politicians better understand constituent concerns, and empower smaller campaigns to compete on a more level playing field.[2] This potential for positive transformation positions AI as a potential catalyst for a more engaged and informed electorate.

On the other hand, this same technology provides a formidable toolkit for those seeking to undermine democratic processes. Malicious actors can leverage generative AI to create and disseminate disinformation at an unprecedented scale, impersonate candidates through "deepfakes," and execute sophisticated voter suppression campaigns.[7] This dual-use nature of AI makes it a "double-edged sword" [12], capable of simultaneously strengthening and weakening the foundations of democracy.[13] This inherent tension creates a complex regulatory challenge for policymakers worldwide: how to craft a governance framework that fosters the benefits of technological innovation while mitigating its profound risks to electoral integrity, all without unduly stifling innovation or infringing upon fundamental rights such as freedom of expression.[14]

2. The Evolving Role of AI in Political Campaigns

The integration of Artificial Intelligence has transformed the mechanics of political campaigning, shifting the paradigm from mass communication to hyper-personalized, data-driven engagement. AI now permeates every stage of the campaign process, from content creation and voter analysis to resource allocation and outreach.

Imagine a time when political campaign relied on in person rallies, printed advertisement and going to door to door connect with voters. Now we see how AI is changing the way candidates reach out to their supporters. Back in 2012, former president, Obama’s campaign team use data analysis to target specific voters more effectively. By the time of the 2016 and 2020 election, AI chat and sentiment analysis become common tool in campaigning. Today, AI driven tool help politicians, craft, personalized message, predict voters, behavior and manage advertisement budget more efficiently. The future of election look even more promising while AI applications, allowing campaigns to be smarter and focused on data like never before.

In India, we can highlight the state like Bihar, Kerala, West Bengal, and Tamil Nadu, where the elections are just few months away. But Digital campaigns are already busy with their plans. These important elections will likely see a more advanced and creative use of artificial intelligence. Which played a major role in previous elections. The fight of portal is shifting from crowded rally and road shows to screens, driven by algorithm, data and AI. And in the day of winning the powerful speeches and well planned. Propaganda events are behind us. Now the digital world has become the new battlefield. The strategies who influence public opinion often work with lines of court and instead of relying solely on personal charm. For example, there are vital AI created posters that show Prime Minister Narendra Modi as Marvel, superhero and former Delhi chief minister Arvind Kejriwal as a character of similar to Harry Potter. While the face is recognizable, the creativity behind this campaign comes from artificial intelligence. AI is no longer just a future concept; it is part of our present reality and is deeply integrated into the working of the world's largest democracy. With a young and tech savvy voted based leading the Way; India is quickly adopting the technological shift in the political landscape.

2.1 Automating Persuasion: AI in Content Generation and Messaging

Political campaigns are increasingly leveraging generative AI to automate the creation of a vast array of communication materials. AI-powered tools are now routinely used to generate first drafts of speeches, scripts for advertisements, and fundraising emails, significantly accelerating the content production pipeline.[6] This automation extends to the creation of novel visual and textual content from simple prompts, allowing a small team to produce a volume of material that would have previously required a large digital staff.[6]

This capability for mass content generation enables campaigns to engage in rapid, iterative testing of messages. They can create and deploy hundreds or even thousands of variations of an advertisement or email daily, continuously refining their messaging based on real-time engagement data.[6] The 2024 Indian general election served as a prominent example, where political parties were projected to spend upwards of $50 million on authorized AI-generated content. This included the creation of personalized video messages addressing voters by name and the translation of speeches into multiple regional languages to broaden their reach.[17]

2.2 The Science of Influence: Micro targeting, Sentiment Analysis, and Predictive Modeling

At the core of AI's electoral impact is its ability to analyze massive datasets to understand and influence voter behavior with unprecedented granularity. This has supercharged several key campaign functions.

Micro targeting: AI elevates traditional micro targeting from a demographic-based practice to a psycho graphic one. By synthesizing vast datasets encompassing voter records, consumer behavior, social media activity, and online interests, AI algorithms can craft hyper-personalized messages designed to resonate with the specific values, concerns, and even psychological vulnerabilities of narrow voter segments.[3] This approach, pioneered by firms like Cambridge Analytical, moves beyond targeting groups based on age or location to targeting individuals based on personality traits like openness or conscientiousness.[3] Initial research indicates that these AI-tailored political advertisements are perceived by voters as significantly more persuasive than generic, non-personalized ads.[3] This automated personalization creates what has been termed a "manipulation machine," capable of scaling persuasive appeals that target individual vulnerabilities without direct human input.[3]

Sentiment Analysis: AI-driven sentiment analysis tools provide campaigns with a real-time dashboard of public opinion. These systems process enormous volumes of unstructured text from social media platforms like X (formerly Twitter) and Facebook to identify and track public attitudes towards

candidates, key issues, and campaign events.[21] This allows campaigns to gauge the public's response to their advertisements, devise rapid counter-messaging to negative narratives, and identify which issues are most salient to different voter groups at any given moment.[21]

Predictive Modeling: By analyzing historical data, campaigns use AI to build predictive models of voter behavior. These models can identify which voters are most likely to be persuadable, which supporters need an extra push to turn out on Election Day (Get-Out-The-Vote efforts), and which individuals are likely to be high-value donors.[19] Some advanced techniques even involve creating simulated populations of AI "agents," conditioned to reflect the demographic and ideological characteristics of real voter segments, to test the potential impact of different policy positions or messages before they are deployed publicly.[25]

The convergence of these techniques creates a paradox. Campaigns can now foster a feeling of intimate, one-on-one conversation with millions of voters simultaneously, as seen with personalized calls in the Indian elections.[17] However; this perceived intimacy is an artifice, generated by an impersonal, automated system executing a persuasion algorithm based on harvested data. This raises profound ethical questions about the authenticity of modern political communication and whether it constitutes genuine dialogue or a form of scaled, algorithmic manipulation.

2.3 Democratizing Digital Campaigning: AI as a Tool for Less-Resourced Candidates

One of the most significant structural impacts of generative AI is its potential to level the playing field in the digital political arena. Historically, a major disparity has existed between well-funded, high-profile campaigns and their smaller, less-resourced counterparts. Large campaigns could afford sizable digital teams capable of producing and disseminating a high volume of sophisticated, targeted advertisements, an area where smaller campaigns were unable to compete.[6]

The current ecosystem of low-cost, user-friendly AI tools disrupts this equation. These platforms, which require no prior knowledge of coding or machine learning, allow campaigns with limited budgets to outsource the production of targeted advertising and other digital content.[6] The content generated by these tools can rival the quality and sophistication of that produced by big-budget campaigns, giving smaller candidates and insurgent political movements a significant boost in their ability to compete for voters' attention online.[6] This democratization of sophisticated campaign tools represents a dual-edged sword: while it can foster greater competition and empower new voices, it also lowers the barrier to entry for malicious actors to launch sophisticated disinformation campaigns.

3. The Positive Impact of AI on Elections

While the risks associated with AI in elections often dominate public discourse, the technology also presents significant opportunities to strengthen democratic processes, enhance voter pasrticipation, and improve the efficiency of campaigns and electoral administration. These positive applications are often focused on overcoming systemic barriers to engagement, such as information complexity and linguistic diversity.

3.1 Enhancing Voter Engagement and Education through Personalization

AI can serve as a powerful tool for civic education and engagement by making complex political information more accessible and digestible for the average voter. AI-powered platforms, such as chatbots and virtual assistants, can be deployed to provide citizens with personalized, on-demand information. These tools can answer procedural questions about how to register to vote, find a polling place, or

understand the voting process, thereby reducing administrative hurdles that can discourage participation.[28]

Furthermore, generative AI can help bridge the information gap between politicians and the electorate. It can be used to condense lengthy and dense policy proposals into clear, easy-to-understand summaries tailored to a user's interests.[29] This function helps voters make more informed decisions based on a better understanding of the substantive issues at stake, moving beyond personality-driven politics. This form of AI application focuses on empowering the voter with knowledge, contrasting sharply with applications designed for psychological persuasion.

3.2 Bridging Divides: AI for Multilingual Translation and Accessibility

In nations characterized by significant linguistic diversity, AI-powered translation tools have emerged as a transformative force for inclusive political communication. India's 2024 general election provided a compelling case study. The ruling Bharatiya Janata Party (BJP) successfully utilized 'Bhashini', an indigenous AI translation tool, to translate Prime Minister Narendra Modi's speeches from Hindi into numerous regional languages in real-time.[17] This allowed his message to reach millions of voters in non-Hindi-speaking regions, overcoming long-standing language barriers that have historically fragmented the national political discourse.[29] By making campaign messages accessible to a wider audience, AI can help reduce the disenfranchisement of linguistic minorities and foster a more unified and inclusive national conversation.

3.3 Optimizing Campaign Efficiency and Resource Allocation

Beyond voter-facing applications, AI offers significant advantages for the internal operations of both political campaigns and electoral management bodies. For campaigns, AI algorithms can analyze vast and disparate datasets—including historical voting patterns, demographic trends, media coverage, and government performance reports—to generate actionable strategic insights.[2] This data-driven approach enables campaigns to allocate their finite resources, such as advertising budgets and staff time, with far greater precision and efficiency, targeting their efforts where they are most likely to have an impact.[28]

For the institutions responsible for administering elections, AI presents opportunities to improve logistical efficiency and security. Appropriately designed AI programs could be used to optimize the allocation of resources to polling stations based on predicted voter turnout, or to support the complex logistics of facilitating voting for citizens abroad.[2] Moreover, AI-powered monitoring systems can be used to enhance election integrity by detecting anomalies, potential fraud, or irregularities in voting data, allowing officials to respond swiftly to potential threats.[28] These applications demonstrate AI's potential to make the mechanics of democracy more robust, efficient, and secure. A regulatory framework that can distinguish between these beneficial uses for civic *enablement* and more problematic uses for voter *persuasion* will be critical to harnessing AI's positive potential while mitigating its risks.

4. The Negative Impact of AI and the Challenge to Democracy

The same technological attributes that empower positive applications of AI in elections—speed, scale, and personalization—also make it a formidable weapon for undermining democratic integrity. The negative impacts range from the overt dissemination of fabricated content to subtle algorithmic manipulation, culminating in a systemic erosion of public trust that poses an existential threat to informed, deliberative democracy.

4.1 The Proliferation of Disinformation: "Deepfakes" and Synthetic Media

The most widely discussed threat from generative AI is its capacity to create "deepfakes"—hyper-realistic but entirely synthetic audio, images, and videos—rapidly and at a negligible cost.[5] This technology enables malicious actors to fabricate content depicting political candidates, election officials, or other public figures saying or doing things they never did, creating potent and highly believable political smears.[7] Because this content is often emotionally provocative, it is primed for viral dissemination on social media platforms, reaching millions before it can be effectively debunked.[32]

Recent elections have provided stark examples of this threat. Shortly before the 2024 New Hampshire primary, an AI-generated robocall mimicking President Joe Biden's voice urged voters not to participate in the election, a clear act of voter suppression.[8] During the Republican primary, a campaign shared fake AI-generated images of a rival candidate in a compromising context.[6] In India's 2024 election, deepfake videos of popular Bollywood actors appearing to criticize the Prime Minister, and of a senior minister making a false statement about affirmative action, circulated widely, prompting police action.[33] This threat is not limited to domestic actors; foreign adversaries, including state-sponsored groups from Russia and China, have been found to use AI-generated content to spread disinformation, stoke conspiracy theories, and sow chaos in the elections of other nations.[36]

4.2 Algorithmic Manipulation and Voter Suppression Tactics

Beyond the creation of overtly false content, AI can be deployed for more subtle forms of manipulation and suppression. Malicious actors can use AI tools to generate and distribute convincingly false messages about the logistics of voting, such as incorrect polling locations, dates, or times, with the specific intent of disenfranchising targeted groups of voters.[8]

A particularly grave concern is the potential for AI to be used to exacerbate existing inequalities in the democratic process. There is a significant risk that AI-driven disinformation and suppression campaigns will be disproportionately aimed at minority communities, such as Black and brown voters in the United States, who already face numerous systemic barriers to political participation.[8] By tailoring discouraging or misleading messages to these specific communities, AI could become a powerful tool for modern-day, digital voter suppression.

4.3 Erosion of Public Trust and the "Liar's Dividend"

Perhaps the most insidious long-term danger posed by the proliferation of synthetic media is not the success of any single piece of disinformation, but the systemic corrosion of public trust in the entire information ecosystem. In an environment saturated with convincing fakes, voters may reach a point of cognitive exhaustion where they "won't believe what they see or hear," abandoning fact-based reasoning in favor of pre-existing biases, emotion, and partisan affiliation.[29]

This erosion of a shared factual reality gives rise to the "liar's dividend": the ability of dishonest political actors to dismiss genuine, verifiable evidence of their own misconduct or corruption by falsely claiming it is a "deepfake".[4] This tactic was observed during the 2024 U.S. election cycle, where candidates attempted to deflect criticism by claiming that real, unaltered videos of their public gaffes were AI-generated fabrications.[10] This phenomenon threatens to create a state of "epistemic chaos," where accountability becomes impossible because objective truth is rendered contestable. While research suggests that AI-generated disinformation has not yet been proven to measurably alter an election outcome, its documented effect is to shape public discourse, amplify harmful narratives, and entrench political polarization.[9] This degradation of the information environment is a direct threat to the deliberative processes upon which

democracy depends.

4.4 Privacy in Peril: Voter Data Exploitation and Surveillance

The engine of AI-driven political campaigning is data—vast quantities of personal data about voters. This data is often collected, aggregated, and used without the full, informed consent of individuals.[1] Modern campaigns construct comprehensive "political dossiers" on millions of voters, combining public electoral rolls with a trove of commercially available data, including purchasing habits, online browsing history, social media activity, and location data.[24]

The Cambridge Analytica scandal remains the quintessential example of this threat. The firm's exploitation of a third-party Facebook application to harvest the personal data of up to 87 million users, which was then used to build psychological profiles for political targeting, exposed the profound privacy vulnerabilities inherent in the digital ecosystem.[3] This practice raises fundamental questions about data protection and the right to privacy in the political context. The use of personal data to identify and exploit individual psychological vulnerabilities for political gain blurs the line between persuasion and manipulation, turning the machinery of digital surveillance into a tool of electoral influence.

5. The Regulatory Landscape in India

As the world's largest democracy, India's approach to regulating AI in elections serves as a critical case study. Its response is characterized by a unique blend of proactive measures from its independent electoral body, the application of existing legal statutes to new technological harms, and an ongoing, often-conflicted debate about the need for comprehensive, AI-specific legislation.

5.1 The Election Commission of India's Proactive Stance: Advisories on Labeling and the Model Code of Conduct

The Election Commission of India (ECI), a constitutional body tasked with conducting free and fair elections, has taken a leading role in addressing the challenges of AI. Rather than waiting for parliamentary legislation, the ECI has adopted a proactive, advisory-led approach. Recognizing the growing influence of AI in shaping public opinion, the ECI issued a series of advisories ahead of and during the 2024 Lok Sabha elections.[39]

A key directive mandates that all political parties, candidates, and campaigners prominently label any AI-generated or synthetically altered content—including images, videos, and audio—with clear notations such as “AI-Generated,” “Digitally Enhanced,” or “Synthetic Content”.[39] This measure is aimed at enhancing transparency and allowing voters to identify machine-generated content. These advisories built upon earlier guidelines that directed parties to refrain from using deepfakes or other distorted content that could disrupt the level playing field.[39] The ECI has also explicitly affirmed that the Model Code of Conduct (MCC), a set of norms agreed upon by political parties for ethical campaigning, applies to all online content, including social media posts and digital advertisements.[42] To add teeth to these directives, the ECI has instructed political parties to promptly remove any violative content within three hours of it being brought to their notice, warning that violations would be dealt with firmly.[43]

This reliance on "soft law" in the form of advisories from an independent constitutional body allows for a flexible and rapid response to emerging technological threats. However, it also creates a degree of legal uncertainty, as these advisories lack the full statutory weight and prescribed penalties of a parliamentary act, making their enforcement dependent on the ECI's institutional authority and willingness to act.

5.2 Applicability of Existing Laws

In the absence of a specific law governing AI or deepfakes, India's legal response relies on the application and interpretation of existing statutes to address new forms of digital harm.

5.2.1 The Information Technology Act, 2000

The IT Act, 2000, along with its subsequent rules, provides the primary legal framework for regulating cyberspace in India. Several of its provisions are applicable to the malicious use of AI-generated content:

- **Section 66D (Cheating by personation):** This section criminalizes the act of cheating by impersonating someone through a computer resource. It is directly applicable to deepfakes that are used to fraudulently impersonate a political candidate or public figure to deceive voters.[44]
- **Section 66E (Violation of privacy):** This provision penalizes the non-consensual capture, publication, or transmission of an image of a person's private areas. While its scope is specific, it could be invoked in cases where deepfakes are used to create non-consensual intimate imagery of political opponents, a tactic that disproportionately targets female politicians.[44]
- **Sections 67 and 67A (Obscene and sexually explicit content):** These sections provide penalties for publishing or transmitting obscene or sexually explicit material in electronic form and are relevant for prosecuting the use of deepfakes to create pornographic content.[45]
- **IT Rules, 2021:** The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, impose due diligence obligations on social media intermediaries. They are required to remove unlawful content, including deepfakes that violate existing laws, upon receiving a court order or notification from a government agency.[46]

5.2.2 The Representation of the People Act, 1951 (RPA)

The RPA, 1951, is the cornerstone of India's electoral law, and its provisions on "corrupt practices" offer a potent, if judicially untested, avenue for regulating AI-driven campaigns. The challenge lies in applying definitions crafted for an analog world to the nuances of digital manipulation.

- **Section 123(4) (Publication of false statements):** This clause defines it as a corrupt practice for a candidate or their agent to publish any statement of fact that is false and which they believe to be false, in relation to the personal character or conduct of any candidate, to prejudice that candidate's election prospects.[48] A deepfake video depicting a candidate in a fabricated scandal or making a false statement would almost certainly fall under this provision. An election can be declared void if a candidate is found guilty of such a practice.[50]
- **Section 123(2) (Undue influence):** This provision prohibits any "direct or indirect interference or attempt to interfere... with the free exercise of any electoral right".[48] Historically, this has been interpreted to cover threats of physical harm, social ostracism, or divine displeasure.[48] A strong legal argument can be made that large-scale, psychologically manipulative microtargeting campaigns, which use AI to exploit voters' cognitive biases and vulnerabilities based on their personal data, constitute a form of "indirect interference" with their right to make a free and informed choice.
- **Section 123(3) (Appeals on grounds of religion, race, caste, etc.):** This section prohibits appeals to vote or refrain from voting on the grounds of religion, race, caste, community, or language.[48] The Supreme Court's landmark judgment in *Abhiram Singh v. C.D. Commachen* (2017) significantly broadened the interpretation of this section, ruling that *any* appeal to religion, caste, etc., in an election is a corrupt practice.[51] This makes the provision highly relevant to AI-generated content designed to promote enmity or hatred between different communities for electoral gain, such as the Hindu supremacist ads reportedly approved by Meta during the 2024 election.[27]

5.3 The Path Forward: The Proposed Digital India Act and Regulatory Debates

The Indian government's official stance on AI regulation has been characterized by a degree of strategic ambiguity. Initially, it adopted a "pro-innovation" approach, with statements suggesting that no specific law to regulate AI was being considered.[54] However, this hands-off posture has evolved in response to growing concerns.

The blueprint for a new, comprehensive Digital India Act, intended to replace the aging IT Act of 2000, explicitly includes provisions for the "regulation of high-risk AI systems".[54] Concurrently, the Ministry of Electronics and Information Technology (MeitY) has issued reactive advisories, such as one in March 2024 that initially mandated government permission for the deployment of "under-tested" AI models. This move was met with strong industry pushback and was subsequently revised, highlighting the ongoing tension between the desire to regulate and the fear of stifling innovation.[12] The current debate within Indian policy circles revolves around whether to pursue a comprehensive, omnibus AI law, amend existing legislation like the IT Act, or continue with a sector-specific, risk-based approach.[54] This reactive and experimental phase of AI governance underscores the complexity of crafting durable policy in a rapidly changing technological landscape.

6. International Regulatory Frameworks: A Comparative Analysis

The global response to the challenge of AI in elections is far from uniform, reflecting diverse legal traditions, constitutional principles, and policy priorities. A comparative analysis of the approaches taken by the European Union, the United States, and through international cooperative efforts reveals a spectrum of regulatory philosophies, from comprehensive, rights-based legislation to a fragmented, disclosure-focused patchwork.

Table 1: Comparative Analysis of AI Election Regulations

Feature	India	European Union	United States
Primary Approach	Advisory-led, reliance on existing laws	Comprehensive, risk-based legislation (legally binding)	Fragmented, state-led, disclosure-focused, federal inaction
Key Legal Instrument	ECI Advisories, IT Act 2000, Representation of the People Act 1951	EU AI Act, General Data Protection Regulation (GDPR)	State-level deepfake laws, FCC robocall ban
Regulation of Deepfakes	Labeling required by ECI advisory; prosecution under existing laws (e.g., defamation, impersonation)	Transparency obligation (labeling); manipulative AI is prohibited if it causes harm	Disclosure required or outright prohibition in some states close to an election
Data Privacy Rules	Digital Personal Data Protection Act (DPDP Act) 2023	GDPR (strict rules on sensitive data like political opinions)	No comprehensive federal privacy law; varies by state (e.g., CCPA in California)
Enforcement Body	Election Commission of India (ECI), Police (under IPC/IT Act)	National supervisory authorities, European AI Board	State Attorneys General, Federal Election Commission (limited scope)

6.1 The European Union's Comprehensive Approach: The AI Act and GDPR

The European Union has adopted the most comprehensive and proactive regulatory stance globally, anchored in two landmark pieces of legislation that work in tandem to govern AI and data use in the political sphere.

6.1.1 The EU AI Act

The EU AI Act is the world's first omnibus legal framework for artificial intelligence, establishing a clear set of rules based on the level of risk an AI system poses.[55] Its provisions are directly relevant to electoral integrity:

- **Prohibited AI Practices:** The Act outright bans certain AI systems deemed to pose an "unacceptable risk." This includes AI that deploys "subliminal, manipulative, or deceptive techniques to distort behaviour and impair informed decision-making, causing significant harm".[2] This prohibition directly targets the kind of psychologically manipulative advertising that could be used in political campaigns.[55]
- **High-Risk AI Systems:** The Act classifies AI systems "intended to be used for influencing the outcome of an election or referendum" as "high-risk".[55] This classification does not ban their use but subjects them to a stringent set of obligations before they can be deployed in the EU market. These requirements include conducting rigorous risk assessments, ensuring high-quality and representative data governance to prevent bias, maintaining detailed technical documentation, enabling human oversight, and ensuring high levels of accuracy and cybersecurity.[55]

- **Transparency Obligations:** For AI systems that interact with humans, such as chatbots, or that generate synthetic content, the Act imposes transparency rules. Users must be made aware that they are interacting with an AI, and any "deepfake" or other manipulated content must be clearly labeled as artificially generated.[55]

6.1.2 The General Data Protection Regulation (GDPR)

While not an AI-specific law, the GDPR is arguably one of the most powerful tools for regulating AI-driven political campaigns because it governs their essential fuel: personal data.

- The GDPR establishes strict rules for the collection, processing, and storage of personal data, requiring a clear and lawful basis for any such activity.[58] For political campaigns, this creates significant hurdles for the kind of large-scale, indiscriminate data harvesting that characterized the Cambridge Analytica scandal.[59]
- Crucially, the GDPR classifies "political opinions" as a special category of sensitive personal data. Processing such data is generally prohibited unless the individual has given explicit, unambiguous consent.[58] This provision makes it extremely difficult for campaigns to legally build the kind of detailed psychographic voter profiles used for microtargeting without direct and informed permission from each voter.[60]

6.2 The United States' Patchwork System: Federal Inaction and State-Level Legislation

In stark contrast to the EU's centralized approach, the United States' regulatory landscape is a fragmented patchwork, characterized by a lack of comprehensive federal legislation and a flurry of activity at the state level.

- **Federal Level:** To date, no overarching federal law has been enacted to specifically regulate the use of AI in political campaigns.[56] Federal agencies have taken limited, targeted actions. The Federal Communications Commission (FCC) has outlawed the use of AI-generated voices in robocalls, a direct response to the fake Biden call in New Hampshire.[8] The Federal Election Commission (FEC) has clarified that its existing regulation against "fraudulent misrepresentation" of candidates applies to AI-generated advertisements. However, the FEC has declined to issue broader rules on AI, with a majority of

commissioners believing they lack the legislative authority from Congress to do so.[63]

- **State Level:** In the void left by federal inaction, numerous states have passed their own laws. At least 26 states have enacted legislation specifically targeting the use of political deepfakes.[64] These state laws generally follow two main models:
  - **Disclosure:** The most common approach is to require a clear disclaimer on any "materially deceptive media" that is generated by AI and published within a specific timeframe before an election (e.g., 60, 90, or 120 days).[64]
  - **Prohibition:** A smaller number of states, including Minnesota and Texas, have taken a stricter approach, outright prohibiting the publication of deceptive deepfakes intended to harm a candidate or influence an election within a certain pre-election window.[64]
  - Most of these laws provide for civil remedies, allowing an aggrieved candidate to seek an injunction to stop the dissemination of the deepfake and to sue for damages.[64]

6.3 Global Cooperation and Self-Regulation: The 'Tech Accord to Combat Deceptive Use of AI'

Alongside government regulation, a significant development has been the emergence of industry self-regulation. The most prominent example is the "Tech Accord to Combat Deceptive Use of AI in 2024 Elections," signed in February 2024 at the Munich Security Conference.[2]

- This voluntary agreement brings together over 20 of the world's leading technology companies, including Google, Meta, Microsoft, OpenAI, and TikTok.[65]
- The signatories have pledged to work collaboratively to counter harmful, deceptive AI-generated content related to elections. Their commitments include developing and sharing technology to detect and address such content, providing transparency about their policies, and supporting public awareness and media literacy campaigns.[65]
- While lauded as a positive and necessary step towards industry accountability, the accord's effectiveness is limited by its voluntary nature. Critics point out that such self-regulatory frameworks lack robust, independent enforcement mechanisms and penalties for non-compliance, making their real-world impact dependent on the goodwill and proactive efforts of the signatory companies.[66]

7. Analysis of Key Case Laws and Incidents

An examination of specific real-world incidents and the legal responses they provoked provides crucial context for understanding the practical challenges and implications of regulating AI in elections. These case studies illustrate the evolution of data-driven manipulation, the dual-use nature of AI in practice, and the role of the judiciary in shaping regulatory action.

7.1 Case Study 1: The Cambridge Analytical Scandal - A Precedent for Data-Driven Manipulation

The scandal involving Cambridge Analytical and Facebook serves as the foundational case study for data-driven electoral manipulation in the digital age.

- **Facts of the Case:** Cambridge Analytical, a British political consulting firm, gained access to the personal data of up to 87 million Facebook users without their explicit consent.[38] This was accomplished through a third-party personality quiz app, "This Is Your Digital Life," which not only collected data from its users but also scraped the data of their entire friend networks, a feature then permitted by Facebook's platform policies.[38] The harvested data—including profile information, page likes, and even private messages in some cases—was used to construct detailed psychographic profiles of voters. These profiles were then leveraged to create and deliver micro targeted political advertisements designed to influence voter behavior in the 2016 U.S. presidential election for the Trump campaign and in the UK's Brexit referendum.[3]

- **Legal and Regulatory Aftermath:** The public outcry following the revelations in 2018 led to significant legal and regulatory consequences. The U.S. Federal Trade Commission (FTC) imposed a landmark $5 billion fine on Facebook (now Meta) for violating a 2012 consent decree related to user privacy.[38] The company also faced a £500,000 fine from the UK's Information Commissioner's Office.[38] In addition to regulatory penalties, Meta agreed to pay $725 million to settle a class-action lawsuit brought by users whose data was improperly shared.[67] A separate shareholder lawsuit, which alleged that company executives mishandled the scandal, was also settled.[68]
- **Significance:** The Cambridge Analytical affair was a watershed moment. It provided a concrete, large-scale example of how personal data, when combined with data analytics, could be weaponries for political purposes. It starkly exposed the vulnerabilities of social media platforms and the inadequacy of existing data protection regimes, serving as a major catalyst for the global debate on digital privacy and directly influencing the push for stronger regulations like the EU's GDPR.[3] It established a clear precedent for the potential harms of data-driven manipulation, setting the stage for the even greater challenges now posed by generative AI.

7.2 Case Study 2: The 2024 Indian General Election - AI as a Double-Edged Sword

The 2024 Indian general election was the world's largest democratic exercise and the first major election to be conducted in the era of widespread generative AI. It provided a comprehensive, real-world laboratory for observing AI's dual-use nature in a high-stakes political contest, with parties reportedly spending an estimated $50 million on AI-generated content.[17]

- **Constructive and Innovative Uses:** Political parties harnessed AI for a range of constructive purposes aimed at enhancing voter outreach and accessibility.
  - Prime Minister Narendra Modi's campaign famously used the 'Bhashini' AI tool to provide real-time translations of his Hindi speeches into multiple regional languages, breaking down linguistic barriers.[17]
  - Parties across the spectrum used AI voice-cloning to send personalized phone calls and WhatsApp messages to millions of voters, addressing them by name and discussing local issues.[17]
  - In a more novel application, deepfake technology was used to "resurrect" deceased and widely revered political leaders, such as M. Karunanidhi in Tamil Nadu, to have them deliver posthumous endorsements for their parties.[30]
- **Malicious and Deceptive Uses:** The election was also rife with the malicious use of AI to create and spread disinformation.
  - Deepfake videos of prominent Bollywood actors, including Ranveer Singh and Aamir Khan, were circulated, showing them appearing to criticize Prime Minister Modi or endorse the opposition.[33]
  - A particularly impactful deepfake featured Home Minister Amit Shah, where his words were altered to make it seem as though he was advocating for the removal of affirmative action policies for certain communities, a highly sensitive issue in India.[34]
  - Political parties also engaged in creating satirical deepfakes to mock their opponents, such as a video showing a jailed opposition leader singing a Bollywood song.[27]
- **Regulatory Response in Action:** This flood of synthetic media prompted a real-time response from Indian authorities. The Election Commission of India issued its advisories on labeling AI content during this period.[39] More consequentially, police in several states made arrests related to the creation and dissemination of deepfakes, particularly the one involving Home Minister Shah. Notably, many of those arrested were affiliated with opposition parties, raising concerns among observers about the potential for selective or politically motivated enforcement of laws against digital content.[26]

- **Significance:** The Indian election is the most significant case study to date of AI's complex role in a democratic contest. It demonstrated that AI is not merely a hypothetical threat but a practical tool being actively deployed for both inclusive communication and potent disinformation.[27] The experience highlighted the challenges of regulation in a fast-moving, politically charged environment, including the critical issue of ensuring impartial enforcement.

7.3 Case Study 3: *Lawyers Voice v. Union of India* - The Role of the Judiciary in Compelling Regulatory Action

This case from the Delhi High Court illustrates the crucial role that judicial intervention and civil society activism can play in pushing regulatory bodies to address new technological threats.

- **Facts of the Case:** In the midst of the 2024 Lok Sabha elections, a Public Interest Litigation (PIL) was filed in the Delhi High Court by the organization 'Lawyers Voice'.[35] The petition sought urgent directions for the ECI and the Union Government to formulate and implement guidelines to regulate the pervasive use of deepfake technologies in political campaigns. The plea argued that the rapid spread of manipulated videos posed a serious threat to a free and fair election and that the existing legal framework was insufficient to address this harm.[35]
- **Court's Decision and Rationale:** The High Court bench, led by the Acting Chief Justice, acknowledged the gravity and urgency of the issue. While it ultimately refrained from issuing a direct judicial order (a writ of mandamus) to the ECI—citing the impropriety of judicial intervention in the middle of an ongoing election process—it did not dismiss the concerns.[35] Instead, the court adopted a posture of judicial persuasion. It directed the ECI to treat the petition as a formal representation and to decide on the matter expeditiously, setting a firm deadline of May 6, 2024.[72] During the hearing, the ECI's counsel assured the court that the commission was already taking action, including having deepfake videos removed and filing criminal complaints against the perpetrators.[35]
- **Significance:** This case is significant for several reasons. First, it demonstrates a viable pathway for civil society to use the legal system to hold regulatory bodies accountable for inaction on emerging technological threats. Second, it shows the judiciary's recognition of deepfakes as a "serious menace" to society and the democratic process.[73] Third, the court's approach—directing the expert regulatory body to act within its mandate rather than legislating from the bench—reflects a principle of judicial restraint while still achieving the goal of prompting swift regulatory attention. The case underscores a functional, if sometimes reactive, interplay between civil society, the judiciary, and electoral bodies in the governance of election technology.

8. Core Challenges in Regulation

Crafting effective, durable, and rights-respecting regulations for AI in elections is a formidable task, fraught with technical, legal, and ethical complexities. These challenges help explain the divergent and often cautious approaches taken by governments worldwide and point to the need for a nuanced, multi-faceted solution.

8.1 Technical Challenges: The Arms Race of Detection and Generation

The primary technical hurdle in regulating AI-generated content is the asymmetrical pace of technological development. The capabilities of generative AI models are advancing exponentially, making the creation of high-fidelity, convincing synthetic media easier, faster, and cheaper.[5] In contrast, the development of reliable tools to detect this synthetic content lags significantly behind.

As AI models become more sophisticated, the subtle artifacts that once betrayed a deepfake—such as unnatural blinking, distorted backgrounds, or an extra finger—are rapidly disappearing.[31] This leads to a perpetual "arms race" between content generation and content detection, a race in which the generators currently have a distinct advantage.[74] This asymmetry places an enormous burden on social media platforms, fact-checkers, and regulatory bodies, who are tasked with identifying and moderating a potential deluge of fabricated content that is increasingly indistinguishable from reality to both human eyes and detection algorithms.[20] This technical reality means that any regulatory strategy based solely on detection and removal is likely to fail.

8.2 Legal and Jurisdictional Hurdles: The "Pacing Problem" and Enforcement Across Borders

The legal challenges are equally daunting, centered on the inherent mismatch between the speed of technological change and the pace of lawmaking, as well as the borderless nature of the internet.

- **The "Pacing Problem":** The legislative process is, by design, slow and deliberative. Crafting a law requires consultation, debate, and consensus-building. AI technology, however, evolves at a breakneck speed. This creates a "pacing problem," where legislation designed to address a specific technology (e.g., a particular type of deepfake) may be obsolete by the time it is enacted.[54] This risk encourages policymakers to either draft technologically-neutral but potentially vague laws, or to avoid legislation altogether in favor of more flexible but less enforceable advisories.
- **Jurisdictional Complexity:** Disinformation campaigns are frequently transnational. A deepfake video targeting an Indian election could be created by a state-sponsored group in Russia, use servers hosted in a third country, and be disseminated via a social media platform headquartered in the United States.[9] This makes legal enforcement exceptionally difficult. Which country's laws apply? How can evidence be gathered and perpetrators be brought to justice across international borders? The fragmented global regulatory landscape, with different countries adopting vastly different rules, exacerbates this problem, creating legal loopholes and safe havens for malicious actors.[15]

8.3 Ethical and Constitutional Dilemmas: Navigating Regulation, Censorship, and Freedom of Expression

Perhaps the most fundamental challenge is balancing the compelling need to protect electoral integrity against the equally important imperative to uphold fundamental rights, particularly the right to freedom of expression.

- In democracies with strong constitutional protections for speech, such as the United States with its First Amendment, any regulation of political communication faces a high legal bar.[63] Courts will strictly scrutinize laws that restrict political speech, even if that speech is false or misleading.
- There exists a fine and often blurry line between malicious disinformation and legitimate forms of political expression, such as satire, parody, or sharp-edged criticism.[9] An overly broad law aimed at banning "deceptive" content could inadvertently criminalize political cartoons or satirical videos, chilling protected speech and giving incumbent governments a tool to suppress dissent.[14]
- Many proposed regulations hinge on the "intent" of the creator or disseminator—for example, whether a deepfake was created with the "intent to deceive." Proving subjective intent in a court of law is notoriously difficult. A piece of satirical content, created without malicious intent, could be stripped of its context and shared by others with the intent to mislead, complicating questions of legal liability.[9]

These challenges create a regulatory "trilemma," where policymakers must make difficult trade-offs between three competing goals: (1) effectiveness in preventing harm, (2) protection of fundamental rights like free speech, and (3) technological neutrality to ensure laws are not quickly outdated. The EU's AI Act prioritizes harm prevention, potentially at some cost to innovation and speech. The U.S. approach

prioritizes free speech, leading to a less effective and fragmented response. India's hybrid model seeks flexibility but struggles with legal certainty. This trilemma explains why there is no simple, one-size-fits-all solution, and why the most robust approaches will likely be hybrid models that combine different strategies to navigate these inherent tensions.

9. Suggestions and Recommendations

Addressing the multifaceted challenges posed by AI in elections requires a comprehensive, multi-stakeholder approach that combines legislative reform, regulatory action, industry accountability, and public empowerment. No single solution will suffice; instead, an ecosystem of mutually reinforcing measures is needed to build resilience and safeguard democratic integrity.

9.1 Strengthening the Legal Framework: A Hybrid Approach

Governments must update their legal frameworks to explicitly address the harms enabled by new technologies, moving beyond the interpretation of outdated statutes.

- **In India, a two-pronged legislative reform is recommended:**

1. **Amend the Representation of the People Act, 1951:** The definition of "corrupt practices" in Section 123 should be modernized.
   - **Section 123(2) on "undue influence"** should be amended to explicitly include the use of personal data for psychologically manipulative microtargeting and the large-scale, automated dissemination of disinformation intended to interfere with the free exercise of electoral rights.
   - **Section 123(4) on "publication of false statements"** should be amended to specifically name digitally altered, AI-generated, or synthetic media as a medium for such publications, removing any legal ambiguity.
2. **Amend the Information Technology Act, 2000:** A new, specific, and bailable offense should be created for the malicious creation and/or dissemination of materially deceptive synthetic media (deepfakes) within an electoral context. The provision should clearly define "malicious intent" to protect satire and parody, and establish clear penalties that are proportionate to the harm caused.

9.2 A Multi-Stakeholder Model: Defining Roles and Responsibilities

Protecting elections is a shared responsibility that cannot fall to any single entity. A collaborative framework is essential.

- **Electoral Bodies (e.g., ECI):** These bodies should be empowered as the primary regulators of campaign conduct in the digital sphere. In India, this means moving from the current Voluntary Code of Ethics to a legally binding **Model Code of Conduct for Digital Platforms and Political Parties**, developed through a transparent and participatory process.[76] These bodies should also establish rapid response teams to monitor the information environment during election periods and swiftly counteract false narratives with credible information.[14]
- **Government and Legislatures:** The primary role of government is to enact clear and enforceable laws. This includes passing legislation that explicitly outlaws all forms of voter suppression, whether digital or physical.[13] Furthermore, governments must adequately fund the law enforcement agencies tasked with investigating digital crimes and provide resources for broad-based public digital literacy programs.[13]
- **Technology Platforms:** Social media companies and AI model developers must assume greater accountability. This requires moving beyond voluntary accords to concrete actions, including:
  - **Radical Transparency:** Maintaining publicly accessible, comprehensive, and searchable archives of all political advertisements, including targeting data.[13]

- **Robust Enforcement:** Proactively and consistently enforcing their own policies against manipulated media, inauthentic accounts (bots), and coordinated influence operations.[64]
- **Localized Moderation:** Investing in content moderation and policy enforcement teams with deep local and linguistic expertise, particularly in non-Western countries, to understand cultural context and effectively combat region-specific harms.[77]

- **Civil Society and Media:** Non-governmental organizations, fact-checking groups, and independent media are the frontline defenders against disinformation. They play a crucial role in monitoring campaigns, verifying content, and educating the public. Supporting these organizations, such as India's Deepfakes Analysis Unit (DAU) which provides a public tipline for content verification, is a critical investment in democratic resilience.[76]

9.3 Mandating Radical Transparency

"Sunlight is the best disinfectant." Mandating transparency in the use of AI and data in campaigns is a powerful regulatory tool that empowers voters and researchers without resorting to censorship.

- **Content Labeling:** Regulations should mandate clear, prominent, and standardized disclaimers on all political advertising that is synthetically generated or significantly altered by AI. Simple "AI-Generated" labels are a start, but more informative labels that specify the nature of the alteration are preferable.[64]
- **Algorithmic and Data Transparency:** Campaigns using AI for voter microtargeting should be required to disclose this fact, along with the general categories of data being used to segment voters. Platforms, in turn, must provide users and researchers with greater insight into why they are being shown a particular political ad.
- **Financial Transparency:** Election laws must be updated to require campaigns to report all spending on AI tools, data brokers, and digital consultants. This financial trail is essential for understanding the modern campaign ecosystem and holding actors accountable.[13]

9.4 Banning Malicious Use-Cases

While broad censorship is dangerous, a narrow set of the most malicious and indefensible uses of AI in elections should be subject to outright prohibition. These are applications where the threat to democratic integrity is so severe, and the value as legitimate speech is so negligible, that a bright-line ban is justifiable.[75] Such a ban should cover:

- **AI-generated content that impersonates election officials** to distribute false administrative information.
- **Deceptive AI content designed to mislead voters about the time, place, or manner of voting**, which constitutes direct voter suppression.
- **The use of AI to generate and disseminate non-consensual sexually explicit imagery of political candidates or their families**, a vile tactic of harassment that disproportionately targets women and is intended to drive them from public life.[77]

9.5 Fostering Resilience: Investing in Digital Literacy and Critical Thinking

Ultimately, the most durable defense against disinformation is a skeptical, discerning, and informed citizenry. Regulation and technology can only go so far; the human element is paramount.

- Governments, educational institutions, and civil society organizations must make a sustained, long-term investment in **public education and digital media literacy programs**.[13]
- These initiatives should begin in primary and secondary education and extend to adult learning programs. They must equip citizens with the critical thinking skills needed to evaluate online information, identify the hallmarks of manipulation, understand the economic and political incentives behind the

content they consume, and practice good information hygiene (e.g., checking sources before sharing).[29] A resilient public is the ultimate safeguard for a resilient democracy.

10. Conclusion

The integration of Artificial Intelligence into political campaigning represents a fundamental and irreversible transformation of the democratic process. This paper has detailed the dualistic nature of this technology. On one hand, AI offers powerful tools to enhance voter engagement, overcome linguistic barriers, and improve campaign efficiency, potentially making democracy more accessible and responsive. On the other, it provides an unprecedented arsenal for spreading disinformation, manipulating public opinion through invasive micro targeting, and eroding the very foundations of public trust. The shift from capital-intensive analytical AI to widely accessible generative AI has democratized the means of influence, fundamentally altering the landscape of political communication and creating challenges that existing legal and ethical frameworks are ill-equipped to handle.

The analysis of regulatory responses in India, the European Union, and the United States reveals that there is no single, perfect solution. The EU's comprehensive, rights-based model offers legal clarity but faces challenges of adaptability. The US's fragmented, speech-protective approach avoids censorship but leaves the electorate vulnerable. India's flexible, advisory-led model allows for rapid response but lacks statutory certainty. This paper concludes that an effective path forward lies not in choosing one model, but in synthesizing the strengths of each. A coherent regulatory ecosystem is imperative—one that is technologically aware, legally robust, and steadfastly committed to upholding fundamental rights. This requires a multi-layered strategy that combines targeted amendments to hard law, co-regulation and mandatory transparency for technology platforms, proactive enforcement by independent electoral bodies, and sustained investment in societal resilience.

The challenge of regulating AI in elections is a microcosm of a much larger question facing democratic societies in the 21st century: how can we sustain a deliberative, truth-based public sphere in an information environment that is increasingly saturated with algorithmically generated, personalized, and often manipulative content? The battle to preserve electoral integrity is not merely about thwarting the next deepfake or penalizing a malicious actor. It is about actively redesigning our informational and political systems for a new technological reality. It requires a renewed commitment to the principles of transparency, accountability, and an informed citizenry. Failure to rise to this challenge risks a future where democratic discourse is irrevocably degraded, and the free and fair election—the cornerstone of self-government—becomes a casualty of the algorithmic age. The task ahead is not simply to regulate a technology, but to fortify democracy itself.

Works cited

1. (PDF) ARTIFICIAL INTELLIGENCE IN POLITICAL CAMPAIGNS - ResearchGate, accessed on October 18, 2025, https://www.researchgate.net/publication/380554615_ARTIFICIAL_INTELLIGENCE_IN_POLITICAL_CAMPAIGNS
2. The use of AI in elections - Eurac Research, accessed on October 18, 2025, https://www.eurac.edu/en/blogs/eureka/the-use-of-ai-in-elections
3. The persuasive effects of political microtargeting in the age of ..., accessed on October 18, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC10849795/
4. The impact of generative AI in a global election year - Brookings Institution, accessed on October 18, 2025, https://www.brookings.edu/articles/the-impact-of-generative-ai-in-a-global-election-year/
5. How AI Puts Elections at Risk — And the Needed Safeguards | Brennan Center for Justice, accessed on October 18, 2025, https://www.brennancenter.org/our-work/analysis-opinion/how-ai-puts-

elections-risk-and-needed-safeguards
6. Generative AI in Political Advertising | Brennan Center for Justice, accessed on October 18, 2025, https://www.brennancenter.org/our-work/research-reports/generative-ai-political-advertising
7. The dangers posed by AI and disinformation during elections - Brookings Institution, accessed on October 18, 2025, https://www.brookings.edu/events/the-dangers-posed-by-ai-and-disinformation-during-elections/
8. How Artificial Intelligence Influences Elections and What We Can Do About It, accessed on October 18, 2025, https://campaignlegal.org/update/how-artificial-intelligence-influences-elections-and-what-we-can-do-about-it
9. AI-Enabled Influence Operations: Safeguarding Future Elections ..., accessed on October 18, 2025, https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-safeguarding-future-elections
10. Did artificial intelligence shape the 2024 US election? - Al Jazeera, accessed on October 18, 2025, https://www.aljazeera.com/news/2024/12/25/did-artificial-intelligence-shape-the-2024-us-election
11. Artificial intelligence, democracy and elections - European Parliament, accessed on October 18, 2025, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/751478/EPRS_BRI(2023)751478_EN.pdf
12. Elections, Accountability, and Democracy in the Time of A.I., accessed on October 18, 2025, https://www.orfonline.org/research/elections-accountability-and-democracy-in-the-time-of-a-i
13. A policy framework to govern the use of generative AI in political ads - Brookings Institution, accessed on October 18, 2025, https://www.brookings.edu/articles/a-policy-framework-to-govern-the-use-of-generative-ai-in-political-ads/
14. The Effect of AI on Elections Around the World and What to Do About It | Brennan Center for Justice, accessed on October 18, 2025, https://www.brennancenter.org/our-work/analysis-opinion/effect-ai-elections-around-world-and-what-do-about-it
15. AI Watch: Global regulatory tracker - United States | White & Case LLP, accessed on October 18, 2025, https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states
16. AI in Political Campaigns: How it's being used and the ethical considerations it raises, accessed on October 18, 2025, https://mediarelations.gwu.edu/ai-political-campaigns-how-its-being-used-and-ethical-considerations-it-raises
17. India's Experiments With AI in the 2024 Elections: The Good, The Bad & The In-between, accessed on October 18, 2025, https://www.techpolicy.press/indias-experiments-with-ai-in-the-2024-elections-the-good-the-bad-the-inbetween/
18. India's latest election embraced AI technology. Here are some ways ..., accessed on October 18, 2025, https://www.pbs.org/newshour/world/indias-latest-election-embraced-ai-technology-here-are-some-ways-it-was-used-constructively
19. Microtargeting and Data Analytics: Transforming Political Campaigns - Hearst Bay Area, accessed on October 18, 2025, https://marketing.sfgate.com/blog/microtargeting-and-data-analytics-transforming-political-campaigns
20. Political microtargeting deepens social divides – and AI is making it easier - Universiteit van Amsterdam, accessed on October 18, 2025, https://www.uva.nl/shared-content/uva/en/news/news/2025/07/political-microtargeting-deepens-social-divides---and-ai-is-making-it-easier.html
21. How Sentiment Analysis Can Help Election Campaigns - NetOwl, accessed on October 18, 2025, https://www.netowl.com/how-sentiment-analysis-can-help-election-campaigns
22. Artificial Intelligence and Sentiment Analysis in Political Campaigns | Request PDF, accessed on October 18, 2025, https://www.researchgate.net/publication/390526300_Artificial_Intelligence_and_Sentiment_Analysis_in_Political_Campaigns
23. Political Sentiment Analysis: How It Works - Insight7 - Call Analytics & AI Coaching for Customer Teams, accessed on October 18, 2025, https://insight7.io/political-sentiment-analysis-how-it-works/
24. CANDIDATE AI: THE IMPACT OF ARTIFICIAL INTELLIGENCE ON ELECTIONS, accessed on October 18, 2025, https://news.emory.edu/features/2024/09/emag_ai_elections_25-09-2024/index.html

25. Using AI for Political Polling - Ash Center, accessed on October 18, 2025, https://ash.harvard.edu/articles/using-ai-for-political-polling/
26. Indian Elections AI Usage, accessed on October 18, 2025, https://6068438.fs1.hubspotusercontent-na1.net/hubfs/6068438/indian-elections-ai-usage.pdf
27. Deep Fakes, Deeper Impacts: AI's Role in the 2024 Indian General ..., accessed on October 18, 2025, https://gnet-research.org/2024/09/11/deep-fakes-deeper-impacts-ais-role-in-the-2024-indian-general-election-and-beyond/
28. Exploring the Impact of AI on Voter Confidence and Election ... - Qeios, accessed on October 18, 2025, https://www.qeios.com/read/UT898Q
29. AI and the Election — The Link - The Magazine of CMU's School of Computer Science, accessed on October 18, 2025, https://magazine.cs.cmu.edu/ai-and-the-election
30. INDIA'S GENERATIVE AI ELECTION PILOT SHOWS ARTIFICIAL ..., accessed on October 18, 2025, https://mediaengagement.org/wp-content/uploads/2024/10/Indias-Generative-AI-Election-Pilot-Shows-Artificial-Intelligence-In-Campaigns-Is-Here-To-Stay.pdf
31. AI-generated disinformation poses threat of misleading voters in 2024 election | PBS News, accessed on October 18, 2025, https://www.pbs.org/newshour/politics/ai-generated-disinformation-poses-threat-of-misleading-voters-in-2024-election
32. From mass networks to personalised voting - Diálogo Político, accessed on October 18, 2025, https://dialogopolitico.org/special-edition-2025-artificial-democracy/from-mass-networks-to-personalised-voting
33. AI and Deepfakes Played a Big Role in India's Elections - New Lines Magazine, accessed on October 18, 2025, https://newlinesmag.com/spotlight/ai-and-deepfakes-played-a-big-role-in-indias-elections/
34. Shaping Robust AI Regulation: Lessons from India's 'Deepfake' Election, accessed on October 18, 2025, https://theharvardpoliticalreview.com/ai-deepfakes-india-election/
35. PIL and Election Commission of India's Response on Deepfakes - S.S. Rana & Co., accessed on October 18, 2025, https://ssrana.in/articles/pil-eci-response-deepfakes/
36. Midterm elections will likely see increased effects of misinformation ..., accessed on October 18, 2025, https://www.newsfromthestates.com/article/midterm-elections-will-likely-see-increased-effects-misinformation-reduced-federal-security
37. VOTER PRIVACY IN THE AGE OF BIG DATA - Wisconsin Law Review, accessed on October 18, 2025, https://wlr.law.wisc.edu/wp-content/uploads/sites/1263/2015/02/1-Rubinstein-Final-Online.pdf
38. Facebook–Cambridge Analytica data scandal - Wikipedia, accessed on October 18, 2025, https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal
39. Election commission of India embraces AI ethics in campaigning: Advisory on labelling AI-generated content, accessed on October 18, 2025, https://indiaai.gov.in/article/election-commission-of-india-embraces-ai-ethics-in-campaigning-advisory-on-labelling-ai-generated-content
40. Election Commission cautions parties against misuse of AI deepfakes in Bihar elections, accessed on October 18, 2025, https://www.thehindu.com/elections/bihar-assembly/election-commission-cautions-parties-against-misuse-of-ai-deepfakes-in-bihar-elections/article70143502.ece
41. Advisory - Election Commission of India, accessed on October 18, 2025, https://www.eci.gov.in/eci-backend/public/api/download?url=LMAhAK6sOPBp%2FNFF0iRfXbEB1EVSLT41NNLRjYNJJP1KivrUxbfqkDatmHy12e%2FzGjJMI0%2FjETs7fjrM8lYn4ipTqYtDEvVosG8Bae5QB8%2Fj5TBF9Esc2hlzORgYtkmzyKzGsKzKlbBW8rJeM%2FfYFA%3D%3D
42. Don't misuse AI: EC issues warning to political parties ahead of Bihar polls; cautions against deepfakes | India News, accessed on October 18, 2025, https://timesofindia.indiatimes.com/india/dont-misuse-ai-ec-issues-warning-to-political-parties-ahead-of-bihar-polls-cautions-against-deepfakes/articleshow/124404510.cms
43. ECI directs responsible and ethical use of social media platforms by political parties and their representatives - ELECTION COMMISSION OF INDIA, accessed on October 18, 2025, https://elections24.eci.gov.in/docs/5ylWJLjQBX.pdf
44. Handling Cases of Deepfake, accessed on October 18, 2025, https://cawach.gujgov.edu.in/dist/documents/sop/cyberAwareness/Deepfake.pdf

45. Deepfakes & Cyber Law, accessed on October 18, 2025, https://www.asianlaws.org/blog-post.php?url=deepfakes-and-cyber-law
46. Legal Dimensions of Deepfake Technology: Privacy, Consent, and Criminal Liability, accessed on October 18, 2025, https://juriscentre.com/2025/07/27/legal-dimensions-of-deepfake-technology-privacy-consent-and-criminal-liability/
47. Deepfakes in India: Legal Landscape, Judicial Responses, and a Practical Playbook for Enforcement - NeGD - National e-Governance Division, accessed on October 18, 2025, https://negd.gov.in/blog/deepfakes-in-india-legal-landscape-judicial-responses-and-a-practical-playbook-for-enforcement/
48. Corrupt practices - India Code: Section Details, accessed on October 18, 2025, https://www.indiacode.nic.in/show-data?actid=AC_CEN_3_81_00001_195143_1517807327542§ionId=29633§ionno=123&orderno=143
49. Representation of the People Act, 1951 - aptiplus, accessed on October 18, 2025, https://aptiplus.in/blogs/representation-of-the-people-act-1951/
50. Discuss the 'corrupt practices' for the purpose of the Representation of the People Act, 1951. Analyze whether the increase in the assets of the legislators and/or their associates, disproportionate to their known sources of income, would constitute 'undue influence' and consequently a corrupt practice. - StudyIQ, accessed on October 18, 2025, https://www.studyiq.com/articles/discuss-the-corrupt-practices-for-the-purpose-of-the-representation-of-the-people-act-1951-analyze-whether-the-increase-in-the-assets-of-the-legislators-and-or-their-associates-di/
51. Corrupt Practices Under RPA Act 1951 - Drishti IAS, accessed on October 18, 2025, https://www.drishtiias.com/daily-updates/daily-news-analysis/corrupt-practices-under-rpa-act-1951
52. Understanding “Corrupt Practices” as per the Representation of People's Act, 1951, accessed on October 18, 2025, https://www.diwanadvocates.com/blog/understanding-corrupt-practices-as-per-the-representation-of-people-s-act-1951
53. R E P O R T A B L E IN THE SUPREME COURT OF INDIA CIVIL APPELLATE JURISDICTION CIVIL APPEAL NO.37 OF 1992 ABHIRAM SINGH ...APPEL, accessed on October 18, 2025, https://www.scobserver.in/wp-content/uploads/2021/10/AbhiramSingh-2-1-2017-pages-46-61Thakur.pdf
54. India's Advance on AI Regulation | Carnegie Endowment for ..., accessed on October 18, 2025, https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en
55. High-level summary of the AI Act | EU Artificial Intelligence Act, accessed on October 18, 2025, https://artificialintelligenceact.eu/high-level-summary/
56. Regulating Artificial Intelligence: U.S. and International Approaches and Considerations for Congress, accessed on October 18, 2025, https://www.congress.gov/crs-product/R48555
57. The EU's Artificial Intelligence Act and its Impact on Electoral Processes: a Human Rights-Based Approach - European Partnership for Democracy (EPD), accessed on October 18, 2025, https://epd.eu/news-publications/the-eus-artificial-intelligence-act-and-its-impact-on-electoral-processes-a-human-rights-based-approach/
58. Personal data protection in electronic voting | Eligo, accessed on October 18, 2025, https://eligovoting.com/electronic-voting-and-personal-data-protection/
59. Technology, data and elections: A 'checklist' on the election cycle - Privacy International, accessed on October 18, 2025, https://privacyinternational.org/sites/default/files/2019-07/Technology%2C%20data%2C%20and%20elections_0.pdf
60. Guidance for the use of personal data in political campaigning | ICO, accessed on October 18, 2025, https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-for-the-use-of-personal-data-in-political-campaigning-1/
61. Data protection guidance for Electoral Registration Officers and Returning Officers, accessed on October 18, 2025, https://www.electoralcommission.org.uk/full-guidance/data-protection-guidance-electoral-registration-officers-and-returning-officers
62. Regulating Artificial Intelligence: U.S. and International Approaches and Considerations for Congress, accessed on October 18, 2025, https://www.congress.gov/crs_external_products/R/PDF/R48555/R48555.2.pdf
63. Artificial Intelligence (AI) and Campaign Finance Policy: Recent Developments | Congress.gov,

accessed on October 18, 2025, https://www.congress.gov/crs-product/IN12222
64. Summary Artificial Intelligence (AI) in Elections and Campaigns, accessed on October 18, 2025, https://www.ncsl.org/elections-and-campaigns/artificial-intelligence-ai-in-elections-and-campaigns
65. AI Elections Accord - Munich Security Conference, accessed on October 18, 2025, https://securityconference.org/en/aielectionsaccord/
66. The Election Year Risks of AI | Brennan Center for Justice, accessed on October 18, 2025, https://www.brennancenter.org/our-work/analysis-opinion/election-year-risks-ai
67. Cambridge Analytica - Wikipedia, accessed on October 18, 2025, https://en.wikipedia.org/wiki/Cambridge_Analytica
68. Meta investors, Zuckerberg settle $8 billion privacy lawsuit tied to Cambridge Analytica scandal - Recorded Future News, accessed on October 18, 2025, https://therecord.media/meta-investors-zuckerberg-settle-privacy-lawsuit
69. Cambridge Analytica, LLC, In the Matter of | Federal Trade Commission, accessed on October 18, 2025, https://www.ftc.gov/legal-library/browse/cases-proceedings/182-3107-cambridge-analytica-llc-matter
70. Mark Zuckerberg settles lawsuit over Cambridge Analytica scandal, reports say - CBS News, accessed on October 18, 2025, https://www.cbsnews.com/news/mark-zuckerberg-meta-lawsuit-settlement-cambridge-analytica-trial/
71. Zuckerberg settles lawsuit over Cambridge Analytica scandal | The Times of Israel, accessed on October 18, 2025, https://www.timesofisrael.com/zuckerberg-settles-lawsuit-over-cambridge-analytica-scandal/
72. Delhi High Court Directs ECI To Expeditiously Resolve Plea To Combat Deepfake Videos During Elections - LawBeat, accessed on October 18, 2025, https://lawbeat.in/news-updates/delhi-high-court-directs-eci-expeditiously-resolve-plea-combat-deepfakes-during-elections
73. Start working against deepfakes, Delhi HC tells Centre - The Hindu, accessed on October 18, 2025, https://www.thehindu.com/news/cities/Delhi/start-working-against-deepfakes-delhi-hc-tells-centre/article68576870.ece
74. the challenges of governing aI-elections - The Global Solutions ..., accessed on October 18, 2025, https://www.global-solutions-initiative.org/wp-content/uploads/2024/04/GS_journal_10_Pomares_Gonzales.pdf
75. Regulating AI Deepfakes and Synthetic Media in the Political Arena ..., accessed on October 18, 2025, https://www.brennancenter.org/our-work/research-reports/regulating-ai-deepfakes-and-synthetic-media-political-arena
76. Civil society raises concerns regarding electoral integrity - ADR, accessed on October 18, 2025, https://adrindia.org/sites/default/files/Civil_society_raises_concerns_regarding_electoral_integrity.pdf
77. Protecting Global Democracy in the Digital Age: Insights from PAI's Community of Practice, accessed on October 18, 2025, https://partnershiponai.org/protecting-global-democracy-in-the-digital-age-insights-from-pais-community-of-practice/
78. Year of elections: Lessons from India's fight against AI-generated misinformation, accessed on October 18, 2025, https://www.weforum.org/stories/2024/08/deepfakes-india-tackling-ai-generated-misinformation-elections/