Panjab University Law Magazine (MAGLAW)
ISSN: 2582-3507, Volume IV Issue II, pp 69-83

ARTIFICIAL INTELLIGENCE, DEEPFAKES, AND ELECTORAL INTEGRITY IN INDIA: LEGAL AND INTELLECTUAL PROPERTY CHALLENGES

Riya Chugh*

ABSTRACT

The advent of artificial intelligence (AI) has transformed multiple facets of society, including political communication and electoral processes. In India, where digital campaigning increasingly dominates elections, AI-generated content such as deepfakes, manipulated images, and voice cloning poses significant challenges to free and fair elections. These technological innovations can undermine voter trust, distort public opinion, and blur the line between authentic political discourse and fabricated propaganda. Furthermore, AI-driven campaign content frequently intersects with intellectual property rights (IPR), as it may involve unauthorized use of copyrighted material, trademarks, and the likenesses of public figures. This paper examines the legal frameworks governing elections, digital communication, and intellectual property in India, identifying gaps in current regulations. By employing a doctrinal research methodology supplemented with comparative insights from the US, EU, and UK, this study analyzes the implications of AI misuse for electoral integrity. The findings suggest that while existing Indian laws provide partial remedies, specific regulatory measures addressing AI's role in electoral campaigns are urgently needed. This study adopts a doctrinal research methodology, supported by comparative analysis of regulatory approaches in the United States, European Union, and United Kingdom, to examine the adequacy of India's existing legal framework on elections, digital communication, and IPR. The analysis finds that current Indian laws offer only partial safeguards, leaving critical gaps in addressing AI-enabled manipulation during electoral campaigns. The research further indicates that India lacks targeted rules for transparency, provenance, accountability, and misuse of AI-generated political content. The paper proposes a multi-pronged reform approach that balances technological innovation with the protection of democratic ideals, ensuring transparency, accountability, and the safeguarding of IPR in electoral contexts.

Keywords: *Artificial Intelligence, Deepfakes, Electoral Integrity, Intellectual Property, India*

* LLM, Dr. B.R. Ambedkar National Law University, Sonipat.

1. INTRODUCTION

Elections form the backbone of India's democratic framework. Since independence, they have served as the most powerful tool for ensuring popular participation and legitimacy of governance. For decades, electoral campaigns relied heavily on physical rallies, posters, and interpersonal networks. However, with the advent of television, and later the explosion of digital technologies, the contours of electioneering underwent a radical transformation. In contemporary times, political communication increasingly unfolds on social media platforms such as Facebook, X (formerly Twitter), Instagram, and WhatsApp, with digital tools shaping not only the reach but also the nature of electoral discourse.

This digital shift, while democratizing outreach, has also introduced significant vulnerabilities. The emergence of Artificial Intelligence (AI) has accelerated both the opportunities and challenges for electoral processes. AI-based applications now allow political parties to micro-target voters, tailor campaign messages, and manage extensive databases of public sentiment. At the same time, the same technology enables the creation of highly sophisticated "deepfakes," synthetic videos and audio recordings that can convincingly imitate real individuals. Unlike earlier instances of misinformation, deepfakes pose a particularly acute danger because they can easily blur the line between truth and fabrication.

The risks posed by deepfakes are manifold. They can distort public opinion, malign reputations of political candidates, and mislead voters in a manner that undermines the constitutional promise of "free and fair elections." In a country like India, where elections involve vast electorates and where literacy and digital awareness vary significantly, the potential harm caused by manipulated AI content is magnified. The viral nature of digital content ensures that even when deepfakes are later exposed, the damage to public trust and electoral integrity is often irreversible. Thus, electoral democracy now finds itself at the intersection of technological innovation and democratic accountability.

In addition to challenges posed to integrity and transparency, AI-generated content also creates questions of intellectual property rights (IPR). Many political campaigns rely on slogans, jingles, logos, and visual designs, which are often protected under copyright or trademark law. When AI tools replicate or manipulate these without authorization, they infringe upon the rights of creators and political organizations. Furthermore, the use of AI to mimic the likeness or voice of public figures whether politicians or celebrities may encroach upon personality rights, which Indian courts have gradually recognized as part of the broader spectrum of intellectual property and privacy. The convergence of electoral law and IPR is thus no longer a theoretical question but an immediate challenge.

The Election Commission of India (ECI) has issued guidelines on responsible use of social media during elections, but such directions remain largely advisory in nature. Similarly, statutes like the Representation of People Act, 1951[1] and the Information Technology Act, 2000[2] were never designed to deal with the unique challenges posed by AI manipulated content. Although intellectual property statutes like the Copyright Act, 1957 and the Trade Marks Act, 1999 provide remedies for unauthorized use of creative works and symbols, their application in the electoral context remains underdeveloped. Consequently, India currently lacks a holistic framework to deal with the growing convergence between AI, electoral integrity, and intellectual property law.

The issue is not confined to India alone. Across the globe, democracies are grappling with the threat of AI-driven disinformation. The United States has seen states like California and Texas enact specific laws prohibiting the use of deceptive deepfakes during election campaigns. The European Union has advanced proposals through its AI Act to regulate synthetic content, especially when it threatens public trust[3]. These comparative developments underline the urgency for India to proactively design legal and policy solutions that strike a balance between technological innovation and the preservation of democratic ideals.

1.1 Research Objectives

There are three main objectives of this study:

1. **To analyze the impact of AI-generated content on electoral fairness in India:** The first objective is to identify how synthetic media, deepfakes, and other AI tools distort electoral competition and influence voter choice.
2. **To examine intersections between IPR and election law in the digital age:** The second objective is to investigate how copyright, trademark, and personality rights are implicated in AI-generated campaign content, and to determine whether current IPR statutes provide sufficient remedies for electoral misuse.
3. **To make recommendations for legislative and policy changes to protect electoral integrity against AI misuse:** The third goal is to promote proposals for enhancing India's regulatory framework in order to safeguard the integrity of elections. framework by aligning electoral governance with the facts of AI technology and drawing on comparative insights.

---

1 The Representation of the People Act, 1951, No. 43 of 1951.
2 The Information Technology Act, 2000, No. 21 of 2000.
3 *Indians Performing Rights Society v. Eastern Indian Motion Pictures Association*, (1977) 2 SCC 820.

In this context, the present study situates itself at the intersection of electoral law, technology, and intellectual property. It explores how AI-generated deepfakes threaten the fairness of elections, examines the adequacy of existing legal frameworks in addressing these concerns, and suggests pathways for reform[4]. By bringing IPR into the debate, the study highlights an often-overlooked dimension of electoral regulation: the protection of creative works, proprietary symbols, and personality rights against misuse during political campaigns.

2. RESEARCH METHODOLOGY

The study adopts a doctrinal research methodology, primarily focusing on the analysis of statutes, case law, and scholarly commentaries. Given the novelty of artificial intelligence (AI) and deepfake technologies in the electoral context, doctrinal research is particularly relevant because it enables the systematic evaluation of existing legal frameworks and their adequacy in addressing emerging challenges. By critically engaging with primary and secondary sources, the methodology situates the issue of AI in elections within the broader domain of electoral integrity, intellectual property rights (IPR), and constitutional values.

The primary sources for this study include key statutes such as the Representation of the People Act, 1951[5], the Information Technology Act, 2000[6], the Copyright Act, 1957[7], and the Trade Marks Act, 1999, alongside judicial interpretations relevant to privacy, free speech, and intellectual property. Although Indian courts have not yet addressed AI-generated deepfakes in elections, existing jurisprudence offers useful analogies for assessing emerging risks.

Secondary sources include academic articles, reports of expert committees, and policy papers published by international and domestic institutions. Literature from comparative jurisdictions, such as the European Union and the United States, is also utilized to understand how other democracies are grappling with the regulation of synthetic media in elections. This comparative dimension not only enriches the study but also provides India with possible legislative and regulatory models.

The study also takes a forward looking approach, considering the dynamic and quick changes in AI. It attempts to evaluate the future applicability of current laws in situations when AI generated material gets more complex and widespread, rather

---

4 Election Commission of India, "Voluntary Code of Ethics for the General Election 2019," *available at:* https://eci.gov.in(last visited Aug. 30, 2025).

5 Representation of the People Act, 1951, No. 43 of 1951.

6 Information Technology Act, 2000, No. 21 of 2000.

7 Copyright Act, 1957, No. 14 of 1957.

than simply listing them. As a result, the approach foresees possible legal gaps and aims to provide practical, proactive policy solutions.

The study employs qualitative content analysis to examine legal texts and scholarly writings. This involves a close reading of legislative provisions and case law to identify gaps, overlaps, and areas of ambiguity. For example, while the Copyright Act protects original works of authorship, its provisions are less clear on works generated entirely by AI. Similarly, while the Election Commission issues guidelines on digital campaigning, these are advisory and lack binding force, raising questions about enforceability[8].

To sharpen the methodological foundation, the study structures its doctrinal analysis around three analytical parameters: **(i)** assessing the adequacy of existing Indian electoral and digital communication laws in addressing AI-generated political content; **(ii)** examining how intellectual property rights frameworks respond to AI-produced material, including deepfakes, cloned voices, and unauthorized likeness use; and **(iii)** evaluating comparative regulatory approaches in the United States, the European Union, and the United Kingdom to identify normative gaps and potential models for reform. These parameters provide a clear evaluative lens, ensuring that the analysis remains focused, systematic, and responsive to the specific legal challenges posed by AI in electoral contexts.

Finally, the methodology is designed to remain normative as well as prescriptive. It not only evaluates what the law currently is but also argues for what the law ought to be in order to safeguard electoral democracy from the misuse of AI. In doing so, it remains mindful of India's constitutional ethos, which prioritizes electoral fairness, freedom of expression, and protection of creative works.

3. DIGITAL THREATS AND LEGAL LANDSCAPE

The past two decades have transformed Indian elections from traditional, ground-based canvassing to digital campaigning driven by social media platforms. Political parties increasingly use platforms like Facebook, Instagram, and X (formerly Twitter) to reach voters, particularly the youth.

3.1. Digital Campaigning in India: Rise of Social Media, AI Tools, and Political Advertising

Artificial intelligence (AI) now occupies a central role in these strategies. From chatbots simulating candidate interactions to algorithms predicting voter preferences, AI has allowed parties to expand outreach at minimal cost. However,

---

8 Election Commission of India, *Model Code of Conduct for Political Parties and Candidates*, *available at:* https://eci.gov.in(last visited Sept. 2, 2025).

these innovations have a darker side: the same tools that enable efficient communication also create avenues for manipulation, misinformation, and distortion of electoral debates.

3.2. AI-Generated Election Content: Deepfakes, Synthetic Media, Automated Bots

Among the most pressing challenges are deepfakes and synthetic media, which use AI to generate realistic but fabricated audio, video, or images. In the electoral context, these can be weaponized to impersonate candidates, spread inflammatory content, or discredit opponents. Unlike traditional propaganda, deepfakes are more convincing and harder to detect, making their impact on public perception potentially devastating.

Automated bots compound the problem by amplifying misinformation. These bots can simulate real user activity, creating an illusion of mass support or outrage around particular candidates or issues. The speed and scale of dissemination can overwhelm fact-checking mechanisms, leaving voters vulnerable to manipulation in critical pre-election periods.

While such technologies have already influenced elections in other democracies, India is not immune. Instances of AI-generated campaign jingles, manipulated videos of political speeches, and fake endorsements on social media indicate an emerging trend that could compromise electoral integrity if left unchecked.

3.3 Intellectual Property Concerns in Digital Campaigns

The rise of digital campaigning has also raised complex questions of intellectual property rights (IPR). Campaign songs, slogans, logos, and images often constitute valuable creative assets that are protected under copyright or trademark law. Unauthorized reproduction or alteration of such material for political advantage not only violates legal rights but also misleads voters.

For example, a political party might use a popular copyrighted song in its campaign without authorization, creating an association between the artist and the party. Similarly, AI tools could be used to generate modified logos or slogans resembling those of rival parties, leading to confusion among voters. Personality rights are also implicated where deepfakes use the likeness of public figures, celebrities, or candidates to endorse particular messages without consent.

Such practices undermine not just the economic interests of rights holders but also the fairness of electoral competition, as they allow campaigns to gain advantage through unlawful means.

3.4. Existing Legal Framework

India's legal landscape has several laws that indirectly touch upon AI misuse and IPR in elections, though none specifically address the unique challenges posed by synthetic media.

- **Representation of the People Act, 1951 (RPA):** The RPA lays down rules for free and fair elections, including provisions against corrupt practices and undue influence. However, its focus is primarily on traditional campaigning methods. It does not explicitly address digital manipulation or unauthorized use of intellectual property in political communication.
- **Election Commission of India (ECI) Guidelines:** The ECI has issued instructions on the use of social media and digital platforms, including requirements for political advertisements to carry pre-certification. While these guidelines reflect awareness of digital threats, their non-binding nature and limited enforcement capacity hinder effectiveness.
- **Information Technology Act, 2000 and Digital Personal Data Protection Act, 2023 (DPDP):** The IT Act penalizes certain forms of cybercrimes, while the DPDP Act governs the use of personal data in digital campaigns. Together, they provide tools to address targeted disinformation and misuse of voter data. Yet, their provisions remain general, and enforcement in election-specific contexts is nascent.
- **Copyright Act, 1957 and Trade Marks Act, 1999:** These laws protect creative works and registered trademarks from unauthorized use. In theory, they can be invoked against political parties that exploit copyrighted songs or misuse logos. However, litigation in election periods is time-consuming, and remedies may arrive too late to prevent electoral damage.

3.5. Case Illustrations: AI Misuse in Elections and IPR Conflicts

Although Indian jurisprudence has not yet seen major rulings on AI-generated electoral content, certain precedents offer insight. In *Anil Kapoor v. Simply Life India* (2023)[9], the Delhi High Court recognized personality rights and restrained unauthorized use of the actor's image and voice, setting a foundation for contesting deepfakes in elections. Similarly, courts have previously upheld copyright protections in cases involving unauthorized use of songs and slogans in advertisements, principles that extend to political contexts.

Internationally, the 2020 U.S. Presidential Election witnessed deepfake campaigns and AI-driven misinformation on platforms like Facebook, prompting several states to introduce laws banning deceptive synthetic media close to

9 *Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 4809.

elections. The European Union's proposed AI Act also includes provisions targeting high-risk AI systems that may impact democratic processes.

These cases highlight that while India lags in explicit legal recognition of AI misuse in elections, judicial reasoning in adjacent areasprivacy, IPR, and free speechcan provide interpretive guidance. Moreover, comparative experiences demonstrate the importance of proactive legislation rather than reactive adjudication.

4. DIFFICULTIES AND CRITICAL EVALUATION

One of the most pressing challenges in safeguarding Indian elections against AI misuse lies in the absence of a robust regulatory framework. Unlike traditional campaign violations, AI-generated content operates in a sphere where attribution is exceedingly difficult. A deepfake video circulated anonymously on encrypted platforms like WhatsApp can spread within minutes, leaving regulators with little capacity to identify its creator or stop its dissemination in real time. The Election Commission of India (ECI), while vigilant, currently lacks both the technological infrastructure and statutory powers to track or penalize such incidents effectively.

4.1. Regulatory Gaps in AI Oversight

The rapid pace of technological evolution further complicates regulation. AI tools that generate hyper-realistic audio-visual content are advancing faster than legal frameworks can adapt. By the time regulations are drafted, new iterations of the technology emerge, rendering earlier safeguards obsolete. Moreover, the scale of misinformation facilitated by AI is unprecedented. Unlike pamphlets or television ads, digital disinformation can be replicated infinitely at negligible cost, overwhelming fact-checking agencies and news outlets tasked with ensuring voter awareness.

These gaps highlight a structural weakness: Indian electoral law, largely framed in the mid-twentieth century, is not equipped to address twenty-first-century digital threats. Without urgent reform, the balance between free expression and electoral integrity risks tipping in favor of manipulation.

4.2. Intellectual Property Implications

AI misuse in elections does not merely threaten democratic values but also raises significant intellectual property (IP) concerns.

Copyright Infringement in AI-Generated Campaign Content

AI tools can generate campaign material by drawing upon pre-existing works without authorization. For instance, an AI model may create a campaign jingle that

mimics the style of a famous musician or reproduce fragments of copyrighted films or songs. During elections, such content is often used to create stronger emotional appeal among voters, thereby infringing upon the rights of original authors. The short electoral cycle leaves little scope for rights holders to litigate, meaning the infringement not only goes unpunished but also directly influences voter behavior.

Trademark Violations with Party Logos and Slogans

Political parties heavily rely on logos and slogans as identifiers of their brand. Misuse of these through AI-generated lookalike symbols or slogans can mislead voters into associating content with a particular party. Such acts constitute trademark infringement under Indian law. For example, an AI tool could generate posters resembling the lotus symbol of the Bharatiya Janata Party (BJP) but used in contexts designed to disparage it, leading to reputational damage and voter confusion.

Concerns over the Right of Publicity and Personality Rights

The unauthorized use of a person's identity is a further aspect. The right of publicity, sometimes referred to as personality rights, is violated by deepfakes that replicate the voice or appearance of well-known people, politicians, or activists. In situations like Titan Industries Ltd. v. Ramkumar Jewellers, Indian courts have acknowledged these rights, which prohibit the illegal commercial use of celebrity photos. As a result, the intersection of AI, elections, and IPR reveals a three-fold challenge: protecting creative works, preserving political identities, and ensuring electoral transparency.

4.3. Lessons from Abroad

Comparative experiences provide valuable insights into how other democracies have confronted similar challenges.

The United States: Legislation Governing Deepfake Elections at the State Level

In the run-up to elections, some U. S. states, such as Texas and California, have established legislation banning the distribution of misleading deepfakes[10]. For example, California legislation forbids the dissemination of manipulated media if it is designed to harm a candidate's reputation within 60 days of an election[11]. These laws represent a significant awareness of the electoral dangers posed by synthetic media, even though enforcement is still difficult.

---

[10] Texas Election Code, 255.004 (2020).

[11] California Assembly Bill No. 730 (2019), Cal. Elec. Code 20010.

European Union: The Digital Disinformation Regulation and the AI Act

The planned AI Act defines AI systems used in elections as "high risk" and mandates stringent transparency and accountability standards. The EU's Code of Practice on Disinformation also promotes the labeling of fake material by platforms and the reduction of financial incentives for disseminators of disinformation. These measures highlight the importance of a proactive regulatory strategy as opposed to a reactive one[12].

United Kingdom: Electoral Commission Guidelines

The UK's Electoral Commission has published guidelines for online campaigning, emphasizing transparency in digital advertising and disclosure of sources. Although the UK does not yet have a specific law targeting deepfakes, its focus on accountability requiring parties to clearly identify themselves in digital content provides a model for curbing anonymity-driven manipulation[13].

For India, these comparative experiences suggest that piecemeal guidelines are insufficient. A dedicated statutory framework addressing both AI misuse and digital IPR violations is required to safeguard electoral fairness.

4.4. Policy Imperatives: Integrating AI Regulation, IPR Protection, and Electoral Oversight

The convergence of electoral law, technology regulation, and intellectual property rights calls for a multidimensional policy response. Four key imperatives emerge:

1. **Dedicated Legislation on AI in Elections:** India must consider enacting laws specifically targeting the use of synthetic media in elections. This could include time-bound bans on deepfakes during election periods, disclosure obligations for AI-generated content, and penalties for malicious dissemination.
2. **Strengthening IPR Protections in Political Contexts:** Copyright and trademark enforcement must be expedited during elections through fast-track tribunals or special benches, ensuring that infringing content is removed promptly. Personality rights should also be codified to protect leaders from unauthorized digital impersonations.
3. **Technological Empowerment of the ECI:** The ECI should be equipped with AI-based detection tools to identify deepfakes and automated disinformation

---

[12] European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (AI Act), COM(2021) 206 final.

[13] Electoral Commission (UK), *Digital Campaigning: Transparency and Accountability*, *available at:* https://www.electoralcommission.org.uk(last visited Sept. 3, 2025).

campaigns in real time. Collaboration with tech companies and fact-checking bodies can enhance monitoring capacity.

4. **Public Awareness and Digital Literacy:** Ultimately, legal reforms must be accompanied by voter education. Citizens should be equipped to identify manipulated content and critically evaluate digital campaign material. This not only curbs the immediate impact of disinformation but also fosters long-term resilience against technological misuse.

Jurisdiction	Regulation on Deepfakes	Election-Specific AI Rules	IP Protection Issues	Enforcement Strength
United States	State-level bans (e.g., Texas, California); Federal bill pending	Limited federal rules; state rules vary	Strong IP laws; personality rights depend on state	Moderate; decentralized
United Kingdom	No standalone deepfake law; addressed through fraud + data protection statutes	Electoral Commission exploring AI disclosure norms	Strong copyright + passing-off protections	High clarity, slow reform
European Union	AI Act regulates high-risk political deepfakes; DSA requires content labeling	Elections Act + DSA impose disclosure duties	Harmonized IP framework; image rights vary	Strong; centralized

The Indian democratic framework has historically shown resilience in adapting to new challenges. By integrating AI regulation, IPR protection, and electoral oversight, India can strengthen its electoral integrity while preserving constitutional values of free expression and fair representation.

5. KEY RESULTS AND INSIGHTS

One of the most significant consequences of AI misuse in elections is the erosion of voter trust. Elections thrive on the perception that citizens are making choices based on accurate information. Deepfakes directly threaten this foundation by blurring the line between truth and fabrication. A manipulated video of a candidate making inflammatory remarks or endorsing controversial policies can go viral before it is disproven, shaping voter perception irreversibly.

5.1. Impact on Voter Trust: How AI-Driven Deepfakes Affect Voter Perception in India

In India, where regional identities, religious affiliations, and caste dynamics often influence voting, deepfakes can be weaponized to exploit social cleavages. Even if subsequently debunked, the “first impression effect” of such media lingers, leaving

voters confused or disillusioned. This creates a broader risk: voters may begin distrusting *all* digital political communication, including legitimate campaigns. Such skepticism undermines electoral participation, weakens representative democracy, and risks disengagement of younger, tech-savvy voters.

Thus, the impact of AI-driven misinformation is not only immediate electoral distortion but also long-term erosion of public confidence in democratic institutions.

5.2. Legal and Institutional Gaps: Limitations of ECI Guidelines, IT Act, and IPR Statutes

The current Indian legal system provides fragmented and insufficient tools to address AI misuse in elections.

From the perspective of intellectual property rights (IPR), the Copyright Act, 1957[14] and Trade Marks Act, 1999[15] offer remedies for unauthorized use of songs, images, or logos. Yet these statutes are not election-specific, and judicial remedies are slow-moving. In a fast-paced campaign, even a temporary viral misuse of IP can influence voters irreversibly before courts intervene.

These legal and institutional gaps leave India's democracy vulnerable to exploitation by technologically savvy actors who can operate with minimal accountability.

5.3. Comparative Takeaways: Regulatory Frameworks from US, EU, and UK Applicable to India

Examining comparative jurisdictions provides crucial insights for India's regulatory design.

In the United States, state-level interventions have targeted election deepfakes. California and Texas[16], for instance, prohibit the distribution of manipulated media within a defined pre-election period if intended to harm a candidate's reputation. While enforcement challenges remain, these laws highlight the value of time-bound restrictions that mitigate electoral distortions at their most vulnerable moment[17].

The European Union's AI Act categorizes AI systems influencing democratic processes as "high risk." This requires developers and users to follow transparency

---

14 Copyright Act, 1957, No. 14 of 1957.
15 Trade Marks Act, 1999, No. 47 of 1999.
16 Texas Election Code, 255.004 (2020).
17 California Assembly Bill No. 730 (2019), Cal. Elec. Code 20010.

obligations, including disclosure of AI-generated content. In tandem, the EU's Digital Services Act places accountability on online platforms to detect and limit disinformation. This layered approach of targeting both content creators and platforms reflects a holistic strategy[18].

The United Kingdom, through its Electoral Commission, emphasizes transparency in political advertising. Mandatory disclosures on the source of digital ads ensure voters know who is funding and promoting content. While not specific to AI, this framework underlines the importance of curbing anonymity in online campaigning[19].

For India, these lessons suggest a three-pronged path: adopt pre-election restrictions on deepfakes, require disclosure of AI-generated content, and mandate platform accountability to prevent viral spread of manipulated media.

5.4. Complementary Measures: Digital Literacy, Platform Accountability, and Awareness Campaigns

While law is a crucial instrument, complementary non-legal measures are equally essential.

- **Digital Literacy Programs**
  A digitally literate electorate is the first line of defense against AI-driven misinformation. Citizens must be trained to identify markers of deepfakes and verify sources before sharing content. Initiatives can be integrated into school curricula, community programs, and awareness drives during election seasons.
- **Platform Accountability**
  Social media platforms play a central role in amplifying election content. They must be compelled, either through legislation or co-regulatory models, to detect and label AI-generated material. Algorithmic transparency and prompt takedown obligations can ensure that manipulated content is flagged before it reaches mass audiences.
- **Public Awareness Campaigns by the ECI**
  The Election Commission should actively engage in public awareness campaigns highlighting the dangers of AI misuse. Just as it promotes voter turnout, the ECI can promote "digital vigilance," encouraging citizens to critically evaluate campaign material. Partnerships with fact-checking organizations and news outlets can further strengthen resilience.

---

18 European Commission, *Digital Services Act*, Regulation (EU) 2022/2065.

19 Electoral Commission (UK), *Political Finance Online Advertising Rules*, *available at:* https://www.electoralcommission.org.uk(last visited Sept. 6, 2025).

- **Collaborative Governance**
  Ultimately, AI-driven electoral challenges cannot be solved by law alone. A collaborative model involving regulators, courts, tech companies, civil society, and voters is required. Such cooperation ensures not only accountability but also adaptability, as AI evolves at a pace faster than traditional legislation.

6. OBSERVATIONS AND CLOSING INSIGHTS

Artificial Intelligence (AI) and deepfake technologies present a dual reality for modern democracy. While these tools can enhance administrative efficiency, widen outreach, and personalise voter engagement, they simultaneously threaten electoral integrity through misinformation, manipulation, and the unauthorised use of intellectual property. The Indian electoral systemby virtue of its vast scale, diversity, and increasing dependence on digital political communication remains particularly vulnerable to such risks.

Although existing legal frameworks such as the Representation of the People Act, 1951, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and core intellectual property statutes offer partial safeguards, they remain fragmented and insufficiently tailored to AI-driven challenges. Similarly, the Election Commission of India's guidelines, despite being forward-leaning, lack binding force and adequate enforcement tools. The result is a regulatory gap that enables malicious synthetic media to circulate unchecked, undermining voter confidence and electoral transparency.

To protect democratic processes while embracing technological innovation, India must adopt a coherent and forward-looking policy framework. The following four-pillar strategy is proposed:

1. Legislative Clarity and Targeted Regulation
Parliament should introduce a dedicated statute governing AI and synthetic media in electoral contexts. Such legislation must define prohibited conductincluding non-consensual deepfakes of candidates, automated disinformation campaigns, and deceptive AI-generated political messagingand provide swift remedies during election periods.

2. Strengthened Intellectual Property and Personality Rights Protections
Amendments to the Copyright Act, 1957, and the Trade Marks Act, 1999, should explicitly address AI-generated misuse of campaign songs, images, symbols, and personal likenesses. Fast-track injunctive relief will be essential to prevent irreparable electoral harm.

3. Enhanced Institutional Capacity for the Election Commission

The Election Commission must be equipped with expanded legal authority, dedicated AI-monitoring infrastructure, and formal collaboration channels with digital platforms. A real-time detection and takedown mechanism for synthetic media should form part of this strengthened institutional mandate.

4. Digital Literacy and Public Awareness Mechanisms

A nationwide digital literacy initiative is necessary to equip voters with the ability to identify manipulated or synthetic content. Collaborative campaigns involving civil society, educational institutions, and media organisations can significantly reduce citizen vulnerability to digital misinformation.

AI in elections is not inherently detrimental; when governed through clear, accountable, and future-proof regulation, it can enrich democratic participation. However, unchecked misuse poses a serious threat to public trustthe bedrock of any democracy. India's legal and institutional response must therefore prioritise transparency, accountability, and adaptability, ensuring that democratic ideals are not eclipsed by technological disruption but are strengthened through responsible innovation.