

Deepfake Democracy: Legal Regulation of AI-Manipulated Political Content and Electoral Integrity in India

Dr. T.V.Rajput

Independent Research, Gujarat, India

Email: rajputthana010@gmail.com



Received 10 August 2026

Accepted 15 August 2026

Published 27 August 2026

Corresponding Author:

Dr. T.V.Rajput

Email: rajputthana010@gmail.com

DOI: <https://doi.org/10.64880/tvsjir.v1i3.11>

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sector.

Copyright: © 2026 The Author(s).



This is an open access article under the [Creative Commons Attribution-Noncommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

OPEN ACCESS

Abstract:

The rapid advancement of artificial intelligence has changed the way politics is communicated and has introduced new difficulties for democratic governance. Because of deepfake technology it is now possible to produce highly realistic but false audio, video, images, and other political material, which can mislead voters, harm the reputations of candidates, influence people's decisions in elections, and erode public trust. This research paper looks at the legal regulation of AI-altered political content in India and the effects this has on the integrity of elections. It looks at how suitable the current legal measures are, including the Information Technology Act, 2000, the Information Technology Rules, 2021, the Bharatiya Nyaya Sanhita, 2023, the Representation of the People Acts, and the regulatory actions taken by the Election Commission of India. The study also examines the problems concerning detection, accountability, the removal of content, political speech, privacy, and the responsibility of intermediaries. A comparative viewpoint is taken in order to find out regulatory methods that could help India in establishing an effective framework. The paper calls for transparent labelling, authentication of digital content, prompt enforcement, responsibility on the part of the platforms, increased voter awareness, and appropriate legal protections in order to safeguard electoral fairness without unduly restricting legitimate political expression in the digital age.

Keywords: Deepfake, Artificial Intelligence, Political Content, Electoral Integrity, Elections in India, Political Disinformation, Misinformation, Election Commission of India, Digital Democracy, Social Media, AI Regulation, Political Communication, Voter Manipulation, Cyber Law, Synthetic Media.

1. Introduction

Artificial intelligence is increasingly becoming part of modern political communication, changing the way information is created and shared during elections. One of the most concerning developments is the use of deepfake technology, through which photographs, videos, and audio recordings can be altered to present false information as genuine. In an election, such manipulated material may show a candidate making statements they never made, attending

events they never attended, or expressing views that are completely different from their actual position. The rapid circulation of such content through social media can influence public opinion before the truth is established. This creates a serious concern for voters who depend on reliable information when making electoral choices. Deepfakes can also harm the reputation of candidates, increase social tension, and weaken public confidence in the electoral process. India has various laws and regulatory measures dealing with misleading digital content, impersonation, and election-related misconduct. However, the speed and sophistication of artificial intelligence present new difficulties for existing legal mechanisms. This paper examines the legal regulation of AI-manipulated political content in India and considers measures necessary to protect electoral fairness, voter confidence, and democratic values.[1]

2. Research Purpose and Methodology

Research Purpose:

- To examine the growing use of AI-generated deepfakes in political communication and their potential impact on electoral integrity in India.
- To analyse the adequacy of the existing Indian legal and regulatory framework for addressing politically manipulated audio, video, images, and other synthetic content.
- To assess the challenges faced by the Election Commission, political parties, candidates, social-media platforms, and voters in identifying and responding to political deepfakes.
- To suggest an effective, transparent, and balanced legal framework that protects electoral integrity while preserving legitimate political expression and technological innovation.

Research Methodology:

This study adopts a doctrinal and analytical research methodology to examine the legal regulation of AI-manipulated political content in India. It analyses relevant laws, regulations, judicial decisions, official guidelines, academic literature, and secondary sources to assess their effectiveness in protecting electoral integrity.

3. Literature Review

The growing use of artificial intelligence in political communication has created new concerns about the authenticity of electoral information. **George (2023)** discussed the risks posed by deepfake technology to Indian elections and stressed the importance of transparency and accountability. **Singh, Goswami and Baro (2024)** examined the growing presence of artificial intelligence and deepfakes in Indian elections, particularly their possible influence on voters and political campaigns. **Gaur (2025)** focused on the need for effective regulation and suggested that transparency, identification of manipulated content and institutional preparedness are important for addressing deepfake-related risks. **Kashyap (2025)** examined weaknesses in the existing Indian legal framework and noted that present laws do not fully address the specific challenges created by synthetic media. **Dahiya (2025)** further considered the impact of artificial intelligence on electoral politics, including misinformation, voter manipulation and regulatory difficulties. These studies collectively indicate that India needs a clearer and practical legal approach to political deepfakes while maintaining a proper balance between electoral integrity and legitimate political expression.

4. Conceptual Understanding of Political Deepfakes

Political deepfakes refer to digitally manipulated or artificially generated audio, video, images, or other media created with advanced artificial intelligence to make individuals appear to say or do things that never actually occurred. In the political context, such content can imitate candidates, political leaders, public officials, or other influential persons and may be used to influence public opinion or electoral choices. Political deepfakes can take different forms, including altered speeches, fabricated interviews, synthetic voices, manipulated photographs, and digitally generated campaign material. Their realistic appearance makes them difficult for ordinary users to identify, particularly when they spread rapidly through social media platforms. Unlike ordinary misinformation, deepfakes can create highly convincing false evidence that appears authentic. Their use during elections may therefore affect the credibility of candidates, mislead voters, damage reputations, and reduce public confidence in democratic processes. Understanding political deepfakes is consequently important for developing appropriate legal safeguards, technological detection mechanisms, responsible political communication practices, and effective measures to protect electoral integrity in India.[2]

4.1 Impact of Deepfakes on Electoral Democracy

Deepfakes can significantly affect electoral democracy by creating realistic but false videos, images, or audio recordings of political leaders and candidates. During elections, such manipulated content can mislead voters, damage reputations, influence public opinion, and create confusion about genuine political statements. The rapid circulation of deepfakes through social media makes their impact more serious because false information can reach large audiences within a short time. Deepfakes may also increase political polarisation, encourage hostility between communities, and reduce public trust in candidates, institutions, and the electoral process. Voters may find it difficult to distinguish authentic content from manipulated material, which can affect their ability to make informed electoral choices. The problem becomes particularly serious when deepfakes are released shortly before voting, leaving limited time for verification or correction. Therefore, effective regulation, transparent identification of AI-generated content, rapid verification mechanisms, and greater public awareness are essential to protect electoral fairness and democratic decision-making.[3]

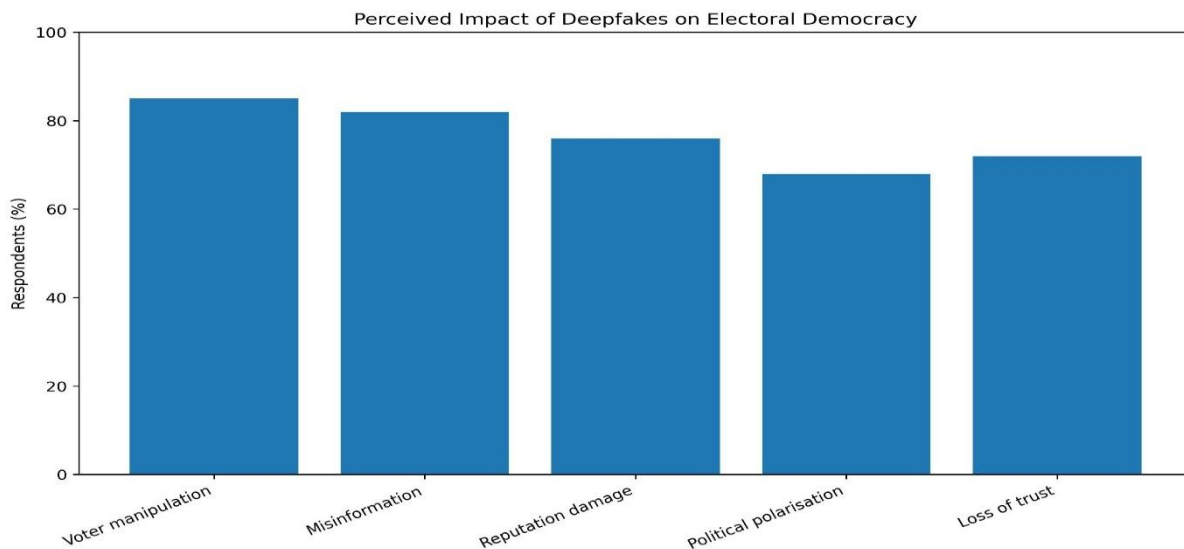


Figure 1: Perceived Impact of Deepfakes on Electoral Democracy**5. Existing Legal Framework in India**

India currently does not have one specific law dealing exclusively with political deepfakes. Their regulation is therefore based on different legal provisions dealing with online deception, impersonation, privacy, unlawful digital content and electoral conduct. The Information Technology Act, 2000 and the Information Technology Rules, 2021 provide an important framework for addressing harmful content circulated through digital platforms. Electoral regulation is further supported by the Representation of the People Acts and the Model Code of Conduct. The Election Commission of India has also issued directions to political parties regarding the responsible use of artificial intelligence and has cautioned against creating or circulating misleading deepfake material during elections. In **Shreya Singhal v. Union of India (2015)**, the Supreme Court examined restrictions on online speech and struck down Section 66A of the Information Technology Act while upholding Section 69A, subject to procedural safeguards. The decision is relevant to deepfake regulation because any attempt to control manipulated political content must be balanced against legitimate political expression. Therefore, India's existing framework provides several legal mechanisms, but the absence of a dedicated law specifically addressing political deepfakes creates difficulties concerning detection, accountability, removal and enforcement during elections.

High Courts have also addressed the misuse of digital platforms where manipulated or deceptive content affects individual rights. In **Swami Ramdev v. Facebook, Inc. (Delhi High Court, 2019)**, the Court dealt with unlawful online dissemination and directed removal of offending content. The judgment demonstrates that Indian courts can provide effective remedies against harmful digital material, although political deepfakes remain a developing legal challenge.[4]

6. Role of the Election Commission of India

The Election Commission of India plays a vital role in protecting the integrity, fairness and transparency of elections in the digital age. With the growing use of artificial intelligence, deepfakes and manipulated political content, the Commission faces new challenges in ensuring that voters receive authentic and reliable information. It monitors election-related content circulated through digital and social media platforms and issues directions to political parties and candidates regarding responsible online campaigning. The Commission has also emphasised the need to identify and appropriately label artificial intelligence-generated or digitally manipulated content. It can direct political actors to remove misleading material and take appropriate action when electoral rules or the Model Code of Conduct are violated. Through coordination with government authorities, technology platforms and election officials, the Commission can strengthen mechanisms for detecting and reporting deceptive content. Public awareness is another important responsibility, as informed voters are better able to recognise manipulated political messages. However, effective regulation requires timely enforcement, technological expertise and cooperation from digital platforms. Therefore, the Election Commission must continuously strengthen its monitoring, verification and enforcement mechanisms while maintaining a fair balance between preventing deceptive content and protecting legitimate political expression during elections.[9]

6.1 Deepfakes and Electoral Integrity

Deepfakes pose a serious challenge to electoral integrity because they can create highly convincing but false audio, video, or visual content involving political leaders, candidates, parties, and public events. During elections, such manipulated content can influence voters before accurate information reaches them, distort public debate, damage the reputation of candidates, and create confusion about genuine political statements. The rapid circulation of deepfakes through social media platforms further increases their potential impact, as misleading content can reach large audiences within a short period. Electoral integrity depends upon voters having access to reliable information and making choices without deliberate technological deception. Deepfakes can undermine this process by presenting fabricated statements or events as authentic, thereby affecting voter perceptions and electoral behaviour. They may also increase social and political polarisation when manipulated content targets sensitive issues or particular communities. At the same time, regulation must avoid unnecessarily restricting legitimate political expression, satire, criticism, or artistic content. Therefore, protecting electoral integrity requires a balanced legal approach involving clear disclosure requirements, rapid verification mechanisms, platform accountability, responsible conduct by political actors, and greater public awareness. Effective regulation should focus on preventing deliberate deception while preserving democratic participation, freedom of expression, and the credibility of the electoral process.[5]

7. Comparative Legal Perspective

A comparative legal perspective examines how India, the United States, and the European Union address political deepfakes through disclosure requirements, platform accountability, election regulations, and artificial intelligence governance. Comparing these approaches helps identify effective safeguards while preserving political expression, innovation, and democratic participation.

Table:1 Comparative Legal Approaches to Regulating Political Deepfakes

Country/Region	Key Legal Approach
India	Election guidelines, IT Rules and platform accountability
United States	State-level restrictions and election-related regulation
European Union	AI governance, transparency and disclosure requirements.

8. Discussion

The increasing use of artificial intelligence in political communication has created new challenges for electoral integrity in India. Deepfake technology can produce highly realistic videos, images, and audio recordings that may falsely portray political leaders or candidates making statements they never made. Such content can influence voters, damage reputations, spread misinformation, and reduce public confidence in the electoral process. The existing legal framework, including the Information Technology Act, 2000, Information Technology Rules, 2021, Bharatiya Nyaya Sanhita, 2023, and election-related regulations, provides certain mechanisms to address

deceptive and harmful digital content. However, these provisions were not specifically designed to deal with the speed, scale, and technical sophistication of modern deepfakes. The Election Commission of India has taken important steps by encouraging responsible use of artificial intelligence and requiring appropriate identification of synthetic content. Nevertheless, effective regulation requires cooperation among election authorities, political parties, candidates, technology platforms, and citizens. Regulation should focus on transparency, rapid verification, accountability, and clear disclosure of artificially generated political material while protecting legitimate political expression. A balanced legal approach is therefore necessary to prevent manipulation without unnecessarily restricting freedom of political communication. Strengthening technological detection, voter awareness, platform responsibility, and enforcement mechanisms can help preserve trust, fairness, and credibility in India's democratic electoral process.[8]

9. Suggestions and Future Regulatory Framework

India should develop a clear and comprehensive regulatory framework to address AI-manipulated political content while protecting legitimate political expression. Political deepfakes should be subject to mandatory and easily visible labelling so that voters can distinguish authentic material from synthetic content. Political parties, candidates, campaign organisations and digital platforms should have clearly defined responsibilities for creating, distributing, detecting and removing deceptive content. The Election Commission of India should establish a specialised monitoring mechanism capable of responding quickly to deepfake complaints during election periods. Digital platforms should maintain transparent reporting systems, preserve relevant evidence and provide rapid corrective measures when manipulated content threatens electoral integrity. The use of reliable watermarking, content provenance and verification technologies should be encouraged to establish the origin and authenticity of political media. Strong penalties should apply to deliberate deepfakes created to impersonate candidates, mislead voters or disrupt elections, while safeguards should prevent legitimate satire, criticism and political commentary from being unnecessarily restricted. Public awareness programmes and digital literacy initiatives should also help voters recognise manipulated content. Regular coordination among the Election Commission, law-enforcement agencies, technology companies and civil society organisations is necessary. Such measures can strengthen electoral transparency, protect informed voting and maintain public confidence in India's democratic process.[9]

10. Conclusion

Deepfakes and other forms of AI-manipulated political content represent a growing challenge to electoral democracy in India. Their ability to create convincing but false audio, video, images, and political statements can mislead voters, damage the reputation of candidates, influence electoral choices, and weaken public confidence in democratic institutions. Although India has existing legal provisions under the Information Technology Act, Information Technology Rules, Bharatiya Nyaya Sanhita, Representation of the People Acts, and regulatory directions of the Election Commission of India, these measures face difficulties in addressing rapidly developing artificial intelligence technologies. Effective regulation therefore requires a coordinated approach involving law,

technology, electoral institutions, political parties, candidates, and digital platforms. Mandatory disclosure of AI-generated political material, reliable content verification, transparent platform policies, rapid response mechanisms, and stronger accountability can help reduce deceptive practices. At the same time, regulation must remain proportionate so that genuine political expression, satire, criticism, and legitimate technological innovation are not unnecessarily restricted. Protecting electoral integrity ultimately requires voters to receive authentic and reliable information when making democratic choices. India should therefore develop a clear, adaptable, and rights-sensitive regulatory framework capable of addressing deepfake threats while preserving democratic participation, political freedom, technological development, and public trust in the electoral process.

References

1. Kalpokas, I., & Kalpokiene, J. (2022). Deepfakes: A realistic assessment of potentials, risks, and policy regulation. Springer. Pp. 1–17.
2. Kalpokas, I., & Kalpokiene, J. (2022). Deepfakes: A realistic assessment of potentials, risks, and policy regulation. Springer. Pp. 19–39.
3. Kalpokas, I., & Kalpokiene, J. (2022). Deepfakes: A realistic assessment of potentials, risks, and policy regulation. Springer. Pp. 65–71.
4. Bennett, T. D. C., & Moosavian, R. (Eds.). (2026). Deepfakes and the law: Challenges, responses, and critique. Taylor & Francis. 366 pp.
5. Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1820. Pp. 1753–1820.
6. Chesney, R., & Citron, D. K. (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs*, 98(1), 147–155. Pp. 147–155.
7. Schick, N. (2020). Deepfakes: The coming infocalypse. Twelve. Pp. 1–224.
8. Benn, C. (2026). Deepfakes and democracy. In S. Nyholm, A. Kasirzadeh, & J. Zerilli (Eds.), *Contemporary debates in the ethics of artificial intelligence*. Wiley. Pp. 1–16.
9. Dahiya, V. (2025). Artificial intelligence and electoral politics in India: Democratic innovation, risks and regulatory challenges. *International Journal of Politics and Media*, 4(2), 18–22.
10. Chugh, R. (2026). Artificial intelligence, deepfakes, and electoral integrity in India: Legal and intellectual property challenges. *Panjab University Law Magazine*, 4(2), 69–83.

Disclaimer/Publisher's Note: The views, findings, and opinions expressed in this publication are solely those of the author(s). The publisher and editorial team are not responsible for any errors, claims, or consequences arising from the use of the published content.