AI-Specific Threats in Indian Elections

Author: Animesh Anand

LL.M (Cyber Law), The ICFAI University, Dehradun

Co-Author: Dr. Saurabh Siddhartha

Assistant Professor, The ICFAI University, Dehradun

ABSTRACT

The adoption of Artificial Intelligence (AI) within democratic processes has introduced both operational efficiencies and constitutional complications that existing legal frameworks were not designed to address. In India, the Election Commission of India (ECI) has begun exploring AI-driven tools for voter verification, electoral roll management, and campaign monitoring. At the same time, political parties spent an estimated $50 million on AI-generated campaign content during the 2024 general elections, including deepfakes of deceased political figures and synthetic media depicting celebrities endorsing specific parties. These developments sit within a legal environment that is still catching up. The right to privacy, recognised as a fundamental right under Article 21 of the Indian Constitution in Justice K.S. Puttaswamy (Retd.) v. Union of India, provides a constitutional benchmark through its four-part proportionality test. The Digital Personal Data Protection Act, 2023 (DPDPA) establishes a consent-based framework for personal data processing but contains broad state exemptions under Section 17 that could allow electoral authorities to bypass these protections entirely. The Representation of the People Act, 1951 (RPA) defines corrupt practices under Section 123 but does not contemplate AI-driven voter profiling or algorithmically generated misinformation as forms of undue influence. This dissertation examines The study proposes regulatory reforms that reconcile technological adoption with the constitutional guarantees of privacy, free and fair elections, and democratic accountability.

Keywords: *Artificial Intelligence, Indian Elections, Deepfakes, Voter Profiling, Right to Privacy, Article 21, Digital Personal Data Protection Act 2023, Representation of the People Act 1951, Election Commission of India.*

---

1. Voter profiling and algorithmic micro-targeting

The threat AI poses to Indian elections is not limited to the production of fake videos. Before a single deepfakes is created, AI systems can be deployed at the back end to build detailed profiles of individual voters, map their political preferences, predict their behaviour, and deliver precisely calibrated messages designed to influence how they vote. This practice, commonly called algorithmic micro-targeting, combines large-scale data collection with machine learning models that segment the electorate into clusters based on caste, religion, income, language, social media activity, and consumption patterns.

The infrastructure for this kind of profiling already exists in India. The country has over 760 million internet users, more than 50 percent of the population.[1] WhatsApp alone has over 500 million users in India, and political parties have built extensive group networks on the platform that remain largely invisible to regulators.[2] During the 2024 general elections, the BJP's volunteer workforce operated an elaborate WhatsApp group infrastructure that powered the distribution of campaign messaging at a granular, booth-level scale.[3] AI tools enabled these networks

[1]Deepfake Democracy: Behind the AI Trickery Shaping India's 2024 Election, AL JAZEERA (Feb. 20, 2024), https://www.aljazeera.com/news/2024/2/20/deepfake-democracy-behind-the-ai-trickery-shaping-indias-2024-elections.

[2]Karen Rebelo, India's Generative AI Election Pilot Shows Artificial Intelligence in Campaigns is Here to Stay, CTR. FOR MEDIA ENGAGEMENT (Oct. 2024), https://mediaengagement.org/research/.

[3]The Era of AI-Generated Election Campaigning is Underway in India, TECHPOLICY.PRESS (May 25, 2024), https://www.techpolicy.press/the-era-of-aigenerated-election-campaigning-is-underway-in-india/.

to send personalised messages to individual voters. In Rajasthan, BJP campaign volunteers received WhatsApp videos from a party leader who addressed each volunteer by name using voice-cloning and lip-matching software.[4]

The legal problem with this practice is that Section 123(2) of the RPA 1951 defines "undue influence" as any direct or indirect interference with the free exercise of electoral rights.[5] The provision was drafted to cover physical coercion, threats of injury, and social ostracism. It does not contemplate the possibility that an AI system could analyse a voter's psychological vulnerabilities through their social media activity and then deliver content specifically designed to exploit those vulnerabilities.

The Aadhaar-voter ID linkage program compounds this risk. The Election Laws (Amendment) Act, 2021 amended the Representation of the People Act, 1950 to allow Electoral Registration Officers to seek Aadhaar numbers from voters for identity verification purposes.[6] While the ECI and the government have described this as voluntary, the practical implementation has been coercive. Form 6B, used for collecting Aadhaar details, offered voters only two options: submit their Aadhaar number or declare they did not possess one.[7] Justice B.N. Srikrishna, former Supreme Court judge who chaired the expert committee that drafted India's original Data Protection Bill, warned that this linkage could create conditions for comprehensive voter profiling at scale, describing the potential as "instead of having a Cambridge Analytica you'll have a Delhi Analytica."[8]

The dangers of this linkage are not theoretical. In 2015, during the National Electoral Roll Purification and Authentication Programme (NERPAP), the ECI attempted to link Aadhaar with voter rolls in Andhra Pradesh and Telangana. The exercise resulted in the deletion of approximately 55 lakh voters from electoral rolls due to Aadhaar data mismatches.[9] Many voters discovered their names missing only on election day. The Supreme Court stayed the programme through its August 2015 order.[10] In 2022, the Supreme Court issued notice on a petition filed by former Army General S.G. Vombatkere challenging the constitutional validity of the Election Laws (Amendment) Act, 2021, with Senior Advocate Shyam Divan arguing that as per the *Puttaswamy* judgment, Aadhaar can be used only for providing government benefits and cannot be insisted upon when a citizen exercises fundamental rights.[11]

In September 2023, in *G. Niranjan v. Election Commission of India*, the ECI assured the Supreme Court that Aadhaar-voter ID linkage would remain voluntary and that non-submission of Aadhaar would not affect voter rights.[12] Despite this assurance, the renewed push for linkage continues. The concern from a legal standpoint is that once Aadhaar is linked to voter IDs, it becomes possible to cross-reference electoral data with banking records, telecom data, welfare scheme databases, and social media profiles. Political parties with access to such cross-referenced datasets, whether directly or through data analytics firms, could build the kind of 360-degree voter profiles that enable AI-driven micro-targeting at an unprecedented level of precision.

The DPDPA 2023 does not adequately address this risk. The Act does not recognise political opinions as a separate category of sensitive personal data, unlike the GDPR which classifies political opinions under Article 9 as a special category requiring heightened protection.[13] If the ECI's data processing activities fall under such an exemption,

[4]India's Experiments With AI in the 2024 Elections: The Good, The Bad & The In-between, TECHPOLICY.PRESS (Sept. 25, 2024), https://www.techpolicy.press/indias-experiments-with-ai-in-the-2024-elections-the-good-the-bad-the-inbetween/.

[5]The Representation of the People Act, 1951, No. 43 of 1951, S. 123(2), INDIA CODE (1951).

[6]Election Laws (Amendment) Act, 2021, No. 30 of 2021, INDIA CODE (2021).

[7]Aadhaar-Voter ID Linkage Concerns, DRISHTI IAS (2023), https://www.drishtiias.com/daily-updates/daily-news-analysis/aadhaar-voter-id-linkage.

[8]Aadhaar-EPIC Linkage Will Deprive India's Electoral Democracy, THE WIRE (Mar. 22, 2025), https://thewire.in/government/aadhaar-epic-linkage-deprive-electoral-system-integrity.

[9]A Move That Endangers the Right to Vote, CIVILSDAILY (Apr. 23, 2025), https://www.civilsdaily.com/news/a-move-that-endangers-the-right-to-vote/.

[10]Aadhaar Voter ID Linkage, SHANKAR IAS PARLIAMENT (Apr. 25, 2025), https://www.shankariasparliament.com/current-affairs/gs-i/aadhaar-voter-id-linkage.

[11]S.G. Vombatkere v. Union of India, W.P. (Civil) No. 848 of 2022 (Supreme Court of India), https://www.livelaw.in/top-stories/supreme-court-eci-electoral-roll-aadhaar-database-linking-aadhaar-voter-id-card-linkage-212841.

[12]G. Niranjan v. Election Commission of India (Sept. 2023) (Supreme Court of India).

[13]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, S.S. 4-5, INDIA CODE (2023).

voter data processed by the Commission would sit entirely outside the DPDPA's consent, purpose limitation, and data minimisation requirements.[14]

2. Deepfakes and synthetic media in the 2024 general elections

The 2024 Indian general elections were the first in which AI-generated synthetic content was deployed at industrial scale across all major political parties. Indian political parties spent an estimated $50 million on AI-generated campaign material, making the 2024 elections the most AI-intensive democratic exercise in history.[15] This expenditure formed part of the broader election spending of approximately $16 billion, which made it also the most expensive election ever conducted anywhere in the world.[16]

The scale of AI deployment was driven by two factors. First, the technology had become cheap and accessible. Voice cloning tools that could produce realistic synthetic audio of any political leader cost as little as ten cents per video, and dozens of smartphone apps could synchronise lip movements with customised scripts within minutes.[17] AI policy expert Sagar Vishnoi described these low-quality deepfakes as "cheapfakes" that had become "democratised, like the new Canva or Photoshop." Second, AI-generated calls were approximately eight times cheaper than traditional human call centres, making the technology attractive to campaign strategists operating under expenditure ceilings. Over 50 million AI-generated voice clone calls were made to voters in the two months before polling commenced in April 2024. This volume of outreach represented a $60 million business opportunity for AI consultants and synthetic media companies working with political parties.

Divyendra Singh Jadoun, a 31-year-old college dropout who founded Polymath Synthetic Media Solutions from the town of Pushkar in Rajasthan, became the most visible figure in this industry. His nine-person company worked on campaigns for several major political parties, including the BJP and the Congress, and expected to generate $241,000 in revenue during the six-week election period alone.[18]Jadoun's company cloned the voice of Rajasthan's then Congress chief ministerial candidate Ashok Gehlot to send personalised WhatsApp messages to individual voters, addressing each voter by name.

Several specific incidents during the 2024 elections illustrate the range of threats posed by synthetic media.

The resurrection of deceased political figures. In South India, the Dravida Munnetra Kazhagam (DMK) party used AI to create a synthetic video of its deceased founder M. Karunanidhi, who died in 2018, delivering a speech endorsing current party candidates and addressing young party workers.[19] In Tamil Nadu, AI was used to digitally revive deceased political leaders to endorse current candidates, exploiting voters' emotional connections with these figures.[20] The All India Dravida Munnetra Kazhagam (AIDMK) created an AI-generated audio clip of the deceased J. Jayalalithaa, a former Chief Minister, urging support for specific candidates. These practices raise a category of legal questions that no Indian statute addresses: the use of a deceased person's likeness and voice, without consent from their estate, as a form of political endorsement generated by AI.

The Rahul Gandhi deepfake. A manipulated video circulated on social media falsely showing Congress leader Rahul Gandhi being sworn in as Prime Minister while the election was still underway. The video used AI voice cloning to make it appear Gandhi had resigned from his party, with a fabricated statement attributed to him: "I can

[14]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, S. 8, INDIA CODE (2023).

[15]DGAP, Generative AI and Its Influence on India's 2024 Elections, GERMAN COUNCIL ON FOREIGN RELATIONS (2024), https://dgap.org/system/files/article_pdfs/A4_Policy%20Paper_AI%20on%20Indias%202024%20Electons_EN.pdf.

[16]Anadi, Deep Fakes, Deeper Impacts: AI's Role in the 2024 Indian General Election and Beyond, GLOBAL NETWORK ON EXTREMISM & TECH. (Sept. 11, 2024), https://gnet-research.org/2024/09/11/deep-fakes-deeper-impacts-ais-role-in-the-2024-indian-general-election-and-beyond/.

[17]Shaping Robust AI Regulation: Lessons from India's 'Deepfake' Election, HARV. POL. REV. (Dec. 6, 2024), https://theharvardpoliticalreview.com/ai-deepfakes-india-election/.

[18]AI Companies Are Making Millions Producing Election Content in India, REST OF WORLD (May 23, 2024), https://restofworld.org/2024/india-elections-ai-content/.

[19]ECI Cracks Down On Deepfakes Before Bihar Polls, MEDIANAMA (Oct. 28, 2025), https://www.medianama.com/2025/10/223-election-commission-deepfakes-advisory-bihar-elections/.

[20]The Digital Election: How Technology Redefined India's 2024 General Election, NETMISSION.ASIA (Feb. 26, 2025), https://netmission.asia/2025/02/26/the-digital-election-how-technology-redefined-indias-2024-general-election-ankita-rathi/.

no longer pretend to be Hindu for the sake of elections." This was shared by BJP-affiliated accounts and was designed to exploit existing religious fault lines in the electorate.

The Amit Shah reservation deepfake. A doctored video of Union Home Minister Amit Shah was widely circulated in which he appeared to announce the removal of reservations for Scheduled Castes and Scheduled Tribes.[21] The Mumbai police registered a case against a social media account affiliated with the Maharashtra State Youth Congress in connection with the video. This incident illustrates how deepfakes can be used to fabricate policy statements that directly affect the interests of marginalised communities and inflame communal tensions during elections.

The liar's dividend. One of the less discussed but more insidious effects of deepfake proliferation is the "liar's dividend," a term describing the phenomenon where the existence of deepfake technology allows political actors to dismiss authentic but damaging videos as fabricated. During the 2024 elections, a video surfaced of a BJP candidate in Uttar Pradesh, Dinesh Lal Yadav, making remarks about the Prime Minister and Chief Minister. The BJP quickly attempted to dismiss the video as a deepfake. However, independent analysis by fact-checkers confirmed the video was authentic. This incident demonstrated how deepfake technology erodes trust not only by producing false content but by providing a credible alibi for genuine misconduct.

3. Platform complicity and intermediary liability failures

The role of social media platforms during the 2024 Indian elections exposed a systemic failure of the intermediary liability framework under the IT Act, 2000. Section 79 of the IT Act grants intermediaries conditional immunity from liability for third-party content, provided they observe "due diligence" and comply with takedown obligations.[22] However, this framework was designed for an era when platforms were passive conduits of user-generated content. When platforms actively deploy AI-powered advertising systems that approve, target, and distribute political content, the passive intermediary model breaks down.

The most damning evidence of this failure came from an investigation by India Civil Watch International (ICWI) and corporate accountability organisation Eko, which tested Meta's content moderation systems during the election. The investigators created 22 advertisements containing AI-generated inflammatory content, modelled on real hate speech prevalent in Indian political discourse, and submitted them to Meta's ad library. Fourteen of the 22 ads were approved within 24 hours.[23] The approved ads contained phrases targeting Muslims, including calls to burn minorities and execute opposition leaders. Three additional ads were approved after minor modifications that did not change the inflammatory substance.[24]

These ads were submitted during the third and fourth phases of the Lok Sabha election, a period that included the legally mandated 48-hour silence period before polling under Section 126 of the RPA 1951, during which no political advertisements can be published.[25] Meta's systems failed to enforce even this basic temporal restriction. YouTube's content moderation performed equally poorly. Researchers from Global Witness and Access Now created 48 test advertisements in English, Hindi, and Telugu containing misleading voting information and calls for violence. YouTube approved all of them for publication. One ad falsely claimed India had raised its voting age to 21, another said women could vote via text message, and a third advocated for the use of force at polling stations.

The legal response to these failures has been fragmented. The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose due diligence obligations on intermediaries but do not specifically address AI-generated political content.[26] MeitY's proposed amendments to these Rules seek to mandate labelling of synthetic

[21]Meta Approved Ads Inciting Violence Against Muslims During Lok Sabha Polls, SCROLL.IN (May 21, 2024), https://scroll.in/latest/1068131/.

[22]The Information Technology Act, 2000, No. 21 of 2000, S. 79, INDIA CODE (2000).

[23]Meta Allowed AI-Generated Anti-Muslim Ads During India Election, MIDDLE EAST MONITOR (May 22, 2024), https://www.middleeastmonitor.com/20240522-meta-allowed-ai-generated-anti-muslim-ads-during-india-election/.

[24]Political Ads Inciting Violence Escape Meta's Filters, MEDIANAMA (May 24, 2024), https://www.medianama.com/2024/05/223-report-reveals-meta-allowed-hateful-political-ads/.

[25]The Representation of the People Act, 1951, No. 43 of 1951, S. 126, INDIA CODE (1951).

[26]The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

media, but these remain at the proposal stage and do not create election-specific obligations.[27] The ECI's advisories, while more targeted, lack statutory authority. The October 2025 advisory mandating labelling of AI-generated campaign content applies only to official party accounts and only during election periods, leaving unofficial campaign networks and inter-election periods entirely unregulated.[28]

4. Algorithmic opacity within the ECI's internal tools

The discussion of AI threats in Indian elections has focused almost entirely on how political parties and external actors use AI to manipulate voters. An equally important but underexplored question is how the ECI itself uses AI systems internally and whether those systems operate with adequate transparency and accountability.

The ECI, operating under Article 324 of the Constitution, has constitutional authority to superintend, direct, and control elections.[29] In exercising this authority, the Commission has increasingly adopted digital tools for voter roll management, polling booth allocation, voter turnout prediction, and campaign expenditure monitoring. AI tools used for voter roll analytics, including deduplication algorithms and automated voter verification systems, make decisions that directly affect whether individuals appear on the electoral roll and can exercise their right to vote.

The 2015 NERPAP experience provides a concrete example of how algorithmic decisions within the ECI can produce large-scale harm. The deduplication exercise that removed 55 lakh voters in Telangana and Andhra Pradesh was driven by automated matching algorithms that flagged apparent duplicates based on Aadhaar data. The UIDAI itself acknowledged in 2018 that Aadhaar-based biometric authentication had a 12% error rate.[30] An error rate of this magnitude, when applied to an electoral roll of over 960 million voters, could affect the voting rights of over 100 million people.

The Comptroller and Auditor General (CAG) in its 2021 report found serious flaws in the Aadhaar database itself, including duplications and unverifiable residency data, raising questions about whether any algorithm operating on flawed input data can produce reliable outputs for electoral purposes.

The ECI has not published any algorithmic impact assessments, algorithmic audit reports, or transparency disclosures about its internal AI systems.[3132] This opacity is constitutionally problematic. The *Puttaswamy* proportionality test requires that any state action restricting fundamental rights must satisfy four conditions: legality, legitimate aim, proportionality, and procedural safeguards.[33] An AI system that deletes voters from electoral rolls without transparent reasoning, independent audit, or effective appeal mechanisms fails the procedural safeguards prong of this test.

5. The campaign silence period and AI circumvention

Section 126 of the RPA 1951 prohibits the display of election material by means of cinematograph, television, or other similar apparatus during the 48-hour period before polling concludes in a constituency This silence period is designed to give voters space for independent reflection before casting their ballots. AI technologies create multiple avenues for circumventing this protection.

Campaign teams deployed AI chatbots on WhatsApp and Telegram to answer voter queries and deliver targeted messaging even during the legally mandated campaign silence period.[34] Because chatbot interactions occur in

[27]Ministry of Electronics & Information Technology, Proposed Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules (2024).

[28]Election Commission of India, Fresh Advisory on Mandatory Labelling of AI-Generated Content in Election Campaigns (Oct. 2025).

[29]INDIA CONST. art. 324.

[31]Internet Freedom Foundation, Digital Technologies and Electoral Integrity in India (2025).

[32]Policy Circle, Artificial Intelligence and the Indian Electoral Process: Transparency and Accountability Concerns (2025).

[33]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

[34]Manufacturing Reality: How AI Is Rewriting India's Election Playbook, OUTLOOK INDIA (Feb. 23, 2026), https://www.outlookindia.com/national/manufacturing-reality-how-ai-is-rewriting-indias-election-playbook.

private one-on-one or small group messages, they are functionally invisible to electoral regulators. Voice clone calls delivered to individual mobile phones fall into a similar regulatory blind spot, as Section 126 was drafted with public broadcasting in mind and does not clearly cover personalised AI-generated audio delivered through private communication channels.

The Meta advertising investigation further exposed that the platform's systems did not enforce the 48-hour silence period for political advertisements. Ads submitted during this period were approved and could have been published had the researchers not removed them voluntarily. This failure points to a structural limitation: the current regulatory framework assumes that election silence can be maintained by controlling a finite number of broadcast channels, whereas AI enables the mass production and distribution of individualised political content through channels that regulators cannot effectively monitor.

Conclusion

This Article set out to examine whether the Indian legal framework, specifically the Representation of the People Act, 1951 and the Digital Personal Data Protection Act, 2023, adequately addresses the challenges posed by AI-driven voter profiling, deepfake-based electoral manipulation, and synthetic media in Indian elections. The research finds that the answer, on both counts, is no.The RPA 1951, enacted seven decades ago to govern elections in a pre-digital democracy, contains no provision that addresses algorithmic voter targeting, AI-generated synthetic content, or automated distribution of political messaging through private digital channels. Section 123, which defines corrupt practices, was drafted for a world in which a human publisher made a deliberate decision to spread a false statement or exercise undue influence over voters. It was not designed for an environment in which AI systems can generate millions of personalised false messages and distribute them through automated channels that evade regulatory detection. The research has demonstrated this gap through specific evidence: the $50 million spent by political parties on AI-generated campaign content in 2024, the 50 million AI voice clone calls made to voters, the deepfake incidents involving Bollywood actors, deceased political figures, and senior political leaders, and the systematic circumvention of the campaign silence period through AI chatbots operating on private messaging platforms.

REFERENCES

Over 30% Indians Believe AI-Generated Deepfake Content Can Sway Elections: Survey, Business Today (Apr. 26, 2024)

Deepfake Democracy: Behind the AI Trickery Shaping India's 2024 Election, Al Jazeera (Feb. 20, 2024)

Shaping Robust AI Regulation: Lessons from India's 'Deepfake' Election, Harvard Political Review (Dec. 6, 2024)

India's Experiments With AI in the 2024 Elections: The Good, The Bad & The In-between, TechPolicy.Press (Sept. 25, 2024)

The Era of AI-Generated Election Campaigning is Underway in India, TechPolicy.Press (May 25, 2024)

AI Amplifies Political Reach but Magnifies Disinformation in India Elections, Asia Pacific Foundation (June 5, 2024)

AI Companies Are Making Millions Producing Election Content in India, Rest of World (May 23, 2024)

ECI Cracks Down On Deepfakes Before Bihar Polls, MediaNama (Oct. 28, 2025)

Regulation (EU) 2016/679 (General Data Protection Regulation), art. 9

Regulation (EU) 2024/1689 (Artificial Intelligence Act), 2024 O.J. (L 1689) (Articles 5, 6, 8-15, 50; Annex III; Recital 62)

Public Official Election Act (South Korea), amended by Act No. 19756, Dec. 27, 2023 (Articles 82-8, 261)