ISSN: 3048-8702(O)

LLRJ

LEX LUMEN RESEARCH JOURNAL

VOLUME 2 - ISSUE 3

2026

LEX LUMEN RESEARCH JOURNAL-ISSN:3048-8702
Open Access, Double blind-Peer Reviewed Law Journal, Licensed by-CC BY-NC-SA.
Editor-in-Chief: Prof. (Dr). Razit Sharma, Publisher: Mrs. Rachana

Volume-2, Issue-3 ***Pages:613-626***

INTERNATIONAL LEGAL LANDSCAPE OF ARTIFICIAL INTELLIGENCE IN ELECTIONS

By- **Animesh Anand[1] & Dr. Saurabh Siddhartha[2]**

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,

[1] **LL.M (Cyber Law), The ICFAI University, Dehradun.**
[2]**Assistant Professor, The ICFAI University, Dehradun.**

Volume-2, Issue-3 *Pages:613-626*

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 whether Indian electoral law, in its current form, can adequately regulate the deployment of AI in elections. It investigates the statutory gaps in the RPA 1951 concerning algorithmic voter targeting, evaluates the DPDPA's capacity to protect voter data from AI-driven manipulation, and analyses the distribution of legal liability for deepfakes and synthetic political content among AI developers, political parties, and digital intermediaries. 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.

INTRODUCTION:

The regulation of Artificial Intelligence (AI) in electoral processes is not a challenge unique to India. Across the globe, democracies are confronting a common problem: generative AI tools have made it cheap and fast to produce synthetic media that can deceive voters, and existing legal frameworks were not built for this.[3] The responses, however, have varied considerably. The European Union (EU) has opted for a comprehensive risk-based regulatory architecture. The United States has seen state-level legislative action, primarily in California, that has already collided with First Amendment protections. South Korea has imposed criminal penalties for election-period deepfakes. Singapore has enacted targeted legislation prohibiting

[3]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689) [hereinafter EU AI Act].

Volume-2, Issue-3 *Pages:613-626*

digitally manipulated candidate depictions during elections. And Brazil has used judicial regulation through its Superior Electoral Court (TSE) to ban deepfakes and mandate AI content labelling in campaign materials.

THE EUROPEAN UNION: RISK-BASED CLASSIFICATION UNDER THE AI ACT 2024

The EU AI Act, formally adopted as Regulation (EU) 2024/1689, entered into force on 1 August 2024 and is the first comprehensive AI legislation enacted anywhere in the world. The Act establishes a four-tier risk classification system: unacceptable risk (prohibited), high risk (regulated with strict compliance obligations), limited risk (subject to transparency requirements), and minimal risk (unregulated).[4]

AI systems used in the electoral context are addressed at two levels within this framework. At the prohibited level, the Act bans AI systems that deploy subliminal, manipulative, or deceptive techniques to distort behaviour and impair informed decision-making, causing significant harm.[5] This prohibition has direct implications for AI tools designed to manipulate voter behaviour through micro-targeting or emotionally exploitative content, though the Act does not define what constitutes "significant harm" in an electoral context, leaving room for interpretive uncertainty.

At the high-risk level, Annex III of the Act explicitly classifies AI systems "intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons" as high-risk systems.[6] This classification triggers a set of compliance obligations under Articles 8 through 15, including the implementation of risk management systems, data quality standards, technical documentation, transparency requirements, human oversight mechanisms, and accuracy and

[4]High-Level Summary of the AI Act, EU ARTIFICIAL INTELLIGENCE ACT, https://artificialintelligenceact.eu/high-level-summary/ (last visited Apr. 10, 2026).
[5]EU AI Act, supra note 1, art. 5(1)(a).
[6]EU AI Act, supra note 1, Annex III, S. 8(b).

Volume-2, Issue-3 *Pages:613-626*

robustness benchmarks.[78] Providers of high-risk electoral AI systems must conduct conformity assessments before placing their systems on the market and register them in a publicly accessible EU database.[9]

The Act does carve out an exception: AI systems whose output is not directly exposed to voters, such as tools used for administrative or logistical organisation of political campaigns, are excluded from high-risk classification. This distinction is worth noting because it separates internal campaign management tools from voter-facing AI applications, a distinction that Indian law does not make at all.

On the transparency side, Article 50 imposes disclosure obligations for generative AI outputs. Providers of AI systems that generate synthetic audio, image, video, or text content must ensure that the output is marked in a machine-readable format as artificially generated or manipulated.[10] For deepfakes specifically, the Act requires that content which has been artificially generated or manipulated to appear authentic must be clearly and visually labelled.[11] This labelling obligation applies to all deepfakes, not just those produced during election periods, making the EU framework broader in temporal scope than the election-specific laws adopted by South Korea or Singapore.

The enforcement timeline is staggered. Prohibited practices took effect in February 2025. General-purpose AI obligations became applicable in August 2025. High-risk system obligations, including those for electoral AI, will take full effect by August 2027.[12] This phased implementation means that the election-specific provisions are

[7]EU AI Act, supra note 1, arts. 8-15.
[8]EU AI Act, supra note 1, art. 9.
[9]EU AI Act, supra note 1, art. 6.
[10]EU AI Act, supra note 1, art. 50.

[11]EU AI Act, supra note 1, Recital 62.
[12]AI Act, Shaping Europe's Digital Future, European Commission, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (last visited Apr. 10, 2026).

Volume-2, Issue-3 *Pages:613-626*

not yet fully enforceable, which limits the Act's immediate practical impact on upcoming European elections.

THE UNITED STATES: STATE-LEVEL RESPONSIVES AND CONSTITUTIONAL TENSIONS

The United States has no federal legislation specifically regulating AI use in elections. The Federal Election Commission (FEC) initiated proceedings to examine whether existing regulations on fraudulent misrepresentation could cover AI-generated campaign content, but no binding federal rules have emerged.[13] The regulatory action has instead come from individual states. By the end of 2024, twenty states had enacted some form of election-related deepfake legislation.[14]

California's 2024 legislative package provides the most detailed state-level response. Governor Gavin Newsom signed three bills into law on September 17, 2024: AB 2655 (the Defending Democracy from Deepfake Deception Act), AB 2839 (Elections: Deceptive Media in Advertisements), and AB 2355 (Political Advertisements: Artificial Intelligence).[15]

AB 2655 targets large online platforms, defined as those with at least one million California users in the preceding twelve months. It requires such platforms to block the posting of "materially deceptive content" related to California elections during the 120 days before an election, label reported content within 72 hours, and develop reporting procedures for residents to flag non-compliant content.[16][17] AB 2839

[13]Political Deepfakes and Elections, THE FIRST AMENDMENT ENCYCLOPEDIA (Jan. 11, 2025), https://firstamendment.mtsu.edu/article/political-deepfakes-and-elections/.
[14]Id. (noting that by end of 2024, twenty states had enacted election-related deepfake laws).
[15]Governor Newsom Signs Bills to Combat Deepfake Election Content, OFF. OF THE GOVERNOR, STATE OF CAL. (Sept. 17, 2024), https://www.gov.ca.gov/2024/09/17/governor-newsom-signs-bills-to-combat-deepfake-election-content/.
[16]AB 2655, Defending Democracy from Deepfake Deception Act of 2024, 2024 Cal. Stat. ch. 710 (codified at CAL. ELEC. CODE S.S. 20510-20518).
[17]California Enacts New Laws to Combat AI-Generated Deceptive Election Content, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP (Sept. 27, 2024).

Volume-2, Issue-3 *Pages:613-626*

broadens the scope beyond platforms to cover any person, committee, or entity, prohibiting the knowing distribution of deceptive AI-generated or manipulated content 120 days before an election and 60 days after. It authorises affected candidates and officials to file civil actions seeking injunctive relief and damages.[18] AB 2355 mandates that any political advertisement created or published by a political committee must include a clear disclaimer if AI was used to generate or substantially alter the content.[19]

However, this legislative package ran into immediate constitutional challenge. On the same day the bills were signed, content creator Christopher Kohls, who had produced an AI-altered parody video of Vice President Kamala Harris, filed suit in the Eastern District of California alleging First Amendment violations.[20] Senior U.S. District Judge John Mendez granted a preliminary injunction against AB 2839 in October 2024, describing it as "a blunt tool that hinders humorous expression and unconstitutionally stifles the free and unfettered exchange of ideas." In August 2025, Judge Mendez struck down AB 2655 on federal preemption grounds, holding that it violated Section 230 of the Communications Decency Act which protects platforms from civil liability for third-party content.[21] AB 2839 was permanently blocked in a separate order later that month.[22]

The California experience illustrates a fundamental tension in the American legal system between regulating deceptive AI content in elections and protecting political speech under the First Amendment. The courts have historically afforded strong protection to political expression, even when that expression involves deliberate falsehoods, as the Supreme Court held in *New York Times v. Sullivan*. This

[18]AB 2839, Elections: Deceptive Media in Advertisements, 2024 Cal. Stat. ch. 709.
[19]AB 2355, Political Reform Act of 1974: Political Advertisements: Artificial Intelligence, 2024 Cal. Stat. ch. 708.
[20]Kohls v. Bonta, No. 2:24-cv-02527 (E.D. Cal. Oct. 2, 2024) (order granting preliminary injunction against AB 2839).
[21]Federal Judge Strikes Down California Deepfake Law, THE CONFERENCE BOARD (Aug. 5, 2025).
[22]AI Deepfake Policy in California, BALLOTPEDIA, https://ballotpedia.org/AI_deepfake_policy_in_California (last visited Apr. 10, 2026).

Volume-2, Issue-3 *Pages:613-626*

constitutional barrier does not exist in the same form in India's legal framework, where Article 19(2) permits reasonable restrictions on speech in the interests of, among other things, public order and the sovereignty of the state. This difference in constitutional architecture makes the American experience instructive as a cautionary example rather than a model for adoption.

SOUTH KOREA: CRIMINAL SANCTIONS FOR ELECTORAL DEEPFAKES

South Korea adopted one of the earliest and most aggressive legislative responses to AI-generated election content. In December 2023, the National Assembly amended the Public Official Election Act (POEA) to impose a blanket ban on election-related deepfakes during the 90 days before an election.[23] The amendment came in the wake of a specific incident during the May 2022 local elections, when a deepfake video of President Yoon Suk-yeol appearing to endorse a local candidate circulated on social media.[24]

Under the amended POEA, any person who shows or distributes political campaign videos, images, or audio created using deepfake technology within the 90-day pre-election window faces a maximum sentence of seven years imprisonment or a fine of up to 50 million won (approximately $37,600).[2526] Outside this 90-day period, anyone who produces, edits, distributes, or posts election-related deepfakes must clearly indicate that the content is "virtual content" created using AI technology, in accordance with regulations issued by the National Election Commission (NEC).[27] Failure to comply with this labelling requirement carries a separate fine of up to 10 million won.

[23]Public Official Election Act, amended by Act No. 19756, Dec. 27, 2023, art. 82-8 (S. Kor.).
[24]AI and Elections: Lessons From South Korea, THE DIPLOMAT (May 2024).
[25]Id. art. 82-8, para. 1.
[26]Id. art. 261, para. 3.
[27]Lasse Schuldt, Every Fake You Make: Blanket Deepfake Bans Are the Next Level in Asia's War on Fake News, VERFASSUNGSBLOG (Oct. 9, 2024).

Volume-2, Issue-3 *Pages:613-626*

The NEC identified 129 instances of election-related deepfake content between January 29 and February 16, 2024 alone, in the run-up to the April 10 National Assembly elections.[28] Despite these numbers, the limited impact of AI-generated disinformation on the actual election outcome was attributed to a combination of legislative deterrence, platform monitoring by companies like Naver, and NEC enforcement.[29]

As Schuldt (2024) observed, the South Korean law represents a departure from earlier fake news legislation across Asia. Previous laws in countries like Singapore (POFMA 2019) and Malaysia (Anti-Fake News Act 2018) typically required proof of probable harm. The amended POEA criminalises every election-related deepfake during the 90-day period without requiring any demonstration that the content caused or was likely to cause harm. This conduct-based approach rather than harm-based approach makes the South Korean model one of the strictest in the world.

In December 2024, the National Assembly went further by passing the AI Basic Act, which establishes a general framework for AI governance in South Korea. However, the Basic Act does not specifically address election-related AI, focusing instead on the classification and regulation of "high-impact AI systems" and imposing obligations on AI developers and deployers.[3031] The election-specific provisions remain within the POEA, creating a dual-track regulatory architecture where general AI governance and election-specific AI regulation operate through separate statutes.

[28]April 10 Elections Under Threat from AI Deepfake Manipulation, THE KOREA TIMES (Feb. 20, 2024).

[29]South Korea Contends with AI and Electoral Integrity, EAST ASIA FORUM (Apr. 1, 2024).

[30]South Korea's Evolving AI Regulations, STIMSON CENTER (June 12, 2025).

[31]AI Basic Act (Act on the Development of Artificial Intelligence and the Establishment of Foundation for Trustworthiness), Act No. 20677, Dec. 26, 2024 (S. Kor.).

Volume-2, Issue-3 *Pages:613-626*

SINGAPORE: TARGETED REGULATION OF DIGITALLY MANIPULATED ELECTION CONTENT

Singapore's approach is distinguished by its precision. On October 15, 2024, Parliament passed the Elections (Integrity of Online Advertising) (Amendment) Bill, which amends both the Parliamentary Elections Act 1954 and the Presidential Elections Act 1991.[32] The Bill came into effect for the first time during the writ of election issued on April 15, 2025, ahead of the May 3, 2025 general election.[33]

The new Section 61MA of the Parliamentary Elections Act makes it an offence to publish online election advertising that contains "realistic representations, created using content that was digitally generated or manipulated, of a candidate saying or doing something that he or she did not in fact say or do."[34] This prohibition applies from the issuance of the writ of election until the close of polling on polling day. The temporal scope is narrower than South Korea's 90-day window, applying only during the formal election period.

The Bill empowers the Returning Officer (RO) to issue corrective directions requiring individuals, social media services, and Internet Access Service Providers to remove offending content or disable access by Singapore users during the election period.[35] Failure to comply with a corrective direction is punishable by a fine of up to SGD 1,000 or imprisonment of up to 12 months for individuals, and up to SGD 1,000,000 for social media platforms.[36] Candidates who have been misrepresented by deepfake content can request the RO to review and act on such content.[37]

[32]Elections (Integrity of Online Advertising) (Amendment) Bill, Bill No. 29/2024, Parliament of Singapore (passed Oct. 15, 2024) [hereinafter Singapore Amendment Bill].
[33]Singapore: Ban on the Publication, Boosting, Sharing and Reposting of Deepfake Content Depicting Election Candidates Comes into Effect, BAKER MCKENZIE (May 2, 2025).
[34]Singapore Amendment Bill, supra note 30, S. 61MA.
[35]New Measures Against Digitally Manipulated Content and Deepfakes During Elections, RAJAH & TANN ASIA (Oct. 2024).
[36]Singapore's Elections (Integrity of Online Advertising) (Amendment) Act: Key Provisions & Penalties, FACIA.AI (Sept. 17, 2025).
[37]New Legal Measures to Uphold Integrity of Online Advertising During Elections, MINISTRY OF DIGITAL DEVELOPMENT AND INFORMATION, SINGAPORE (Sept. 9, 2024).

Volume-2, Issue-3 *Pages:613-626*

The penalties for creating or disseminating prohibited content are substantial: fines of up to SGD 50,000 and imprisonment of up to five years, with doubled penalties if the content is likely to affect the election outcome.[38] There is a defence available for accused persons who can prove that they did not know and had no reason to believe that the representation of the candidate was untrue. The Bill also exempts inoffensive manipulations such as animated characters, beauty filters, or memes that do not mislead or harm public order.

What is notable about Singapore's approach is its institutional design. Rather than relying on courts or a separate regulatory body, enforcement is channelled through the Returning Officer, an existing election official who can issue corrective directions in real time during the election period. This avoids the delays inherent in judicial proceedings and allows for rapid removal of deepfake content, a practical necessity given that elections in Singapore are typically conducted within a compressed timeframe.

BRAZIL: JUDICIAL REGULATION THROUGH TSE RESOLUTION No. 23.732/2024

Brazil's regulatory response has taken a distinctive institutional form. Unlike the legislative approaches seen in the EU, South Korea, and Singapore, Brazil's regulation of AI in elections has been primarily driven by the Superior Electoral Court (TSE), which exercises both judicial and administrative authority over elections under Article 23, IX of the Electoral Code.[39] In February 2024, more than six months before the October municipal elections, the TSE approved Resolution No. 23.732/2024, which amended the existing electoral propaganda regulation (Resolution No. 23.610/2019) to incorporate twelve measures addressing AI use in campaigns.[40]

[38]Singapore Bans Deepfakes in Elections, REED SMITH (Nov. 4, 2024).
[39]Brazilian Judges Regulate Elections ... and AI, VERFASSUNGSBLOG (Mar. 15, 2024).
[40]Regulating the Use of AI for Brazilian Elections: What's at Stake, ATLANTIC COUNCIL DFRLAB (May 29, 2024).

Volume-2, Issue-3 *Pages:613-626*

The Resolution imposes two core obligations. First, it mandates that any campaign content generated or edited by AI must feature a disclaimer acknowledging the use of AI, including specification of the tool employed.[41] Second, it imposes an outright ban on the use of deepfakes in elections, specifically prohibiting "the use of synthetic content in audio, video format or a combination of both, which has been digitally generated or manipulated, even with authorization, to create, replace or alter the image or voice of a living, deceased or fictitious person" to harm or favour a candidacy.[42] Candidates who deploy deepfakes face the revocation of their electoral registration or mandate.

In August 2024, the TSE signed memorandums of understanding with Meta, TikTok, LinkedIn, Kwai, X, Google, and Telegram, securing commitments from these platforms to act in partnership with Brazilian authorities to remove disinformation content during the election period.[43] These agreements were valid through December 31, 2024. The TSE also operated an Electoral Disinformation Alert System enabling citizens to report suspicious content.

The DFRLab's six-month monitoring study (May to October 2024) identified seventy-eight instances of content directly related to local candidates that was either confirmed or alleged to be synthetic.[44] However, the study also found significant enforcement difficulties. Local court rulings across the country lacked consistency in classifying deepfakes. In one case, a judge rejected the classification of an obviously manipulated image as a deepfake, calling it a "crude montage" rather than a deepfake. The DFRLab concluded that the regulations exposed confusion stemming from both a misunderstanding of the definition of deepfakes and a lack of clarity in the electoral rules regarding the classification of synthetic content.

[41]The Challenges of Identifying Deepfakes Ahead of the 2024 Brazil Election, ATLANTIC COUNCIL DFRLAB (Oct. 2, 2024).
[42]TSE Resolution, supra note 37, art. 9-B.
[43]Post Elections Briefing: Brazil, DIGITAL ACTION (Mar. 20, 2025).
[44]Brazil's Electoral Deepfake Law Tested as AI-Generated Content Targeted Local Elections, ATLANTIC COUNCIL DFRLAB (Nov. 26, 2024).

Volume-2, Issue-3 *Pages:613-626*

Brazil's experience also revealed a gendered dimension of AI-driven electoral harm. Deepfake technology was used to target women candidates through fabricated intimate imagery, aiming to damage their reputations and deter participation.[45] This pattern of gender-based AI attacks in elections have not been adequately addressed by any of the jurisdictions examined it raises questions about whether election-specific AI regulation needs to incorporate gender-sensitive protections.

IMPLICATIONS FOR THE INDIAN ELECTORAL FRAMEWORK

India's current regulatory position on AI in elections consists almost entirely of non-binding ECI advisories. The March 2024 advisory directing parties to remove deepfakes within three hours and the October 2025 advisory mandating labelling of AI-generated content lack statutory authority and detailed enforcement mechanisms.[46] The RPA 1951 does not address AI-driven practices under its corrupt practice's provisions.[47] The DPDPA 2023 grants broad exemptions to state instrumentalities under Section 17 that could allow the ECI to process voter data outside the Act's protections.[48]

The comparative analysis suggests four specific reform directions for India. First, drawing from the EU model, India could classify voter-facing electoral AI systems as high-risk under a sector-specific framework, requiring conformity assessments, transparency documentation, and human oversight. Second, drawing from South Korea and Singapore, India could enact criminal sanctions for the creation and distribution of election-related deepfakes during a defined pre-election period, with mandatory labelling requirements outside that period. Third, drawing from Brazil, India could mandate AI content disclaimers in all campaign materials and establish a real-time reporting mechanism for citizens to flag synthetic electoral content. Fourth,

[45]Artificial Intelligence and Information Integrity: Latin American Experiences, INT'L IDEA, Policy Paper No. 34 (2025).
[46]Election Commission of India, Advisory on Responsible Use of Artificial Intelligence and Synthetic Media in Election Campaigns (Mar. 2024).
[47]The Representation of the People Act, 1951, No. 43 of 1951, S. 123, INDIA CODE (1951).
[48]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, S. 17, INDIA CODE (2023).

Volume-2, Issue-3 *Pages:613-626*

unlike any of the jurisdictions examined, India should address the gap in algorithmic transparency within the ECI itself, requiring the Commission to disclose the AI tools it uses for electoral administration and to subject these tools to independent audit.

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.

The DPDPA 2023, despite being India's first comprehensive data protection statute, is structurally inadequate for the electoral context. Its failure to classify political opinions as sensitive data, its broad exemptions for state instrumentalities under Section 17, and its delayed enforcement timeline mean that voter data processed during the most consequential elections in Indian history has been and continues to

Volume-2, Issue-3 *Pages:613-626*

be processed outside any effective data protection framework. The Aadhaar-voter ID linkage program, which Justice B.N. Srikrishna described as creating conditions for a "Delhi Analytica,"further compounds the risk by enabling cross-referencing of voter data with banking, telecom, and welfare databases at a scale that makes comprehensive voter profiling not just possible but practically inevitable.

The intermediary liability framework under the IT Act fares no better. Meta's approval of 14 inflammatory AI-generated political advertisements during the 2024 elections, including during the legally mandated silence period and YouTube's blanket approval of test advertisements containing misinformation and incitement to violence demonstrate that the conditional immunity model of Section 79 is not fit for purpose in an era when platforms actively deploy AI-powered advertising systems that approve, target, and distribute political content.The World Economic Forum identified AI-driven misinformation as the single most severe global risk in the near term. India, with 960 million registered voters, 760 million internet users, and extraordinary linguistic and demographic diversity, sits at the epicentre of this risk. The evidence from 2024 and 2025 shows that AI-driven electoral manipulation is not a future threat but a present reality. BOOM's 2025 annual report documented that AI-generated disinformation more than doubled compared to 2024, with fake news bulletins, fabricated celebrity endorsements, and manipulated videos of political leaders circulating with increasing sophistication.