LEGAL FRAMEWORK AND CHALLENGES OF DEEPFAKE TECHNOLOGY IN INDIAN POLITICS AND ELECTIONS

Abhishek Choudhary[*]

ABSTRACT

This article explores the rapid rise of deepfake technology in Indian electoral politics, focusing on its misuse, legal ambiguity, and broader democratic implications. It will examine how AI-generated synthetic media, ranging from doctored videos of politicians like Rahul Gandhi and Kamal Nath to impersonations of celebrities, have been used to sway opinion and disrupt democratic discourse, tracing how synthetic media infiltrated public discourse and shaped digital narratives. India's present framework, the Information Technology Act 2000,[1] Bharatiya Nyaya Sanhita 2023,[2] Digital Personal Data Protection Act 2023,[3] and the IT (Intermediary Guidelines and Digital Media Ethics Code)[4] Rules 2021, addresses related harms such as impersonation, defamation and obscenity, and the Election Commission has issued targeted advisories.[5] Yet none defines deepfakes or mandates provenance and labelling at scale. This article synthesises the legal position, presents case studies from 2023–2025, For instance, a viral AI-generated video showed Rahul Gandhi announcing policies he never endorsed, confusing thousands within hours on WhatsApp by analyzing high-profile cases from recent elections and comparing India's approach with regulations in the United States, European Union, and China, we identify critical gaps in protection and accountability. Our recommendations include enacting targeted deepfake legislation, mandating disclosures and watermarks for political content, reinforcing rapid takedown policies, empowering victims, especially women and expanding digital literacy. Taken together, these measures point toward

[*] BA LLB, SECOND YEAR, MUMBAI UNIVERSITY, RIZVI LAW COLLEGE.

[1] Information Technology Act 2000 (India)

[2] Bharatiya Nyaya Sanhita 2023 (India)

[3] Digital Personal Data Protection Act 2023 (India)

[4] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (India)

[5] Election Commission of India, *Compendium of Instructions on Model Code of Conduct* (ECI 30 January 2018) https://ceoelection.bihar.gov.in/pdf/Compendium_MCC.pdf accessed 18 October 2025

a multi-layered strategy essential for safeguarding the integrity of India's democracy amid rising synthetic media threats.

Keywords: Deepfakes, Indian Elections, IT Act, Bharatiya Nyaya Sanhita, 2023, DPDP.

INTRODUCTION

Deepfakes use advanced algorithms to create hyper-realistic videos and audio that show people saying or doing things they never actually did. Today, inexpensive software lets almost anyone clone voices, lip-sync speeches, or swap faces with ease. In India, a country where mobile access and multilingual platforms dominate, these fake media spread rapidly through encrypted messaging apps and short-video channels.[6] The 2024 General Election saw deepfakes weaponised as campaign tools: deceased leaders were brought back to life digitally, actors were shown backing parties without their consent, and candidates appeared to announce policies they hadn't proposed. Even after these fakes are exposed, they can still shape first impressions, stoke controversy, and discourage voter turnout. This rising threat presents a complex challenge: how do we stop harmful synthetic media without undermining space for satire, creative remix, or legitimate political criticism?[7]

TECHNOLOGY PRIMER: HOW POLITICAL DEEPFAKES ARE MADE AND DETECTED

Most visual deepfakes are created using generative adversarial networks (GANs) or diffusion models, which learn from thousands of images or videos of a specific person to produce convincing new material.[8] For audio, neural networks analyse voice patterns and spectrograms to clone someone's speech, replicating everything from their tone to their rhythm. But it's not just cutting-edge tools; simple video editors and audio overdubs can also be used for quick and inexpensive fakes.

Detecting deepfakes is an ongoing challenge. For video, experts look for telltale signs like unnatural blinking, mismatched lighting, odd facial angles, or subtle artefacts that betray

[6] Josh A Goldstein and Andrew Lohn, 'Deepfakes, Elections, and Shrinking the Liar's Dividend' Brennan Center for Justice (23 January 2024) https://www.brennancenter.org/our-work/research-reports/deepfakes-elections-and-shrinking-liars-dividend accessed 18 October 2025.

[7] World Economic Forum, The Global Risks Report 2024 (2024) https://www3.weforum.org/docs/WEF_TheGlobalRisksReport2024.pdf accessed 18 October 2025; IPSOS, '2024 Voter Misinformation Survey' (2024).

[8] Goldstein (n6).

manipulation. In audio, they search for spectral glitches, tiny inconsistencies in the waveform. Another approach is to trace content back to its origin, verifying it against known provenance markers.[9]

As deepfake technology improves, so do detection methods. This arms race means we can't rely on technical tools alone. Effective governance must combine smart detection with process controls like requiring disclosures, adding watermarks to synthetic media, and ensuring platforms respond rapidly to reported fakes.[10]

INDIA'S CURRENT LEGAL FRAMEWORK

India does not yet define or regulate 'deepfakes' as a distinct legal category. Instead, a patchwork of norms covers downstream harms: the Information Technology Act 2000[11] (IT Act), The Bharatiya Nyaya Sanhita 2023[12] (BNS), The Digital Personal Data Protection Act 2023[13] (DPDP), and the IT (Intermediary Guidelines and Digital Media Ethics Code)[14] Rules 2021 ('IT Rules 2021'). During elections, the Election Commission of India[15] (ECI) relies on the Model Code of Conduct and specific advisories.

Information Technology Act 2000:[16] The IT Act was written long before today's AI-powered deepfakes, but several provisions still come into play, like:

- **Section 66C** addresses identity theft by punishing those who fraudulently use another person's electronic signature or credentials, which is relevant for deepfake impersonations.[17]
- **Section 66D** addresses cheating by personation using computer resources. This provision has been invoked in political deepfake cases, but requires evidence of intent.[18]
- **Section 66E** punishes the non-consensual capturing or sharing of private images, though the synthetic nature of deepfakes complicates its application here.[19]

[9] ibid
[10] Ministry of Electronics and Information Technology, 'Advisory to Intermediaries on Deepfakes' (15 March 2024)
[11] Information Technology Act 2000 (India).
[12] Bharatiya Nyaya Sanhita 2023 (India).
[13] Digital Personal Data Protection Act 2023 (India)
[14] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (India).
[15] Election Commission of India, Press Note... (2024).
[16] Information Technology Act 2000 (India) .
[17] Information Technology Act 2000 (India) s 66C.
[18] Information Technology Act 2000 (India) ss 66D
[19] Information Technology Act 2000 (India) s 66E.

- **Sections 67 and 67A** focus on obscene or sexually explicit content, thereby applying to intimate deepfakes.[20]
- **Section 79 (Safe Harbour)** provides platforms with conditional immunity if they remove unlawful content diligently.[21] This was clarified in *Shreya Singhal v Union of India,*[22] which held that platforms are only required to remove material on orders from a court or a government agency, balancing platform neutrality against harm prevention.

Bharatiya Nyaya Sanhita 2023:[23] The BNS replaces the IPC and modernises offences relevant to synthetic impersonation, such as:

- **Sections 318 and 319** address digital fraud and personation, suitable to tackle deepfake-enabled scams.[24]
- **Section 353** targets public mischief, which extends to disinformation spread by deepfakes.[25]
- **Section 356** covers defamation, providing a remedy for reputational damage caused by deepfake media.[26]

These can apply to deceptive videos or audio that induce harm or erode public tranquillity. Still, attribution, cross-border evidence. Prosecutors must adapt and stretch these provisions to fit, and it’s often tough to prove who made the video, or if there was real intent to deceive.

Digital Personal Data Protection Act 2023:[27] The DPDP Act regulates the processing of personal data (including images, voice and biometrics), potentially covering non-consensual synthetic use of a person’s likeness.[28] However, the widespread exemption for publicly available data often relevant to celebrities limits its protective reach, and the Act does not address provenance or labelling of synthetic content.

IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021:[29] The IT Rules 2021 require platforms to exercise due diligence, use automated tools to identify and remove

[20] Information Technology Act 2000 (India) ss 67, 67A
[21] Information Technology Act 2000 (India) s 79.
[22] Shreya Singhal v Union of India (2015) 5 SCC 1 (SC).
[23] Bharatiya Nyaya Sanhita 2023
[24] Bharatiya Nyaya Sanhita 2023 (India) s 318, s 319
[25] Bharatiya Nyaya Sanhita 2023 (India) s 353
[26] Bharatiya Nyaya Sanhita 2023 (India) s 356
[27] Digital Personal Data Protection Act 2023 (India)
[28] Digital Personal Data Protection Act 2023 (India) s 4–7
[29] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (India)

unlawful content such as deepfakes, act promptly on flagged content (especially during elections), and comply with government advisories regarding detection, labelling, and removal.[30]

Election Commission guidance and Model Code:[31] For the 2024 elections, the ECI mandated clear labelling of AI-generated or synthetic content by political parties and candidates. Required pre-certification of campaign content and fast removal of fake materials, with penalties for non-compliance. Sent advisory letters warning parties that misleading deepfakes are strictly prohibited. The ECI also set up a Deepfakes Analysis Unit to coordinate takedowns and checks. While these measures showed regulatory assertiveness, they were time-bound and limited to registered parties during the campaign period. In sum, India's existing legal and regulatory response to deepfakes is reactive and fragmented, relying on the adaptation of general laws rather than deepfake-specific regulation.[32]

DEEPFAKES IN INDIAN ELECTIONS: CASE STUDIES

Indian elections in 2024 saw an unprecedented wave of deepfake activity. Bollywood stars became prime targets. Both Aamir Khan and Ranveer Singh were swept up in deepfake controversies during the 2024 elections.[33] Convincingly realistic videos surfaced online, one falsely showing Khan endorsing a political party, the other portraying Singh criticising Prime Minister Modi. Millions, particularly in rural and semi-urban communities, initially believed these fabricated clips. While Ranveer Singh promptly reported the incident to the police, tracing and prosecuting the creators proved to be a significant challenge.

Deepfakes also resurrected the voices and likenesses of deceased political icons. Campaign videos featuring *M. Karunanidhi* and *J. Jayalalithaa*,[34] both long gone, they were AI-generated to make it seem as though they were endorsing current candidates. These synthetic appearances

[30] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (India)
[31] Election Commission of India, *Compendium of Instructions on Model Code of Conduct* (ECI 30 January 2018) https://ceoelection.bihar.gov.in/pdf/Compendium_MCC.pdf accessed 18 October 2025
[32] Election Commission of India, 'Press Note: Responsible and Ethical Use of Social Media – Removal of Fake Content within Three Hours' (6 May 2024) NoECI/PN/72/2024 https://elections24.eci.gov.in/docs/5ylWJLjQBX.pdf accessed 18 October 2025
[33] Hindustantimes,'Deepfakes of Aamir Khan and Ranveer Singh raise worries over AI misuse in Lok Sabha election'(2024)
[34] GNET Research, 'Deep Fakes, Deeper Impacts: AI's Role in the 2024 Indian General Election and Beyond' (10 September 2024) https://gnet-research.org/2024/09/11/deep-fakes-deeper-impacts-ais-role-in-the-2024-indian-general-election-and-beyond/ accessed 18 October 2025.

stirred their supporters and raised difficult ethical and legal questions about digital legacy and consent.

Female politicians in India have endured especially damaging attacks during recent elections, as non-consensual and sexually explicit deepfakes circulated widely online. These fake videos not only inflicted significant emotional distress and harmed professional reputations but also undermined their sense of personal safety and eroded public trust in the democratic process. Many targeted women faced relentless online harassment and felt isolated or powerless to respond, highlighting how deepfakes can compound existing gendered risks in political life.[35]

DEMOCRATIC IMPACT

A large number of new voters found it difficult to distinguish genuine information from fake news. Studies indicate that over one-third of first-time voters were influenced by misleading content, much of which circulated through WhatsApp — now one of the main sources of political information for many citizens.[36]

Manipulated videos and posts, including deepfakes, were deliberately targeted at India’s social divisions. They often played on religious and caste-based sensitivities, deepening mistrust and hostility among communities.[37] The widespread use of digital misinformation led to growing skepticism among voters. Many began to doubt the credibility of political messages, media reports, and even official communications, weakening faith in democratic institutions.[38] Political campaigns increasingly relied on micro-targeted deepfakes to present different narratives to different groups. As a result, voters received conflicting promises and messages, creating confusion and distorting their understanding of real political agendas.

JUDICIAL RESPONSES: HOW INDIAN COURTS ARE TACKLING DEEPFAKES

Two landmark Supreme Court judgments shape how deepfakes might be regulated in India. The first, Justice K.S. Puttaswamy v. Union of India (2017),[39] made it clear that privacy is a fundamental right. So, if someone’s digital likeness or biometric data is misused in a deepfake,

[35] World Economic Forum (n 7)
[36] Koan Advisory, ‘The Impact of Misinformation on Indian Voters’ (2024) https://www.koanadvisory.com/wp-content/uploads/2024/05/From-Smartphones-to-Ballot-Boxes-The-Impact-of-Misinformation-on-Indian-Voters-Report_compressed.pdf accessed 18 October 2025
[37] GNET Research (n 34)
[38] World Economic Forum (n 7)
[39] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (SC)

it isn't just a technical violation—it strikes at the heart of personal autonomy and dignity. Any law that regulates deepfakes must, therefore, be grounded in legality, necessity and must be proportionate to the harm caused.

The second, Shreya Singhal v. Union of India (2015),[40] set another important precedent by striking down Section 66A of the IT Act[41] because it was vague and overbroad. The Court said that online content should only be removed when there is a clear government or court order. All new laws, especially those targeting deepfakes, need to be clearly defined and have proper procedural safeguards.

The Delhi High Court recognised Anil Kapoor's personality rights when his digital likeness and mannerisms were misused in deepfakes for commercial gain.[42] Courts have taken the view that these rights, protected under Article 21,[43] including shielding people from AI-driven impersonation. Most deepfake complaints lead to police reports, but actual prosecutions rarely succeed. The main obstacles are the technical difficulty in tracking down creators, the global spread of this kind of content, and its ability to go viral fast.

CHALLENGES AND GAPS: WHAT THE LAW STILL MISSES

India doesn't yet have a law that directly targets deepfakes—there's a Deepfake Prevention Bill in the works, but it hasn't been passed. The definitions of "deepfake" or "synthetic media" are still fuzzy, leading to uneven enforcement. Existing laws tend to react after harm has happened, rather than proactively requiring creators to label AI-generated content or be held accountable.[44] Any restriction on deepfakes has to walk a tightrope: if it's too broad, it could violate free speech rights under Article 19(1)(a).[45] Courts have insisted that curbs on such content must be clearly spelt out, serve legitimate aims, and address the specific harm involved proportionately.

Tracking deepfake creators is hard, especially when platforms are encrypted or content comes from overseas. Even with new platform rules, companies are often slow to remove deepfakes. Plus, global operations and "safe harbour" rules mean platforms aren't always held to account

[40] Shreya Singhal v Union of India (2015) 5 SCC 1 (SC)
[41] Information Technology Act 2000 (India) s 66A
[42] Anil Kapoor v Simply Life India Ors, CS (COMM) 652/2023 (Del HC, 20 September 2023).
[43] Constitution of India art 21
[44] PIB, 'Government of India Taking Measures To Tackle Deepfakes' (Press Release, 3 April 2025) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2119050 accessed 18 October 2025
[45] Constitution of India art 19(1)(a).

under Indian law. Women, minorities, and vulnerable groups face the brunt of non-consensual intimate deepfakes. Support systems are lacking; there aren't enough mechanisms for rapid takedown, trauma-informed support, or ensuring anonymity for victims. Current takedown procedures simply aren't fast enough given how quickly deepfakes can spread online. While platforms are protected by safe harbour laws as long as they meet their obligations, debates continue about whether they should be made to scan proactively for harmful content—a move that brings its own privacy and legal questions.[46]

COMPARATIVE ANALYSIS: GLOBAL REGULATORY APPROACHES

In the United States, regulation of deepfakes largely occurs at the state level, rather than through a single federal framework. Several states, such as California, Texas, and Virginia, have enacted laws criminalising deepfakes related to elections or non-consensual intimate content. However, the First Amendment's[47] strong protection of free speech limits how far these laws can go. As a result, most American regulations are narrow and intent-based, focusing only on content created with clear malicious or deceptive intent.

The European Union has adopted a comprehensive and proactive framework for addressing the risks posed by deepfakes and AI-generated content. The AI Act (2024)[48] introduces mandatory risk assessments and transparency requirements, obliging developers and platforms to identify, label, and manage AI-generated media. The Digital Services Act (DSA)[49] strengthens platform accountability, requiring swift removal of harmful or illegal content and transparency in moderation practices. Additionally, the General Data Protection Regulation (GDPR)[50] applies to any biometric or personal data used in deepfakes, reinforcing individuals' control over their digital likeness.

China follows a strict, state-driven regulatory model. Under the Deep Synthesis Regulations (2023),[51] all AI-generated content must be clearly labelled as synthetic. Platforms are legally required to detect, monitor, and remove harmful deepfakes proactively. Violations attract

[46] Election Commission of India, Press Note (2024)
[47] US Const amend I
[48] Regulation (EU) 2024/1689 Artificial Intelligence Act OJ L
[49] Regulation (EU) 2022/2065 Digital Services Act OJ L 277
[50] Regulation (EU) 2016/679 General Data Protection Regulation OJ L 119
[51] Cyberspace Administration of China, 'Provisions on the Administration of Deep Synthesis Internet Information Services' (10 January 2023) https://www.chinalawtranslate.com/en/deep-synthesis accessed 18 October 2025

severe penalties, reflecting China's focus on national security, social stability, and information control.

What India Can Take Away. India can look at these varied models and combine their best elements. Targeted laws, mandatory disclosure, clear rules for platforms, cross-border cooperation, and victim-focused remedies could offer a balanced and effective way to regulate deepfakes while upholding constitutional rights and social sensitivities.

RECOMMENDATIONS

India urgently needs a comprehensive and clearly defined Deepfake Prevention Bill[52] to tackle the growing misuse of synthetic and manipulated media. The proposed law should specify what qualifies as a "deepfake" and impose penalties for its malicious creation or circulation, especially in cases linked to elections, non-consensual sexual content, impersonation, and fraud. At the same time, it must protect legitimate forms of expression such as satire, parody, and investigative journalism. The Information Technology Act, 2000,[53] should also be updated to explicitly cover synthetic media and make the safe harbour protection of intermediary's conditional upon proactive monitoring and timely removal of harmful content. In addition, the Digital Personal Data Protection Act (DPDPA)[54] it should narrow its public data exceptions to prevent the misuse of biometric and facial data for generating deepfakes.

To limit the spread of harmful deepfakes, watermarking and authentication should be made compulsory for all AI-generated content. Building verification systems using blockchain technology and setting up a national deepfake detection centre will help trace the origin of suspicious media. It's also important to make detection tools open-source for use by fact-checkers and the general public.[55]

Specialised cybercrime units and a well-trained judiciary are vital for enforcement. The Election Commission should receive the technical upgrade needed to tackle AI-based threats

[52] THE DEEPFAKE PREVENTION AND CRIMINALISATION BILL, 2023 (Bill No.LXX of 2023) https://sansad.in/getFile/BillsTexts/RSBillTexts/Asintroduced/2e214202543549PM.pdf accessed 18 October 2025.

[53] Information Technology Act 2000 (India).

[54] Digital Personal Data Protection Act 2023 (India) s 4–7

[55] Government of India Taking Measures To Tackle Deepfakes (Press Information Bureau (PIB), 3 April 2025) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2119050 accessed 18 October 2025

during campaigns. Victim support and takedown processes should be quick, standardised, and include trauma-informed care.[56]

Dedicated reporting portals can ensure anonymity and provide immediate counselling, especially for women and marginalised groups targeted by deepfakes. Laws should focus on issues of consent and dignity rather than just obscenity. A nationwide campaign is needed to teach people how to spot deepfakes and stay safe online. Supporting independent fact-checkers and curriculum changes in schools will help build a digitally literate, resilient society. India must negotiate treaties that make it easier to share evidence and remove harmful content across borders. Agreements with global platforms can speed up enforcement and ensure India's rules are respected in the digital world.

CONCLUSION

Deepfakes pose a profound threat to the core pillars of India's democracy, truth, trust, and informed public choice. The 2024 general elections revealed the dangerous extent of digital manipulation, while India's current legal framework remains fragmented and reactive. The challenge now lies not only in combating technological misuse but in safeguarding constitutional values in the digital age. India must respond with urgency and clarity through comprehensive legislative reform, technological innovation, public education, victim support, and international cooperation. The Supreme Court's rulings in *Justice K.S. Puttaswamy v. Union of India*[57] and *Shreya Singhal v. Union of India*[58] provide essential constitutional guardrails, reminding lawmakers that any regulation must be precise, proportional, and consistent with fundamental rights. Protecting privacy, free expression, and electoral integrity cannot rest on the state alone; it demands a whole-of-society approach involving citizens, platforms, educators, and policymakers alike. The future of India's democracy will depend on our ability to adapt swiftly, to cultivate digital literacy, strengthen institutional capacity, and uphold ethical responsibility in the face of emerging technologies.

[56] Election Commission of India, 'Press Note: Responsible and Ethical Use of Social Media' (2024)
[57] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (SC)
[58] Shreya Singhal v Union of India (2015) 5 SCC 1 (SC)