REGULATING DEEPFAKES IN INDIA: ANALYSING THE CONSTITUTIONAL AND STATUTORY FRAMEWORK

"Privacy is the constitutional core of human dignity."

-Justice D.Y. Chandrachud

I. ABSTRACT

This paper examines the legal challenge posed by deepfake technology in India. This paper uses incidents such as the 2023 Rashmika Mandanna case and AI-manipulated content during the 2024 general election to demonstrate how synthetic media threatens privacy, dignity, and electoral integrity while also serving legitimate purposes in entertainment, education, and public health. The paper evaluates India's constitutional framework under Articles 21 and 19(1)(a) and highlights the vertical application gap that leaves victims without direct recourse against private perpetrators. It then assesses the adequacy of existing statutory tools, the IT Act, BNS, IRWA, DPDPA, and the newly introduced IT Rules 2026 Amendment, identifying persistent lacunae around definitions, preventive safeguards, creator liability, and cross-border enforcement. The paper also touches upon the judiciary's emerging jurisprudence on personality rights, showing that while courts have provided meaningful interim relief, litigation-driven protection is inherently ad hoc and inaccessible to most victims.

II. KEYWORDS

Deepfakes, Privacy, Personality Rights, Electoral Integrity, Synthetic Media Regulation

III. INTRODUCTION

Artificial intelligence now can create of hyper-realistic synthetic media in the form of videos, audio recordings, and images. They offer legitimate and efficient use in entertainment, education, healthcare, and accessibility but at the same time it also poses threats to privacy, reputation, integrity, and public trust. They are so realistic that the distinction between authentic and fabricated content collapses. It is extremely difficult to detect them and traditional legal frameworks are not tailored to deal with deepfakes. This challenge is not just technological but also legal and constitutional. This paper addresses the same research gap. It also analyses India's constitutional framework and statutory mechanisms. The paper concludes by assessing the limitations of the current legal framework and proposes reforms aimed at developing a comprehensive and future oriented regulatory framework for synthetic media in India. This paper argues that although India has expanded constitutional protections, enacted

statutory safeguards, and witnessed significant judicial intervention, these mechanisms remain fragmented and reactive rather than preventive.

IV. OBJECTIVES

- To examine the technology, typology, and dual nature of deepfake harms with specific reference to India's legal and social landscape.
- To critically analyse India's constitutional framework, particularly Article 21's expanding privacy jurisprudence and its tension with Article 19(1)(a), as applied to deepfake related harms and the constitutional vacuum that persists.
- To evaluate the adequacy of India's statutory framework, including the IT Act, BNS, DPDPA, IRWA, and the IT Rules 2026 Amendment, in addressing the full spectrum of deepfake harm, and to identify specific lacunae in each instrument.
- To study the judicial response of Indian courts, particularly the Delhi High Court's emerging personality rights jurisprudence, to deepfake-related violations of privacy, dignity, and identity.
- To assess global regulatory approaches and derive concrete, constitutionally grounded recommendations for a more robust Indian legal framework.

V. RESEARCH QUESTIONS

- Is India's current constitutional and statutory framework sufficient to address the layered harms caused by deepfakes, or does a fundamental legal vacuum persist despite recent regulatory developments?
- How have Indian courts applied Article 21's privacy jurisprudence and the personality rights doctrine to deepfake-related cases, and what are the structural limitations of judicial intervention as a primary mechanism of protection?
- Do deepfakes pose a structural threat to India's electoral integrity, and what specific legislative mechanisms are required to address election-related synthetic media?

VI. LEGAL ANALYSIS

(a) Technology, Typology of Harm, and India's Dual Reality

At its technical foundation, deepfake creation proceeds through three stages facial mapping gathers biometric data on an individual's features, GAN based processing synthesises the target's face onto another body or into a fabricated scene and voice cloning replicates the

target's speech patterns. It creates synthetic content until the output is capable of defeating detection.

Kukreti, Kumar, and Raj identify four deepfake modalities that raise distinct legal challenges: video deepfakes, audio deepfakes (voice cloning), image manipulation, and hybrid forms combining media types.[1]

Non-Consensual Intimate Imagery (NCII) targeting women, constitutes the majority of deepfake content, approximately 96-98% of deepfake videos online and as a result victims experiencing anxiety, depression, and post-traumatic stress disorder.[2] Deepfakes can damage elections by spreading fake statements of leaders, voice cloned scams impersonate executives or judges to commit financial fraud. Most dangerous is the loss of trust in digital media, where even real videos can be dismissed as fake.[3]

The rapid WhatsApp misinformation spread, limited media literacy, weak AI forensic capacity, and slow legal processes are the proof that India is especially vulnerable due to its massive internet youth population. Deepfake technology is advancing much faster than laws and regulation, creating major challenges for India.[4] The real challenge is creating laws that prevent misuse without harming innovation and creativity.[5] India's vulnerability therefore stems less from the technology itself than from the inability of existing institutions to respond effectively to rapidly evolving synthetic media.

(b) Constitutional Analysis: Articles 21 and 19(1)(a)

The constitutional analysis of deepfakes begins with Article 21, which guarantees the right to life and personal liberty. In *K.S. Puttaswamy v. Union of India (2017)*[6], a nine-judge bench of the Supreme Court unanimously held that the right to privacy is intrinsic to Article 21, encompassing bodily integrity, personal dignity, informational self-determination, and

---

[1] Abhishek Kukreti, Vivek Kumar and Avishek Raj, "THE IMPACT OF DEEPFAKE TECHNOLOGY ON LEGAL SYSTEMS: A GLOBAL PERSPECTIVE" (2026) 7(1s) ShodhKosh: Journal of Visual and Performing Arts, DOI: 10.29121/shodhkosh.v7.i1s.2026.7068 https://www.granthaalayahpublication.org/Arts-Journal/ShodhKosh/article/view/7068?__cf_chl_f_tk=_9ahoCYaZkRhxNDnnyuF2OZZt3AbUDZjuh2J83hEcac-1783445693-1.0.1.1-Yuy76WAKxnsUHHIpOloVWT9APs3UNiyHAH0IPMeXpAU

[2] *Id.*

[3] Bobby Chesney and Danielle Citron, "DEEP FAKES: A LOOMING CHALLENGE FOR PRIVACY, DEMOCRACY, AND NATIONAL SECURITY" (2019) 107 California Law Review 1753. https://scholarship.law.bu.edu/faculty_scholarship/640

[4] Biranchi Naryan P. Panda and Isha Sharma, "DEEPFAKE TECHNOLOGY IN INDIA AND WORLD: FOREBODING AND FORBIDDING" (2025) 4(3) Law and Humanities Quarterly Reviews 18 (Asian Institute of Research), DOI: 10.31014/aior.1996.04.03.152 https://www.asianinstituteofresearch.org/lhqrarchives/deepfake-technology-in-india-and-world:-foreboding-and-forbidding

[5] *Supra at note 2.*

[6] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1; *supra note at 6*; *supra at note 2*

autonomy over one's identity. This forms the constitutional basis for deepfake claims, unauthorised use of biometric data violates privacy, fake sexual or defamatory content harms dignity and autonomy, and the resulting humiliation or loss affects the right to live with dignity. However, Article 21 operates primarily as a vertical constraint, it governs State action against individuals, not the actions of private actors against each other. Since deepfakes are predominantly created and disseminated by private individuals, companies, and platforms, victims have no direct constitutional recourse against these actors. As Chandel and Kundu demonstrate that there is no explicit constitutional right to identity or to control one's digital persona, the horizontal application of fundamental rights to private deepfake creators is not recognised and the Constitution provides no framework for consent in relation to AI-generated secondary use of personal data.

Article 19(1)(a) adds a further layer of complexity. Freedom of speech and expression encompasses the right to satire, parody, political commentary, and artistic expression, all of which deepfake technology can serve. In *Shreya Singhal v. Union of India (2015)*[7], the Supreme Court struck down Section 66A of the IT Act as unconstitutionally over broad, affirming that restrictions on online expression must be narrowly tailored, necessary, and proportionate to the harm addressed. In *Subramanian Swamy v. Union of India (2016)*[8], the Court balanced privacy and reputation against free speech in a digital context. Any deepfake law must thread this needle, targeting deceptive, non-consensual, or harmful synthetic media while explicitly carving out clearly labelled satire and protected artistic expression.

The constitutional framework therefore establishes important normative principles but cannot independently regulate synthetic media. Constitutional rights define the boundaries within which legislation must operate, but they do not provide comprehensive standards governing AI-generated content or effective remedies against private creators. This explains why statutory reform remains indispensable.

(c) India's Statutory Framework: Provisions and Lacunae

i. The Information Technology Act, 2000

The IT Act is the primary legislative instrument for cyber activities in India and contains several provisions applicable to deepfake related offences. Section 66E punishes the violation of privacy by capturing, transmitting, or publishing private images or videos without consent,

[7] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[8] Subramanian Swamy v. Union of India, (2016) 7 SCC 221.

directly applicable to NCII deepfakes. Section 67 criminalises the publication of obscene material in electronic form, relevant to sexually explicit deepfakes. Section 67A imposes stricter penalties for transmitting sexually explicit content without consent. Section 69A empowers the government to direct blocking of online content that threatens national security or public order, including harmful deepfakes. Sections 66C and 66D address identity theft and impersonation through computer resources.[9]

In the *Rashmika Mandanna case*, Delhi Police invoked Sections 66C and 66E alongside Sections 465 and 469 IPC. While an FIR was registered and subsequently arrest was made, that was attributable to the victim's public profile and sustained media attention, not to any systematic protective mechanism. The IT Act provides no definition of deepfake or synthetic media, no mandatory disclosure obligations for AI-generated content, and no preventive framework, it is entirely reactive, requiring harm to occur before any legal process is triggered. This demonstrates that the IT Act addresses the consequences of deepfake misuse rather than regulating synthetic media itself. Consequently, investigators are compelled to fit AI-generated harms into statutory provisions enacted decades before generative AI emerged, resulting in fragmented enforcement and legal uncertainty.

ii. The Bharatiya Nyaya Sanhita, 2023

Section 356 criminalises defamation, applicable to deepfakes fabricating statements or depicting individuals in derogatory scenarios. Section 351(1) covers criminal intimidation, relevant to deepfake based blackmail. Section 318(1) addresses cheating by personation, applicable to identity fraud. Sections 76 and 77 address voyeurism and stalking respectively. Multiple provisions, Sections 354, 354A, 354B, 354C, 354D, 375, and 509, collectively provide protection against sexual offences and harassment.[10]

Khamari says BNS provisions present significant prosecution challenges in the deepfake context, they require proof of mens rea that may be difficult to establish when the "act" is algorithmic, perpetrators routinely operate anonymously, defeating the initial step of identification; and the rapid viral dissemination of deepfakes means harm is often irreversible before any FIR is registered.[11]

[9] Information Technology Act, 2000 (Act 21 of 2000), ss. 66C, 66D, 66E, 67, 67A, 69A.
[10] Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), ss. 318(1), 351(1), 354, 354A–D, 356, 375, 509, 76, 77
[11] *Supra at note 2.*

Therefore the BNS remains primarily a post-offence criminal law mechanism rather than a preventive regulatory framework capable of limiting viral dissemination before irreversible harm occurs.

iii. The Indecent Representation of Women (Prohibition) Act, 1986

It prohibits indecent representation of women in various media, including digital formats, and applies to deepfakes that depict women in derogatory or sexualised ways without consent. The Act allows for imprisonment and fines for those involved in producing or distributing such content.[12] However, its application to deepfakes is limited by the transnational nature of online platforms, the anonymity of creators, and enforcement mechanisms designed for an analogue era that have not been updated to address AI generated content at scale.

Consequently, the Act remains useful for addressing specific harms against women but cannot effectively regulate the broader ecosystem of AI-generated synthetic media.

iv. The Digital Personal Data Protection Act, 2023

The DPDPA strengthens the privacy framework for personal data processing. Section 4 requires explicit consent before processing personal data, which includes biometric data such as facial images and voiceprints, making the unauthorised use of a person's image in deepfake creation a potential violation. Section 11 grants data principals the right to access, correct, and erase personal data, theoretically allowing deepfake victims to demand removal of unauthorised content. Sections 12, 14, and 25 impose financial penalties for non-compliance.[13]

Chandel and Kundu observe that the act is concerned with primary data processing and does not clearly regulate secondary or AI generated use of personal data. A deepfake creator may source training data from publicly available social media images and may have collected that data lawfully, the DPDPA provides no explicit framework addressing the same.[14]

Consequently, the DPDPA protects personal data rather than regulating synthetic identity creation itself. The distinction leaves significant uncertainty regarding AI training datasets and secondary algorithmic use of publicly available biometric information.

v. The Cybersecurity Framework

[12] Indecent Representation of Women (Prohibition) Act, 1986, ss. 2(c), 3, 4, 6, 7
[13] Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 4, 11, 12, 14, 25
[14] *Supra at note 6.*

Section 70B of the IT Act, issues advisories on cyber threats including deepfakes, though it has no specific mandate for the same. State level cybercrime investigation cells have technical expertise for investigating cybercrimes involving deepfakes, but face resource constraints. The IT Rules 2021, Rule 3(1)(b), Rule 3(2), and Rule 4(4), directs social media intermediaries to remove harmful content upon receiving appropriate orders and to maintain grievance redressal mechanisms.[15] These institutional mechanisms remain largely advisory and complaint-driven. They neither provide specialised forensic infrastructure nor enable coordinated real-time responses to rapidly spreading deepfakes.

vi. The IT Rules 2026 Amendment

The IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, is India's first explicit regulatory framework for AI generated synthetic content. Rule 2(1)(wa) defines Synthetically Generated Information (SGI), *"synthetically generated information' means audio, visual or audio-visual information which is artificially or algorithmically created, generated, modified or altered using a computer resource, in a manner that such information appears to be real, authentic or true and depicts or portrays any individual or event in a manner that is, or is likely to be perceived as indistinguishable from a natural person or real-world event; Provided that the purposes of this clause, an audio, visual or audio-visual information shall not be deemed to be 'synthetically generated information', where such audio, visual or audio-visual information arises from (a) routine or good-faith editing, formatting, enhancement, technical correction, colour adjustment, noise reduction, transcription, or compression that does not materially alter, distort, or misrepresent the substance, context, or meaning of the underlying audio, visual or audio-visual information; or (b) the routine or good-faith creation, preparation, formatting, presentation or design of documents, presentations, portable document format (PDF) files, educational or training materials, research outputs, including the use of illustrative, hypothetical, draft, template-based or conceptual content, where such creation or presentation does not result in the creation or generation of any false document or false electronic record; or (c) the use of computer resources solely for improving accessibility, clarity, quality, translation, description, search ability, or discoverability, without generating, altering, or manipulating any material part of the underlying audio, visual or audio-visual information;"*.[16]

[15] *Supra at note 2.*
[16] IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, Rule 2(1)(wa).

The rules require users to label AI generated content, mandate quick removal of harmful deepfakes, impose verification duties on major platforms, and protect intermediaries acting in good faith.[17] This amendment displays shifts from reactive regulation to proactive accountability and it is, currently, better suited to the rapid spread of deepfakes. Although the amendment represents India's first proactive attempt to regulate AI-generated content, it focuses primarily on intermediary obligations. It leaves unresolved questions relating to creator liability, civil remedies, evidentiary standards, and victim compensation, limiting its effectiveness as a comprehensive regulatory framework.

(d) Judicial Response: Personality Rights and Precedent

Indian courts have exercised a significant role in developing a nascent but significant body of personality rights jurisprudence. The constitutional anchor for the same is Puttaswamy (2017), which recognised privacy as a fundamental right and it provides basis for all subsequent deepfake related claims.[18]

In *Anil Kapoor v. Simply Life India & Ors.*[19], the Delhi High Court held that the defendants had unlawfully used the actor's likeness for commercial purposes without consent by creating and selling AI generated deepfakes and other synthetic content. Ex parte injunction protecting Kapoor's personality rights, including his name, image, voice, and persona was granted and defendants were ordered to cease such activities. Infringing links were blocked. The transfer of domain names like 'www.anilkapoor.in' was directed. This ruling marked a significant step in extending personality rights protection to AI generated deepfake content.

In *Amitabh Bachchan v. Rajat Negi & Ors.*[20], Amitabh Bachchan's image and likeness was use manipulated without consent, for commercial and derogatory purposes. An injunction as issued to prevent further misuse and defendants were directed to remove deepfake content across platforms. This case reinforced personality rights and privacy against technological manipulation.

In *Sadhguru Jagadish Vasudev & Anr. v. Igor Isakov & Ors.*[21], the Delhi High Court directed the Department of Telecommunications and Ministry of Electronics and Information

[17] MeitY Notifies the IT Amendment Rules 2026 (February 16, 2026).
[18] *Supra at note 15.*
[19] Anil Kapoor v. Simply Life India & Ors., 2023 SCC OnLine Del 6914.
[20] Amitabh Bachchan v. Rajat Negi & Ors., 2022 SCC OnLine Del 4110.
[21] Sadhguru Jagadish Vasudev & Anr. v. Igor Isakov & Ors., Delhi HC (2024).

Technology to require service providers to block or suspend relevant websites and social media accounts using AI-generated impersonation content.

Though courts have intervened but there is no precedent addressing the systemic dimensions of deepfake harm at scale, no standardised forensic evidentiary framework for AI content attribution, and no mechanism for victims without resources to access swift relief without expensive High Court litigation.[22]

These decisions indicate that Indian courts are willing to expand personality rights jurisprudence to emerging AI disputes. However, litigation remains expensive, time-consuming, and largely inaccessible to ordinary victims. Judicial innovation therefore cannot substitute for comprehensive legislative regulation.

e) Deepfakes, Electoral Democracy, and the 2024-2025 Crisis

Deepfakes threaten not only individual privacy but also democratic legitimacy. Elections depend upon informed decision-making, yet synthetic media enables fabricated political speech capable of influencing voters before verification mechanisms can respond.

During 2024 general election because of rise in spread of AI-generated content misinformation storm occurred. Deepfakes were used for multiple purposes during the election cycle which included translating campaign messages across languages, fabricating statements attributed to rival leaders, and even cases of resurrection of deceased political figures in life like video also appeared.[23]

During 2020 Delhi Legislative Assembly elections, it was alleged that a political party created a deepfake video of its leader speaking in languages he did not know, it raised direct questions about voter manipulation.[24] During the Lok Sabha election campaign, Actor Ranveer Singh's video was circulated in which he appeared to criticise Prime Minister Modi and urge votes for Congress, this video was manipulated using deepfake technology, leading Maharashtra Police cyber cell to register an FIR against an X user under Sections 417, 468, and 469 IPC and the IT Act.[25] A video showing Home Minister Amit Shah led to a case being registered against a Maharashtra Youth Congress social media handle, the video was created using deepfake

[22] *Supra at note 6.*
[23] Bloomberg, "India Elections 2024: Could Deep Fakes Undermine Trust in Electoral System?" (April 20, 2024). https://www.bloomberg.com/features/2024-ai-election-security-deepfakes/
[24] *Supra at note 2.*
[25] Deccan Herald, "Ranveer Singh Files FIR Over Misleading Deepfake Video" (May 2024). https://www.deccanchronicle.com/entertainment/bollywood/ranveer-singh-takes-legal-action-against-deepfake-video-890649

technology.[26] West Bengal Police also confirmed that a video of Congress leader Adhir Ranjan Chowdhury urging votes for the BJP was digitally manipulated using deepfake which resulted in an FIR under Sections 499/500 IPC and Section 66D of the IT Act.[27]

In December 2024, a fake video of Prime Minister Narendra Modi and Italian Prime Minister Giorgia Meloni, originally from an official event, was uploaded on Facebook by a user named Mohammad Saif which was manipulated and several BJP workers in Agra lodged a formal complaint and a case was promptly registered under the IT Act.[28] This shows that deepfakes are not limited to a country and fabricated video may cause diplomatic embarrassment, distort bilateral relations, and generate international misinformation cycles. No single national jurisdiction can fully contain it. It is a textbook illustration of why cross-border cooperation is an operational necessity.[29] The absence of statutory framework is highlighted in electoral context. The existing provisions fail to provide preventive remedies and does not clearly allocate responsibility among creators, intermediaries, and other responsible parties.[30]

While courts have tried to control the damage by recognising personality rights but the harm extends far beyond individual reputation. They have the ability to manipulate public discourse and electoral processes. This indicates that the challenge also equally can be said as constitutional and democratic.

VII. EU AI ACT

EU Artificial Intelligence Act is a European regulation which provides comprehensive regulation on AI. It sorts systems into four tiers. First, unacceptable risk, it is prohibited. (e.g. social scoring systems and manipulative AI). Secondly, high risk AI systems, which are regulated, it covers most of the text addresses. Thirdly, limited risk, they are subject to lighter transparency obligations, developers and deployers must ensure that end-users are aware that they are interacting with AI (chatbots and deepfakes). Lastly, Minimal risk, they are unregulated (including the majority of AI applications currently available on the EU single

[26] Deccan Herald, "Amit Shah Deepfake Video: Case Registered Against Maharashtra Youth Congress Social Media Handle" (2024) https://www.deccanherald.com/india/amit-shah-deepfake-video-case-registered-against-maharashtra-youth-congress-social-media-handle-3001154

[27] ThePrint, "Adhir's 'vote for BJP' video manipulated: Police" (May 3, 2024) https://theprint.in/india/adhirs-vote-for-bjp-video-manipulated-police/2068994/

[28] ETV Bharat, "Case Filed After PM Modi & Italian PM Giorgia Meloni's Video Altered Using Artificial Intelligence" (December 20, 2024). https://www.etvbharat.com/en/!state/pm-narendra-modi-italian-prime-minister-giorgia-meloni-video-tampered-with-ai-case-filed-by-bjp-in-agra-enn24122002659

[29] *Supra at note 2.*

[30] *Supra at note 13.*

market, such as AI enabled video games and spam filters.[31] It treats AI systems as artefacts whose permissible risk must be certified before market entry.[32] Enforcement of the act is centralised through the European AI Office and national market-surveillance authorities, backed by fines reaching seven per cent of global turnover.[33]

The key principles of the AI Governance framework have been carefully designed to ensure cross-sectoral applicability and technology neutrality, enabling relevance across diverse use cases and stages of technological evolution.[34] India does not propose a new comprehensive AI law and instead relies on existing legal frameworks with targeted amendments where necessary.[35] On comparison with EU Act, India's AI governance leans more towards principles based and that not all risks can be anticipated in advance. EU AI Act provides classifications, scopes, categories, etc and the role of organisations for certainty.[36] Unlike the EU's ex-ante risk-based regulatory model, India continues to rely primarily upon existing legislation and supplemented by amendments. This provides regulatory flexibility, it also creates uncertainty because without a unified enforcement mechanism one needs to find remedy across multiple statutes.

VIII. ANSWERING THE RESEARCH QUESTIONS

The above analysis shows that India's constitutional and statutory framework provides only fragmented protection against deepfakes. While constitutional principles, statutory provisions, and judicial decisions collectively offer partial remedies, they do not operate as an integrated regulatory regime. Consequently, victims remain dependent upon multiple overlapping legal mechanisms that are largely reactive after the harm is done rather than preventive.

Indian courts have significantly expanded personality rights jurisprudence through decisions, however, judicial intervention remains case-specific, expensive, and dependent upon litigation, making it an inadequate substitute for comprehensive legislative regulation.

---

[31] The EU Artificial Intelligence Act, High-level summary of the AI Act. (February 27, 2024) https://artificialintelligenceact.eu/high-level-summary/

[32] REGULATION 2024/1689 OF THE EUR. PARL. & COUNCIL OF JUNE 13, 2024 (EU ARTIFICIAL INTELLIGENCE ACT). INTERNATIONAL LEGAL MATERIALS, CAMBRIDGE CORE. (2025). https://www.cambridge.org/core/journals/international-legal-materials/article/regulation-20241689-of-the-eur-parl-council-of-june-13-2024-eu-artificial-intelligence-act/64F1F6734F8C66CA3EEA149C9759194E

[33] The EU Artificial Intelligence Act. https://artificialintelligenceact.eu/

[34] India AI Governance Guidelines (February 15 2026) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2228315&reg=48&lang=2

[35] *Id.*

[36] India and the EU on Privacy and AI Regulation: Convergence or Divergence? (January 19, 2026) https://www.privacyengine.io/blog/india-eu-privacy-ai-regulation-dpdp-gdpr-eu-ai-act/

Deepfakes pose a structural threat to electoral integrity by enabling fabricated political speech, voter manipulation, and large-scale misinformation. The analysis shows that existing criminal provisions respond only after dissemination has occurred. Effective regulation therefore requires preventive obligations for creators and intermediaries, rapid takedown mechanisms, and specialised rules governing AI-generated political content during elections.

IX. SUGGESTIONS

1. Legislative Reforms: Enact a dedicated legislation Deepfake & Synthetic Media. Amend current legislations to recognise Digital Forgery of Identity covering AI-based face, voice, and identity manipulation. Like EU, India must adopt a risk based classification for AI and deepfakes.
2. Technical & Forensic Capacity Building: Mandate standardised invisible digital watermarks or disclaimers for all AI-generated content produced by AI tools. These disclaimers should be displayed with the same level of seriousness and mandatory visibility as the statutory warnings related to smoking and tobacco depictions.
3. Establish fast-track Identity Courts granting immediate reliefs like rapid removal of harmful deepfake and NCII (Non-Consensual Intimate Imagery) content and a specialised AI Forensic Laboratory under the Indian Cyber Crime Coordination Centre dedicated to deepfake detection, forensic analysis, and expert evidentiary support for courts and law enforcement.
4. Awareness & Social Responsibility: Launch nationwide media literacy and awareness campaigns to educate the public about deepfakes, AI, Synthetic media etc. and how genuine content is also falsely dismissed as fake
5. International Cooperation: India should promote or join an international convention or enter into regional agreements to ensure cross-border cooperation in identifying and prosecuting perpetrators of deepfakes targeting Indian citizens.