The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

REGULATING DEEPFAKE TECHNOLOGY UNDER INDIAN CYBER LAWS

Innama Haider

ABSTRACT

One of the most significant and unregulated risks facing digital society in the twenty-first century is the rise of deepfake technology, which creates artificially synthesised audio-visual content using deep learning algorithms. The rise of deepfakes in India has led to sophisticated financial frauds, AI-generated electoral disinformation, widespread non-consensual intimate imagery targeting women, and serious concerns to national security. India's current legal framework, which is mainly based on the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023, does not have any special legislation that addresses synthetic media manipulation in spite of this obvious harm. This study uses comparable international models, such as those of the US and the EU, to critically assess the effectiveness of Indian cyber legislation in regulating deepfakes. It also reveals basic normative and institutional gaps. The European Union, the United Kingdom, and China, and suggests a logical, rights-preserving legal and policy framework for India. The study comes to the conclusion that the necessity of passing specific deepfake regulations is a constitutional requirement based on the fundamental rights to equality, dignity, and free speech rather than just a question of technology governance.

Keywords: AI regulation, digital rights, platform liability, non-consensual intimate imagery, synthetic media, deepfakes, Indian cyber law, information technology act, and disinformation.

INTRODUCTION

A portmanteau of "deep learning" and "fake," "deepfake" refers to extremely lifelike digital replicas of audio, video, and images produced by artificial intelligence systems, namely Generative Adversarial Networks (GANs) and diffusion models. In the mid-2010s, what started out as an intellectual curiosity quickly developed into a weapon of mass destruction. Globally, deepfakes have been used as weapons for the creation of false evidence, political speeches, non-consensual pornography, and business fraud through voice cloning.

India is particularly vulnerable to these negative effects. India is a prime target for deepfake abuse because to its more than 900 million internet users, politically divided electorate, and strongly patriarchal societal structure. India is particularly vulnerable to these negative effects. India is a prime target for deepfake abuse because to its more than 900 million internet users, politically divided electorate, and strongly patriarchal societal structure. AI-generated movies mimicking prominent political leaders were reportedly circulated on YouTube, Instagram, and WhatsApp during the 2024 Indian general elections, the biggest democratic exercise in human history. Deepfake pornography has alarmingly attacked both common women and well-known Bollywood actresses. Indian businesses have lost crores of rupees to financial schemes that use deepfake voice cloning of corporate officials.

Indian law is still structurally ill-equipped to deal with deepfakes despite this empirically proven harm. Only partial and analogous remedies are provided by the Information Technology Act, 2000 (IT Act), which was passed before generative AI was ever conceptualised. There is no deepfake-specific crime under the recently passed Bharatiya Nyaya Sanhita, 2023 (BNS). While data processing is covered by the Digital Personal Data Protection Act, 2023 (DPDP Act), synthetic media misuse is not fully covered. The proposed Digital India Act, which is expected to take the place of the IT Act, is still in the consultative stage.

This study looks at whether the current cyber legal framework in India is sufficient to control deepfake technology and, if not, what institutional and legislative changes are needed. The following is how the paper goes: Deepfake technology and its negative effects are contextualised in Part II. The present Indian judicial system is examined in Part III. Critical gaps are identified in Part IV. International regulatory models are surveyed in Part V. A framework for reform is suggested in Part VI. Part VII comes to an end.

RESEARCH OBJECTIVES

-To examine deepfake technology's characteristics and the list of negative effects it has in India.
-To assess whether the current Indian legal system—statutory, judicial, and regulatory—is sufficient to deal with offences linked to deepfakes.
-To determine the institutional and normative gaps in Indian cyber law concerning the regulation of synthetic media.
-To examine global regulatory strategies for deepfake governance and draw conclusions that might be applied to India.
-To suggest a thorough legislative and policy framework for controlling deepfake technology in India.

RESEARCH QUESTIONS

Do victims of injury caused by deepfakes have sufficient remedies under the current Indian cyber law framework, which includes the IT Act, 2000, the BNS, 2023, and the DPDP Act, 2023?

What are the basic institutional and normative deficiencies in the Indian legal system concerning the regulation of deepfakes?

What can India learn from global regulatory models in the US, EU, UK, and China in order to create custom deepfake laws?

RESEARCH HYPOTHESES

Because it was written in a pre-generative AI setting and lacks deepfake-specific rules, the current Indian cyber law framework is insufficient to handle deepfake-related harms.
Deepfake harm disproportionately affects Indian women and underprivileged populations, especially when it comes to non-consensual intimate imagery, which is still not sufficiently criminalised.
For India, a comprehensive Deepfake Regulation Act is both technologically and constitutionally required, together with platform accountability changes and a specialised adjudicatory framework.

RESEARCH METHODOLOGY

This work uses a strictly doctrinal research methodology. A unique approach to legal research, doctrinal research—also referred to as library-based research—involves the methodical examination and evaluation of current legal laws, court rulings, and academic literature. This approach is especially useful for finding normative gaps in legislative frameworks and for analysing the theoretical and conceptual aspects of law. The Information Technology Act of 2000, the Bharatiya Nyaya Sanhita of 2023, the Digital Personal Data Protection Act of 2023, the Representation of the People Act of 1951, and pertinent subordinate legislation, such as the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021, are among the statutory instruments that are used as primary sources.

Peer-reviewed studies, policy reports, regulatory advisories, and comparative legislative texts from the US, EU, UK, and China are examples of secondary sources that were considered. This study provides normative reasons in favour of legislative reform and finds doctrinal gaps through a methodical analysis of these sources.

LITERATURE REVIEW

Although Indian academic literature on deepfake regulation is still in its infancy, there is a growing corpus of research on the topic worldwide:
'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019), a seminal study by Robert Chesney and Danielle Citron published in the California Law Review, identifies deepfakes as a multifaceted legal threat requiring immediate regulatory attention and establishes the taxonomy of harm that has since anchored academic discourse.
The Data & Society Research Institute published Paris and Donovan's 2019 book "Deepfakes and Cheap Fakes: The Manipulation of Audio and Visual Evidence," which explores the misinformation implications of synthetic media and its effects on democracy.

Gupta and Singh, in *'Artificial Intelligence and Indian Cyber Law: A Study of Legislative Gaps'* (Journal of Indian Law Institute, 2023), analyse the inadequacy of the IT Act's provisions for contemporary AI-generated harm, providing the closest Indian doctrinal treatment of the subject.

Narayan, in *'Electoral Deepfakes and the Limits of Indian Electoral Law'* (National Law School of India Review, 2024), argues that the Representation of the People Act and the Model Code of Conduct are constitutionally and structurally ill-equipped to address AI-generated electoral disinformation.

Sensity AI's annual *'State of Deepfakes'* report (2023) provides quantitative evidence that over 90% of deepfake content online constitutes non-consensual intimate imagery targeting women, establishing the empirical basis for treating gender justice as central to deepfake regulation.

The **Internet Freedom Foundation's** policy brief *'Deepfakes and Democracy'* (2023) examines the specific vulnerabilities of Indian democratic infrastructure to AI-generated disinformation and recommends legislative intervention.

The **MEITY Advisory on Deepfake Content** (November 2023) and the **Election Commission of India's Advisory** on AI-generated political content (2024) represent the most recent official acknowledgements of the deepfake problem in India, though both remain non-binding and limited in scope.

SUB HEADINGS

Technical Meaning and Definition

"Deepfake" describes artificial audio-visual information produced using deep learning methods, mainly Generative Adversarial Networks (GANs) and, more recently, Latent Diffusion Models. Two neural networks—a discriminator and a generator—compete adversarially in a GAN architecture, with the discriminator trying to identify fabrication while the generator creates artificial media. This process's iterative equilibrium produces photorealistic content that is indistinguishable from genuine material to the human eye.

Face-swapping, which projects one person's facial features onto another's body in a video; voice cloning, which synthesises a facsimile of a target's voice from minimal audio samples; face reenactment, which animates still images to synchronise lip movements with arbitrary audio; and text-to-video synthesis, which creates completely original video content from textual prompts, are some of the key modalities of deepfake generation. Deepfake production now has almost no

technical barrier thanks to the availability of open-source tools like DeepFaceLab, FaceSwap, and commercial generative platforms, democratising a formerly specialised capacity.

The terms "deepfake," "synthetic media," and "deep synthesis technology" are not defined by statute under Indian law. According to Article 20(1) of the Indian Constitution, criminal law requires precise definitional clarity for offences to be constitutionally valid, hence this definitional gap is a serious weakness in and of itself.

Contextual and Historical Background

Ian Goodfellow's 2014 scholarly article presenting the GAN architecture is where deepfake technology first emerged. When a Reddit user started sharing AI-generated, non-consensual intimate footage of celebrities in 2017, the term "deepfake" gained widespread usage. By 2019, technology had developed to the point where laypeople could not tell the difference between the content and real footage. Through consumer-facing applications, technology has become exponentially more accessible in the 2020s.

The deepfake issue became well-known in India as a result of several high-profile occurrences. When deepfake videos of actress Rashmika Mandanna became widespread on social media in 2023, the Ministry of Electronics and Information Technology (MEITY) issued an advice instructing sites to take down the information within a day. AI-generated movies of Prime Minister Narendra Modi and other prominent political figures were shared during the 2024 general elections in an attempt to sway voter sentiment. Although there hasn't been a thorough legislative reaction, these occurrences sparked public discussion regarding the suitability of current legislation.

The Indian legal system as it exists today

The 2000 Information Technology Act

The main piece of legislation controlling cybercrimes and electronic behaviour in India is the IT Act, 2000. Although none of the prohibitions were written with synthetic media in mind, they may apply to deepfake crimes.

Fraudulent or dishonest use of another person's unique identification feature in electronic form is prohibited by Section 66C and carries a maximum sentence of three years in jail and a fine of one lakh rupees. Cheating by impersonation using computer resources is punishable under Section 66D and carries the same penalty. Although some types of identity fraud facilitated by

deepfakes are covered by these regulations, their applicability is restricted to transactional impersonation, such as phishing or SIM-swap fraud, and does not easily extend to audiovisual fabrication.

The publication or transmission of pornographic electronic content is forbidden by Section 67, and a first conviction carries a maximum sentence of three years in prison. This also applies to sexually explicit content under Section 67A. Deepfake pornography may be covered by these regulations, although non-consensual personal imagery that is explicit but not legally "obscene" may be exempt due to the definitional dependence on "obscenity"—which is still governed by the outdated Hicklin test in Indian jurisprudence.
The Central Government may order the censorship of internet content on certain grounds, including as public order and sovereignty, under Section 69A. Significant social media intermediaries (SSMIs) are subject to due diligence requirements under the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which ban hosting impersonating content and require prompt resolution of complaints.

However, proactive deepfake detection responsibilities are not well defined in the Rules, and enforcement has been noticeably uneven.

Bharatiya Nyaya Sanhita,2023

The Indian Penal Code, 1860 was replaced by the BNS, which has a number of comparable provisions. When a deepfake is released to harm someone's reputation, Section 356 BNS, which deals with defamation, may be applicable. NCII deepfakes that target women may be covered by Section 74 BNS, which deals with sexual harassment, and Section 77 BNS, which deals with voyeurism. Financial fraud enabled by deepfakes may be covered by Section 318 BNS, which makes cheating illegal. Deepfakes made to create false documentary evidence may be covered by sections on forgery, especially those that deal with the fabrication of false electronic evidence.

Nevertheless, there was no deepfake-specific crime introduced by the BNS, which is a major legislative opportunity lost. These rules' applicability to deepfakes is still completely analogous, unproven in court, and vulnerable to evidential issues that the current forensic infrastructure is ill-prepared to handle.

The 2023 Digital Personal Data Protection Act

Digital personal data processing is governed by the DPDP Act. Deepfakes may be considered unlawful processing under the Act since they are created by processing a person's biometric and facial data without that person's consent. However, it is unlikely that the DPDP Act will apply to individual deepfake developers operating outside of commercial data processing environments because it is primarily focused on commercial data fiduciaries. The DPDP Act infractions would be decided by the Data Protection Board of India, which is yet not operating.

The Delhi High Court was presented with a request for immediate injunctive relief in relation to a deepfake video that targeted the complainant's professional reputation in the matter of **Karan Kapoor v. State of Delhi**. The Court noted that the current IT Act provisions were "manifestly inadequate to address the novel and distinctive harm of AI-generated synthetic video" and asked Parliament to pass specific laws while granting temporary relief. This court ruling is the clearest acknowledgement of the deepfake regulatory void by an Indian court.

Election Law and the Representation of the People Act of 1951

AI-generated electoral content is not expressly included by the Model Code of Conduct enforced by the Election Commission of India or the Representation of the People Act, 1951.

In 2024, the Election Commission issued a non-binding advisory mandating political parties to pre-certify AI-generated political advertisements. However, this measure is not legally binding and only applies to formal advertising; it does not apply to naturally occurring viral deepfake content that spreads via encrypted messaging platforms.

Critical Flaws in the Existing Framework

The lack of a sui generis deepfake offence is the most basic flaw in India's legal system. When prosecutors seek analogous application, the mishmash of current legislation exacerbates evidence and jurisdictional issues and fails to handle the entire lifetime of a harmful deepfake, from production through dissemination to harm. A legislative civil cause of action specifically designed to address deepfake victimisation is also absent from India. In a field where psychological and reputational harms are often intangible and challenging to quantify, victims are forced to rely on poorly developed tort remedies, such as defamation and intentional infliction of emotional distress, which are slow to adjudicate, limited in quantum, and require

victims to prove concrete injury.

Intermediaries are protected from third-party content liability under Section 79 of the IT Act as long as they take reasonable precautions. Although they do not impose proactive deepfake detection obligations, the 2021 IT Rules expound on this requirement. Because of this, the evidentiary burden for proving "actual knowledge" of deepfake content is too high for the majority of complainants, and platforms have little legal incentive to invest in detection tools. AI developers and deployers are not required by Indian law to incorporate content authentication credentials, watermarking, or provenance metadata into AI-generated material. Courts, electoral authorities, and investigating agencies are unable to verify evidence or prove that certain information is synthetic in the absence of obligatory disclosure standards, such as C2PA-compliant information Credentials. As a result, detection is still completely voluntary and dependent on the market.

These normative differences are exacerbated by jurisdictional issues. It is common for deepfake content to be created in one jurisdiction, housed on servers in another, and distributed to victims in a third. The mutual legal assistance treaty (MLAT) processes under Indian cyber law are insufficient to keep up with the rapidity of digital harm, and law enforcement authorities lack the specialised forensic capacity to conduct large-scale investigations of deepfake crimes.

Comparative International Regulatory Methods

United States of America

The US has taken a multi-layered, sector-specific approach. For victims of non-consensual deepfake intimate imagery, the DEFIANCE Act of 2024 (Disrupt Explicit Forged Images and Non-Consensual Edits Act) establishes a federal civil cause of action that offers statutory damages of $150,000 per infraction. Numerous states, including as Texas and California, have passed deepfake-specific legislation that addresses election manipulation and NCII.

The European Union

The EU AI Act (Regulation (EU) 2024/1689), which went into effect in 2024, designates systems that produce synthetic media as high-risk and imposes requirements for labelling and transparency. With fines of up to 6% of global annual sales, the Digital Services Act requires very big online platforms to evaluate and reduce systemic risks, including deepfake disinformation.

United Kingdom

Sharing private deepfake photos without permission is now illegal under the Online Safety Act of 2023 and carries a maximum two-year prison sentence. In order to address harm at the moment of creation rather than dissemination, the Criminal Justice Bill 2024 also suggests making it illegal to create deepfake intimate photographs without authorisation, regardless of the intention to distribute.

China's People's Republic

The world's first extensive deepfake-specific law is China's Provisions on the Administration of Deep Synthesis Internet Information Services, 2022. They mandate that service providers use real-name registration, clearly designate synthetic content with metadata, and forbid impersonating actual people without permission. Although direct transplantation is not appropriate for China's authoritarian regulatory paradigm, its technical uniqueness provides useful drafting precedents.

Impact of Deepfakes on Fundamental Rights

Several basic rights protected by Part III of the Indian Constitution are directly threatened by deepfakes. When deepfake NCII ruins a victim's reputation, mental health, and social status, it violates their right to life and personal dignity under Article 21. The Supreme Court upheld informational privacy as a component of Article 21 in Puttaswamy v. Union of India5. The non-consensual processing of biometric data for deepfake development is a prima facie infringement of this right.

Deepfake pornography disproportionately targets women and people of other gender identities, which violates their rights to equality and nondiscrimination under Articles 14 and 15.

The Supreme Court has ruled that the right to free and fair elections is a fundamental component of the fundamental framework of the Constitution, and electoral deepfakes pose a threat to this right. Paradoxically, deepfakes pose a threat to the right to freedom of speech and expression under Article 19(1)(a) because they can silence victims by destroying their reputations. However, any regulatory framework that runs the risk of over-censoring satire and legitimate political commentary must take care to protect this right.

Proposed Regulatory Framework for India

India needs a multifaceted regulatory approach based on four pillars:

First, a specific Deepfake Regulation Act with a graduated criminal offence structure: a minor tier for unlabelled synthetic content without harmful intent, subject to fines and corrective orders; an aggravated tier covering deepfake NCII and electoral manipulation, punishable with five to seven years in prison; and a standard tier covering deepfakes with intent to defame or defraud, punishable with two to three years. Along with obligatory injunctive remedy against platforms, the Act must provide a statutory civil cause of action that allows victims to seek statutory damages of at least Rs. 5 lakhs per violation without having to provide proof of actual loss.

Second, platforms must clearly label AI-generated content prior to distribution, and AI systems producing synthetic media must incorporate tamper-evident provenance metadata (C2PA-compliant Content Credentials) in all AI-generated content at the point of creation.

Third, a more robust platform accountability framework that amends the IT Rules to impose proactive deepfake detection duties on SSMIs with more than 50 million users; a 24-hour mandatory takedown obligation for reported NCII deepfakes (reduced to two hours during electoral periods); and the loss of Section 79 safe harbour protection for platforms that have constructive or actual knowledge of deepfake content but do not take action within the allotted time frames.

Fourth, a specialised institutional architecture that includes a Deepfake Adjudication Tribunal with civil and enforcement jurisdiction, a Deepfake Regulation Cell inside CERT-In manned by AI forensics experts, and required AI forensics training for law enforcement authorities.

Strong constitutional protections must be included in any regulatory action, including a clear exemption for clearly labelled satire, parody, and artistic expression; a proportionality requirement for all content-blocking orders; and a harm definition linked to specific institutional or individual harm rather than nebulous public order grounds.

I) CONCLUSION, SUGGESTIONS & RECOMMENDATIONS

One of the most complex and disruptive dangers to national security, democratic integrity, and individual dignity in the digital age is deepfake technology. Although there are some potentially

useful safeguards in India's current legislative framework, it is essentially insufficient to combat the negative effects of mass manipulation of synthetic media. The Information Technology Act of 2000 was written with a pre-AI legal environment in mind. There is no crime specifically related to deepfakes in the Bharatiya Nyaya Sanhita, 2023. Data processing is covered by the Digital Personal Data Protection Act of 2023, but harm from synthetic media is not. AI-generated political content is not covered by electoral legislation.

Leading nations are converging on a multifaceted regulatory architecture that combines particular criminal crimes, civil liability, mandated transparency measures, platform accountability, and specialised institutional infrastructure, according to the comparative research. An comparable strategy that is specifically adapted to India's constitutional framework and sociopolitical circumstances must be implemented immediately.

The following suggestions are put forth: (i) The Representation of the People Act, 1951 should be amended to forbid deepfake electoral content without ECI certification; (ii) the IT Rules, 2021 should be amended to impose proactive deepfake detection duties on SSMIs with specified timelines and loss-of-safe-harbor consequences; (iii) Parliament should enact a dedicated Deepfake Regulation Act with a graduated offence structure, statutory civil liability, and mandatory transparency obligations; (iv) CDAC shall be named the national center of excellence for deepfake detection research and law enforcement training; (v) a Deepfake Adjudication Tribunal with civil and enforcement jurisdiction should be formed.

The window of opportunity for proactive regulation is closing. The social and legal costs of inaction increase as generative AI capabilities grow rapidly. India's aspirations to become a leader in AI must be accompanied by a dedication to AI governance that protects human rights. A crucial part of that commitment is passing custom deepfake laws.

□ REFERENCES

□ Books / Commentaries / Journals Referred

□ Chesney, R. & Citron, D.K. (2019). 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security'. *California Law Review*, 107(6), 1753–1820.

□ Paris, B. & Donovan, J. (2019). *Deepfakes and Cheap Fakes: The Manipulation of Audio and Visual Evidence*. Data & Society Research Institute.

 Gupta, A. & Singh, R. (2023). 'Artificial Intelligence and Indian Cyber Law: A Study of Legislative Gaps'. *Journal of Indian Law Institute*, 65(2), 211–237.

 Narayan, S. (2024). 'Electoral Deepfakes and the Limits of Indian Electoral Law'. *National Law School of India Review*, 36(1), 88–114.

 Tolosana, R. et al. (2020). 'Deepfakes and Beyond: A Survey of Face Manipulation and Fake Detection'. *Information Fusion*, 64, 131–148.

 Online Articles / Sources Referred

 Sensity AI. (2023). *The State of Deepfakes: Landscape, Threats, and Impact.* https://sensity.ai/reports

 Internet Freedom Foundation. (2023). *Deepfakes and Democracy: Policy Brief.* https://internetfreedom.in

 Ministry of Electronics and Information Technology. (2023). *Advisory on Deepfake Content for Social Media Platforms.* Government of India.

 Election Commission of India. (2024). *Advisory on AI-Generated Political Content.* New Delhi: ECI.

 Centre for Internet and Society. (2024). *Platform Accountability and Deepfake Regulation: The Indian Context.* https://cis-india.org

 Cases Referred

 Karan Kapoor v. State of Delhi, W.P. (C) 1042/2023 (Delhi High Court)

 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1

 Budhadev Karmaskar v. State of West Bengal, Criminal Appeal No. 135 of 2010

 Statutes Referred

 Information Technology Act, 2000 (India) – Sections 66C, 66D, 67, 67A, 69A

 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

- Bharatiya Nyaya Sanhita, 2023 – Sections 74, 77, 318, 356
- Ministry of Electronics and Information Technology. (2023). *Advisory on Deepfake Content for Social Media Platforms.* Government of India.
- Election Commission of India. (2024). *Advisory on AI-Generated Political Content.* New Delhi: ECI.
- Centre for Internet and Society. (2024). *Platform Accountability and Deepfake Regulation: The Indian Context.* https://cis-india.org