The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

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

LEGAL CHALLENGES OF DEEPFAKE AND SYNTHETIC MEDIA IN INDIA

AARTI SUKHRAM

ABSTRACT

Deepfake and AI-generated synthetic media present unique threats to "individual rights" and "public order" in India. "Synthetic media" means any content such as images, videos, audios, or text which is created by any AI or machine techniques. Here this article researches the Indian legal framework considering these technologies. How statutes, especially the Information Technology Act, 2000 and other criminal laws, address impersonation, individual privacy violations, obscenity, and defamation arising from deepfakes. We analyse relevant constitutional rights, freedom of speech and privacy, and the extent of reasonable prohibitions. Legal rulings to deepfake misuse including recent injunctions in social-media cases are analysed. Finally, we emphasize enforcement challenges e.g. technical, evidentiary, and jurisdictional and offer recommendations, including legislative amendments, platform accountability, watermarking or labelling of synthetic content, and developments for law enforcement and courts. Our conclusions emphasize the need for a balanced outlook that protects individuals from damage while respecting free expression.

Keywords: Deepfake, Artificial Intelligence, Personality Rights, Synthetic media

INTRODUCTION

Deepfakes are audio, visual or text media generated or controlled by artificial intelligence to realistically represent incidents or statements that never happened. These synthetic contents can portray individuals saying or doing anything they never said or did. Widely, deepfakes have been used to generate pornographic contents by impersonate public figures for fraud or propaganda, and generate fake evidence. In India, excessive smartphone and social-media use have raise these concerns. For example, falsify videos of public officials persuading financial

schemes have appeared on WhatsApp and Twitter, and fabricated illicit images of private persons and celebrities spread widely.

Indian law does not yet recognize "deepfake", the word is not defined in any statute. The courts and regulators have tried to apply existing laws on defamation, privacy, and cybercrime to these new threats. The Constitution of India guarantees freedom of speech and expression under Article 19(1)(a), but permits "reasonable restrictions" on this freedom under Article 19(2) for interests including defamation, public order, and security. Simultaneously, the Supreme Court has held that the right to informational privacy, control over one's image and data, is part of the fundamental right to life and personal liberty under Article 21.

Deepfakes incite both values: Firstly, they can *deceive or swindle the public*, and secondly, they can *defame and infringe individuals' privacy and reputation* without consent. In this article we will look main legal issues coming out from deepfakes in India and evaluate how the existing legal framework and judicial trends can alleviate the harms.

LEGAL ISSUES

Deepfakes deals with several areas of law:

1. **Freedom of Expression vs. Misinformation:** Deepfakes can spread false or misleading statements, testifying to the tension between free speech and its abuse. Indian law prohibits speech that causes defamation, incites violence, or threatens public order. The IT Act's invalidate of Section 66A in *Shreya Singhal* (2015)[1] reiterated broad speech rights online, but also underlined that content violating legal framework e.g. defamatory or dangerous, may be curtailed. Deepfake is often responsible for misinformation or politically strangled stunts which leads riot, personal or public harmony destructions, social imbalances etc.

2. **Privacy and Personality Rights:** Deepfake technology often uses an individual's image or voice without consent. While Indian statute does not recognize a unified "right of publicity," the Supreme Court has affirmed a wide right to privacy, including control over one's personal data and likeness.[2] In *Puttaswamy case*[3], the Court warned that "dangers to privacy… can originate…from non-state actors" as well as the State,

[1] *Shreya Singhal v. Union of India* AIR 2015 SC 1523.
[2] Mahalwar, V., 2021. Burgeoning right of publicity: An overview of the Indian experiences. *The Journal of World Intellectual Property*, *24*(1-2), pp.28-40.
[3] (2017) 10 SCC 1 (India).

pressing for a robust data protection regime.[4] Misuse of personal media via AI-generated synthetic content clearly implicates this right. Victims may seek remedy under privacy principles, but litigation is very complicated because of unrecognised statutory definitions of image or similar rights.

3. **Identity Theft and Impersonation:** Deepfakes can facilitate criminal impersonation. Under the IT Act, Section 66C punishes identity theft by computer resource, and Section 66D punishes cheating by personation using a computer or communication device[5]. A deepfake video mimicking a person's voice or appearance to deceive others could fall within these prohibitions. Similarly, general offences like cheating (s.420 IPC) or forgery (ss.463–468 IPC) may apply where false media causes financial or legal harm. Prosecutions would depend on proving intentional misrepresentation and intent to defraud.

4. **Defamation and Reputation:** Synthetic media can damage an individual's reputation. Under the IPC, criminal defamation is punishable under ss.499–500 when false imputations harm a person's dignity or reputation. A deepfake video depicting someone saying defamatory statements or behaving disgracefully could attract these provisions.[6] In particular, courts have granted interim injunctions against deepfake content deemed defamatory. For example, the Delhi High Court prohibited distribution of a fake video depicting senior advocate Gaurav Bhatia being beaten, observing that such fabrication caused reputational harm[7]. Victims may also seek civil remedies under defamation law.

5. **Sexual Harassment and Obscenity:** Deepfakes have been used to place individuals, especially women, into pornographic or indecent content. There are several laws for restricting indecent contents or damage to women's modesty i.e. the IT Act, Section 67 prohibits *electronic transmission of obscene material*, Section 67A criminalizes *sexually explicit content*, and Section 67B bans *child pornography.* The IPC also contain outraging modesty of a woman under Section 354 or Section 509 and voyeurism under Section 354C, capturing a woman's image in private act. Non-consensual

[4] *Ibid.*

[5] Firdaus, M., 2025. Navigating the Legal Labyrinth: Ethical and Jurisprudential Challenges of Non-Consensual Celebrity Impersonation through Deepfake Technology. *LawFoyer Int'l J. Doctrinal Legal Rsch.*, *3*, p.156.

[6] Bateman, J., 2022. *Deepfakes and synthetic media in the financial system: Assessing threat scenarios*. Carnegie Endowment for International Peace.

[7] Gaurav Bhatia vs Naveen Kumar & Ors., CS (OS) 274/2024

insertion of a woman's face into pornographic video could potentially be prosecuted as both obscene content and an affront to her dignity.[8]

6. **National Security and Public Order:** Deepfakes may be armed for communal discord or terror. Inciting videos or announcements can provoke panic or unrest, in particular, politically. Indian statute criminalizes offences such as sedition under s.124A IPC and waging war under s.121 IPC in relevant cases, and the IT Act includes cyber-terrorism, s.66F.The IT Rules also categorize "misinformation" intended to disturb public order as "unlawful."[9] Regulatory authorities and courts are vigilant to the potential of AI-generated information to threaten sovereignty or peace.

7. **Data Protection and Consent:** Deepfakes depend on large datasets of images, videos, or biometric data. The recent Digital Personal Data Protection Act, 2023 (DPDP Act) establishes individuals' rights over their personal data and fiduciaries' obligations to process data lawfully.[10] If there is misuse of personal data e.g. a voice recording in the deepfake content then victims have a right to invoke DPDP remedies.

8. **Intermediary Liability:** there are lots of deepfake content spreads on social media and messaging platforms. The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose due diligence on intermediaries and require prompt removal of unlawful information.[11] "Unlawful" is defined broadly to include content that "knowingly or intentionally communicates any misinformation or information which is patently false and untrue or misleading".[12]

EXISTING STATUTORY FRAMEWORK AND JUDICIAL TRENDS

India has not yet enacted any specific law for the "deepfake or synthetic media crimes," but there are some available laws are applied to synthetic-media crimes. The **Information Technology Act, 2000**, Its Chapter XI talks about computer related offences:

---

[8] Vaibhav Yadav**,** Tackling Non-Consensual Dissemination of Intimate Images in India's Contemporary Legal Framework, 61 Int'l Annals Criminology 355, 355–83 (2023).

[9] Halder, D., 2011. Information Technology Act and cyber terrorism: A critical review. *Cyber Crime and Digital Disorder*, pp.75-90.

[10] Digital Personal Data Protection Act, 2023 – A Brief Analysis, *available at:* https://www.barandbench.com/view-point/digital-personal-data-protection-act-2023-a-brief-analysis (last visited on 26th July, 2025).

[11] Maamar, N., 2024, November. Due diligence obligations of providers of intermediary services. In *New Digital Services Act* (pp. 57-129). Nomos Verlagsgesellschaft mbH & Co. KG.

[12] *Supra* note 9; also see, *available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2119050#:~:text=,the%20time%20being%20in%20force* (last visited on 26th July, 2025).

1. **Identity theft (s.66C)** and **personation (s.66D)**: These provisions punish for using computer resources to fraudulently impersonate another's identity. Deepfake impersonation could fall here.
2. **Privacy violation (s.66E):** This provision punishes for violation of privacy by capture, distribution or publication of images of persons' private parts without their consent. Courts might examine deepfake portrayals of private acts (e.g. simulating nudity) to such invasions focusing at photography.
3. **Obscenity (s.67 & 67B):** Section 67 prohibits publishing or transmitting obscene material electronically and Section 67B bans child pornography. Deepfake "revenge porn" or minors' portrayal could be charged under these provisions.
4. **Cyber-terrorism (s.66F):** This was introduced in 2008. It talks about acts threatening India's security. An intentional worldly deepfake to sabotage, e.g. a fake emergency broadcast, may lead this offence.

The **Indian Penal Code** also applies:

Defamation (ss.499–500 IPC): False statements or images harming reputation.

1. **Criminal intimidation (s.503 IPC):** Threatening injury to person or reputation.
2. **Identity-related offences:** like cheating (s.420 IPC) or forgery (ss.463–468 IPC) when deepfakes are used in fraud.
3. **Sexual offences:** such as outraging modesty (s.354 IPC) or voyeurism (s.354C IPC, added in 2013 to penalize capturing a woman in a private act without consent).
4. **Obscenity (ss.292–293 IPC)** and child protection laws (POCSO Act ss.13–15).
5. **Hate and sedition:** If deepfakes spread hate propaganda, provisions like s.153A (promoting enmity) or s.124A (sedition) could apply, though these charges are rarely used and must meet strict standards.

At the constitutional level, courts balance Article 19 freedoms with 19(2) restrictions. In *Puttaswamy case*, the Supreme Court emphasized the need to protect "informational privacy" in the face of new technologies. It noted that digital data can be misused by both governments and private actors, implying that legislation should evolve to safeguard individuals. Conversely, in *Shreya Singhal v. Union of India* (2015), the Court struck down IT Act s.66A

for overbreadth, reinforcing that internet regulations must be carefully circumscribed. These precedents inform deepfake regulation: laws must target concrete harms like defamation or fraud without unduly stifling legitimate expression or satire.

Indian courts have only begun to confront deepfake cases. In National Stock Exchange of India Ltd. v. Meta Platforms, Inc. (Bombay High Court, July 2024)[13], the NSE sought removal of AI-generated videos of its CEO falsely endorsing stock-picking schemes. The court, while treating it as an interim issue, ordered Meta and other intermediaries to disable the offending content under Rule 3(1) of the IT (Intermediary) Rules, 2021. Similarly, in Gaurav Bhatia v. Naveen Kumar & Ors. (Delhi High Court, April 2024),[14] the plaintiff obtained an injunction against YouTube and Twitter channels posting deepfake videos depicting him being beaten. Justice Neena Bansal Krishna of the Delhi High Court found these videos "patently false" and "oversensationalised," noting the serious reputational harm and potential for future abuse. These cases reflect a judicial willingness to apply general law to novel AI-fraud scenarios, granting quick relief to victims.

On the legislative horizon, India has proposed updates. The Bharatiya Nyaya Sanhita, 2023 and Digital Personal Data Protection Act, 2023 both recognize harms related to deepfakes. For example, BNS Section 356 (defamation) and Section 351 (intimidation) would cover using synthetic media to tarnish reputation or threaten victims, and Section 77 would penalize non-consensual images of a woman's private act. The DPDP Act emphasizes that personal data use must be lawful and consent-based, indirectly supporting rights against unauthorized AI use of one's likeness.

CASE ANALYSIS

(1) Financial Fraud via Deepfake: In the NSE v. Meta case, sophisticated deepfake videos featured the NSE's Managing Director, urging viewers to join fraudulent investment groups. The Bombay High Court treated the videos as misleadingly using the company's trademark and CEO's likeness in violation of its exclusive rights. Emphasizing the due-diligence duties of intermediaries under the IT Rules, the court ordered immediate takedown of the fabricated videos and related content. This case underscores how deepfakes can facilitate large-scale fraud

[13] INTERIM APPLICATION (L) NO.21456 OF 2024 IN COM IPR SUIT (L) NO.21111 OF 2024, Bombay High Court.

[14] *Supra note 7.*

and how intellectual property law (protecting the NSE logo and name) combined with cyber-liability norms can be mobilized to stop them.

(2) Defamation of a Public Figure: The Gaurav Bhatia litigation illustrates deepfake use in political/activist disputes. False YouTube and social-media videos depicted the senior advocate being physically assaulted by fellow lawyers in court – an event that never occurred. Deepfake clips, along with fabricated news posts, falsely claimed Bhatia was manhandled for alleged misconduct. The Delhi High Court found the mix of video and text to be "oversensationalised and patently false," dangerously undermining Bhatia's reputation[15]. It restrained further distribution and directed platforms (Twitter and YouTube) to remove the content. This case highlights courts' readiness to impose interim injunctions to preserve individual dignity when deepfakes are weaponized in online defamation.

(3) Celebrity Identity Misuse: Although not yet adjudicated by Indian courts, numerous media reports document celebrities as deepfake targets. For instance, a viral video in 2024 showed actor Akshay Kumar endorsing a gambling app – a clip quickly identified as AI-generated. The actor reportedly lodged a cyber-complaint and urged removal of the fake ad. Similar incidents involving Bollywood actresses (Rashmika Mandanna, Alia Bhatt) etc. have raised public outcry about non-consensual pornography created by deepfake software. While these stories are not legal decisions, they indicate the real-world scale of the problem: popular individuals often lack effective recourse against rapidly spreading synthetic content until a court or platform intervenes.

CHALLENGES IN ENFORCEMENT

Several obstacles hinder effective legal enforcement against deepfakes in India:

1. **Technical Detection and Attribution:** Deepfakes are increasingly realistic and hard to distinguish from authentic media, even by experts. Identifying the technology used or the "origin" of a fake video can require sophisticated forensic tools. Victims may first need to prove that a clip is a synthetic creation, which can be expensive and time-consuming. Courts have observed that deepfakes can function as false evidence that mislead fact-finders[16]. The lack of AI-detectors in mainstream law enforcement means many instances go unnoticed until widespread.

[15] *Supra* note 7; also see, *available at: https://legal.economictimes.indiatimes.com/news/litigation/hc-orders-removal-of-defamatory-content-against-gaurav-bhatia-from-social-media/109353505#:~:text=The%20deepfake%20videos%20showing%20Bhatia,are%20patently%20false%2C%20it%20said* (last visited on 26th July, 2025).

2. **Jurisdictional and Platform Issues:** Deepfake content often spreads via global platforms (YouTube, Twitter, Telegram, WhatsApp). Indian law requires takedown via the IT Rule. In practice, intermediaries usually demand a court order or government notice before disabling content. The NSE case showed that even a major stock exchange needed a court directive for expedited action. Cross-border content-sharing means that by the time a video is taken down in India, it may persist elsewhere.

3. **Burden on Victims:** Under current law, victims bear the burden of showing how a deepfake harms them. There is no presumption of malicious intent merely because content is AI-generated. In litigation, victims must prove defamation or intimidation elements. As courts in the Bhatia case noted, malicious posts "cause harm" and "persistent threat" to future reputation, but obtaining relief requires prompt legal action, which can be costly and slow. Ordinary individuals may lack resources to pursue injunctions or damages.

4. **Lack of Specific Penal Offence:** Because there is no distinct "deepfake" statute, offences must be shoehorned into existing categories. This can limit deterrence: a creator of a malicious deepfake might rationalize the act as parody or harmless if they perceive that no unique rule forbids the creation itself. Some stakeholders have called for specific legislation a "Deepfake Prohibition Act" to criminalize the generation or dissemination of malicious synthetic media with intent to deceive. Until then, prosecutors rely on analogues (fraud, defamation, obscenity) which may not fully capture the new modus operandi.

5. **Balancing Free Expression:** Regulators must tread carefully to avoid overbroad censorship. Some uses of synthetic media (e.g. satire or film production) are lawful and protected by free speech.[17] Proposed laws or platform policies risk chilling legitimate art or commentary if worded too widely. Supreme Court has repeatedly struck down vague speech restrictions.[18] Thus, any enforcement approach must clearly distinguish malicious deepfakes (forgery, fraud, harassment) from permissible creativity. This

[16] Khoo, B., Phan, R.C.W. and Lim, C.H., 2022. Deepfake attribution: On the source identification of artificially generated images. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *12*(3), p.e1438.
[17] Bourgault, J.R., 2025. Free Speech and Synthetic Lies: Deepfakes, Synthetic Media, and the First Amendment. *Student Journal of Information Privacy Law*, *3*(1), p.49.
[18] India's section 66A scrapped: Win for free speech, *available at:* https://www.bbc.com/news/world-asia-india-32029374(last visited on 26th July, 2025).

balancing act complicates drafting of new rules and the training of enforcement officials.

6. **Awareness and Training:** Police, prosecutors, and judges may lack awareness of deepfake technology. Many may not recognize a fake even when presented. There is a need for capacity-building within the Indian Computer Emergency Response Team (CERT-In) and law enforcement agencies (such as the I4C cybercrime cell) to identify AI-manipulated content. Without forensic expertise, cases may be dismissed as "user generated content" or outside the scope of traditional cybercrime.

7. **Privacy of Accused:** Ironically, investigating a deepfake case can raise privacy issues. Law enforcement must be cautious not to over-collect data from platforms or infringe user privacy in tracing deepfake sources. The IT Act itself protects personal data and communications from unauthorized interception, which may limit certain investigative tools.

Overall, while Indian authorities have taken steps (such as CERT-In advisories in 2023–2024 and the 2021 IT Rules update) to sensitize industry, enforcement on the ground remains largely reactive and piecemeal.[19]

CONCLUSION AND RECOMMENDATIONS

Deepfake and synthetic-media technology pose a multifaceted legal challenge for India. The existing framework – spanning the IT Act, IPC, and recent data protection law provides some recourse against abuses like as identity theft, defamation or obscenity. However, the legal landscape is unsettled. Courts have begun to apply these laws to deepfake cases, granting relief in high-profile instances, but there is no comprehensive statute addressing the root phenomenon.

To mitigate these gaps, several measures are advisable:

1. **Legal Clarity:** India should consider updating its statutes to explicitly cover malicious synthetic media. This could take the form of specific amendments, for instance, adding a section to the IT Act or IPC criminalizing creation or distribution of non-consensual deepfakes intended to harm or an omnibus "Deepfake" provision. Such a law should

[19]Government of India Taking Measures To Tackle Deepfakes*, Available at:* https://www.pib.gov.in/PressReleasePage.aspx?PRID=2119050#:~:text=,promptly%20remove%20harmful%20content%20online(last visited on 26th July, 2025).

define key terms (e.g. "synthetic voice or image") and target malevolent uses (fraud, defamation, harassment) while carving out exemptions for lawful expression e.g. news reporting, satire, parody. Transparent framing will help police and courts handle cases consistently.

2. **Platform Accountability:** Intermediaries should adopt clearer protocols for identifying and labelling AI-generated content.[20] The government's late-2023 advisory recommended that platforms embed indelible watermarks or metadata in synthetic media to tag it as "synthetic". This could be codified, requiring AI content generators to disclose machine-generation. Platforms should also invest in better AI-detection tools and fast-track credible removal requests for suspected deepfakes. Strengthening the grievance and appellate mechanism under the IT Rules will empower victims to challenge any refusal by intermediaries to act.

3. **Law Enforcement and Judiciary Training:** Authorities need technical support. Establish dedicated cyber-forensic labs skilled in deepfake detection, and train investigating officers and prosecutors on the nuances of AI content. The Indian Cyber Crime Coordination Centre (I4C) and CERT-In can lead workshops for police and magistrates. Educating stakeholders will improve evidence-gathering e.g. forensic analysis of video files and judicial understanding of when to grant relief.

4. **Public Awareness:** Citizens must learn to critically assess media. Government campaigns through CERT-In and consumer forums can alert people to the existence of deepfakes and encourage prompt reporting of suspicious content via the National Cyber Crime Reporting Portal. Awareness will help contain the viral spread of fakes and reduce victims' damages.

5. **Multi-Stakeholder Collaboration:** Regulators should engage AI researchers, digital platforms, and civil society in crafting guidelines. Drawing on international best practices such as the EU's AI Act requirements for audio-visual transparency, or U.S. proposals for penalizing non-consensual deepfake pornography can inform Indian policy while adapting to our context. Any solutions must balance security and ethics with the constitutional commitment to free discourse.

---

[20] He, X. and Fang, L., 2024. Regulatory Challenges in Synthetic Media Governance: Policy Frameworks for AI-Generated Content Across Image, Video, and Social Platforms. *Journal of Robotic Process Automation, AI Integration, and Workflow Optimization*, *9*(12), pp.36-54.

6. **Victim Support Mechanisms:** Fast-track remedies like emergency injunctions and expedited investigation are crucial. Victims of deepfake harassment should have access to quick legal assistance or legal aid.[21] Consideration should be given to criminalizing failure to remove confirmed deepfake harassment upon demand, to shift some onus onto perpetrators and negligent platforms.

In summary, India's laws can be interpreted to address some deepfake harms, but the technology's rapid evolution calls for proactive reforms. A combination of targeted legal amendments, enhanced enforcement capacity, and technology-based safeguards e.g. labeling, forensic tools will be needed. By acting now, India can better protect individual dignity and public trust without undermining legitimate innovation and expression.

[21] Ali, M., Fernando, Z.J., Huda, C. and Mahmutarom, M., 2025. Deepfakes and Victimology: Exploring the Impact of Digital Manipulation on Victims. *Substantive Justice International Journal of Law*, *8*(1), pp.1-12.