
LEGAL CHALLENGES OF DEEPPAKES AND AI-GENERATED CONTENT IN INDIA

***Kurunandan Patel**

An Article on Emerging Technology, Individual Rights and the Indian Legal Framework.

Article Received: 08 August 2026

***Corresponding Author: Kurunandan Patel**

Article Revised: 28 August 2026

An Article on Emerging Technology, Individual Rights and the Indian Legal Framework.

Published on: 18 September 2026

DOI: <https://doi-doi.org/101555/ijrpa.5268>

ABSTRACT

Deepfakes and other forms of AI-generated or synthetically manipulated content have created a new category of legal and social risk. By using artificial intelligence to imitate a person's face, voice, appearance or manner of expression, synthetic content can appear authentic even when the depicted event never occurred. The technology itself is not inherently unlawful; it can support education, entertainment, accessibility, research and creative expression. The legal difficulty arises when synthetic content is used without consent to deceive, impersonate, defame, invade privacy, facilitate fraud, spread misinformation or create sexually explicit material involving real persons. India therefore faces the challenge of applying existing laws to rapidly changing technology while also protecting freedom of speech and innovation.

This article examines the principal legal challenges created by deepfakes and AI-generated content in India. It considers the Information Technology Act, 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, privacy and constitutional principles, intellectual property and personality rights, criminal liability, intermediary responsibility, and the emerging regulatory approach to synthetic media. It also discusses the need for transparent labelling, rapid grievance redressal, preservation of evidence, human review and stronger coordination between platforms, investigators and courts. The article argues that India should adopt a technology-neutral but harm-sensitive approach: regulation should focus on the unlawful use and consequences of synthetic content rather than treating every AI-generated work as illegal.

KEYWORDS: Deepfakes; Artificial Intelligence; Synthetic Media; Cyber Law; Privacy; Personality Rights; Freedom of Speech; Intermediary Liability; Information Technology Act; Digital Rights; Misinformation; Indian Legal System.

1. INTRODUCTION

Artificial intelligence has changed the way digital images, audio and videos can be created and modified. A person can now generate highly realistic material that resembles an actual photograph, recording or public statement. Deepfakes are a particularly important form of synthetic media because they can place a real person's face or voice into content that the person did not create or participate in. The increasing realism of such material creates a serious evidentiary and legal problem: the ordinary viewer may find it difficult to distinguish genuine content from manipulated content.

The legal importance of deepfakes lies not merely in their technical sophistication but in the harm that may follow from their use. A fabricated video can damage reputation, create a false endorsement, impersonate a public figure, mislead consumers, interfere with public discourse, or violate an individual's privacy. Synthetic intimate material can cause particularly serious personal harm. At the same time, not every manipulated image or AI-generated video should be prohibited. Satire, parody, artistic expression, film-making, education and legitimate experimentation may involve synthetic media without causing unlawful harm.

India's existing legal framework contains several provisions that may apply to harmful synthetic content. The Information Technology Act, 2000 addresses identity theft, cheating by personation using computer resources, privacy violations and certain categories of obscene or sexually explicit electronic material. The IT Rules, 2021 impose due-diligence duties on intermediaries. Constitutional protections of speech and privacy provide a broader framework for evaluating restrictions. Recent government measures concerning synthetically generated information demonstrate that the regulatory conversation is continuing to develop.

2. Meaning and Nature of Deepfakes

The term 'deepfake' generally refers to synthetic or manipulated audio-visual content created with machine-learning or related computational techniques to make it appear that a person said or did something that they did not actually say or do. Deepfakes may involve face replacement, voice cloning, lip-sync manipulation, synthetic avatars or combinations of real and generated material. The technology can be used for harmless creative purposes, but it can also be used to create deceptive or unlawful content.

It is useful to distinguish deepfakes from ordinary photo or video editing. Traditional editing may be obvious or limited to changes in lighting, cropping or background. Deepfake systems can reproduce facial expressions, voices and movements in a manner that creates a much

stronger impression of authenticity. This creates an evidentiary challenge for courts, investigators, journalists and members of the public because visual or audio appearance alone may no longer be sufficient to establish authenticity.

The central legal question should therefore be framed around harm, consent, deception and context. A synthetic advertisement clearly labelled as fictional is legally different from a fabricated recording falsely presented as a real statement. Likewise, a parody that is reasonably understood as satire is different from a deceptive impersonation designed to obtain money or damage someone's reputation.

3. Why Deepfakes Create a Legal Problem

3.1 Deception and Impersonation

Deepfakes can make one person appear to be another person. When used for fraud, this can overlap with legal concepts of cheating, personation and identity theft. The Information Technology Act contains provisions addressing identity theft under Section 66C and cheating by personation using a computer resource under Section 66D. These provisions are particularly relevant where synthetic media is used as part of a fraudulent digital transaction.

3.2 Privacy and Personal Autonomy

A person's face, voice and other identifying characteristics can be closely connected with personal autonomy and dignity. Using such characteristics without consent can create a serious privacy concern, especially when the material is intimate or humiliating. The constitutional recognition of privacy in India strengthens the importance of consent and proportionality when personal information or identity is digitally manipulated.

3.3 Reputation and Defamation

A false video may communicate an apparently factual allegation about an individual. If viewers believe the fabricated material, reputational injury may follow. Existing civil and criminal legal principles concerning defamation may therefore become relevant depending on the facts. The challenge is evidentiary: the victim must be able to establish that the content is fabricated and that the publication satisfies the relevant legal requirements.

3.4 Sexualised and Non-Consensual Synthetic Content

One of the most serious uses of deepfake technology is the creation or distribution of non-consensual sexualised content involving a real person. Existing provisions concerning obscene and sexually explicit electronic material may become relevant, together with other criminal and civil remedies depending on the circumstances. The law must also recognise the

speed with which such material can spread and the importance of rapid removal and effective grievance redressal.

3.5 Misinformation and Public Trust

Synthetic political speeches, fabricated news clips or false recordings can weaken trust in legitimate information. The risk is not limited to individual victims; widespread synthetic misinformation can affect public debate and social stability. Regulation must, however, be carefully designed so that combating misinformation does not become a pretext for suppressing lawful criticism, satire or political expression.

4. Constitutional Dimensions

4.1 Freedom of Speech and Expression

Article 19(1)(a) of the Constitution protects freedom of speech and expression. AI-generated content may fall within the broad sphere of expression, particularly where it is used for art, commentary, parody or research. Any restriction must therefore operate within the constitutional framework, including the permissible restrictions under Article 19(2). The legal system should distinguish between expression that is merely artificial and expression that causes legally recognised harm.

4.2 Right to Privacy

The Supreme Court's privacy jurisprudence recognises privacy as a constitutional value connected with dignity, autonomy and personal liberty. Deepfakes can interfere with these interests when a person's identity, likeness or voice is used without meaningful consent. A proportionate legal response should consider the purpose of processing, the nature of the content, the degree of deception, the actual or foreseeable harm and the availability of less restrictive alternatives.

4.3 Equality and Dignity

Synthetic content can disproportionately affect individuals who have limited resources to monitor the internet or obtain legal assistance. The principle of dignity also becomes important when a person is depicted in a humiliating or degrading manner. Effective legal remedies should therefore not depend entirely on a victim's ability to identify every account or platform on which manipulated content has appeared.

5. Existing Legal Framework in India

5.1 Information Technology Act, 2000

The Information Technology Act, 2000 is technology-neutral in important respects and contains provisions capable of applying to harmful AI-generated content. Section 66C addresses identity theft; Section 66D addresses cheating by personation using a computer resource; Section 66E addresses violation of privacy; and Sections 67 and 67A address certain categories of obscene and sexually explicit material in electronic form. Section 69A provides a statutory mechanism concerning blocking of public access to information in specified circumstances. The relevance of each provision depends on the facts and the legal ingredients that can be established.

5.2 Intermediary Due Diligence

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 establish due-diligence obligations for intermediaries. Their framework is important because harmful synthetic content is commonly distributed through social-media and other online services. Intermediary responsibility, grievance mechanisms and lawful removal processes can therefore become central to the practical protection of victims.

5.3 Emerging Regulation of Synthetically Generated Information

The Government has increasingly focused on synthetic media. In 2025, MeitY published proposed amendments concerning synthetically generated information, recognising risks including misinformation, privacy violations, impersonation and fraud. By February 2026, MeitY's published IT Rules materials reflected amendments relating to synthetically generated information. This indicates a move toward more explicit treatment of synthetic content within the intermediary framework, including questions of labelling, accountability and compliance.

5.4 Digital Personal Data Protection Framework

The Digital Personal Data Protection Act, 2023 provides a statutory framework concerning the processing of digital personal data. Its relevance to AI-generated content depends on the facts, including whether personal data is processed in creating or distributing synthetic content and whether the statutory conditions and obligations apply. The Act should therefore be considered alongside, rather than as a complete substitute for, the IT Act and other legal remedies.

6. Personality Rights and Intellectual Property

Indian courts have increasingly addressed protection of an individual's name, image, voice and persona. Deepfake technology can exploit these elements commercially or deceptively. The Delhi High Court's 2023 proceedings involving actor Anil Kapoor illustrate the growing importance of personality rights, including concerns over unauthorised use of name, image and voice and associated claims such as passing off and unfair competition. Such cases demonstrate that the law of personality rights can provide an important civil remedy where existing criminal provisions do not fully capture the harm.

Copyright questions may also arise where AI-generated material incorporates protected photographs, films, sound recordings or other works. However, copyright analysis is fact-specific and should not be treated as automatically establishing ownership over every AI-generated output. A careful legal approach must distinguish between the unlawful use of an existing protected work and the separate problem of impersonating a person through synthetic content.

7. Important Judicial Developments

7.1 K.S. Puttaswamy v. Union of India

The Supreme Court's decision recognising privacy as a fundamental right is highly relevant to synthetic media because deepfakes can interfere with personal autonomy, dignity and control over information about oneself. The judgment provides the constitutional foundation for evaluating privacy intrusions and the proportionality of State measures affecting privacy.

7.2 Anil Kapoor v. Simply Life India & Ors.

In proceedings before the Delhi High Court, actor Anil Kapoor sought protection against unauthorised exploitation of his personality, including his name, image, voice and other aspects of his persona. The court's order is significant for the developing Indian jurisprudence on personality rights and demonstrates the potential of civil injunctions to address unauthorised digital exploitation of a person's identity. The case is especially relevant to AI-era concerns because synthetic technologies make unauthorised imitation increasingly easy.

7.3 Shreya Singhal v. Union of India

The Supreme Court's decision striking down Section 66A of the Information Technology Act is important when considering online speech. It reinforces the need for legal restrictions on digital expression to satisfy constitutional standards. Any future deepfake regulation should therefore be sufficiently clear and targeted so that lawful speech is not unnecessarily restricted.

8. Liability of Different Actors

8.1 The Creator

The creator or user who knowingly generates harmful synthetic content may bear primary responsibility when the conduct satisfies the requirements of an applicable offence or civil wrong. Intent, knowledge, deception, consent and resulting harm will often be important factual questions.

8.2 The Uploader or Distributor

A person who republishes or forwards a deepfake may contribute to its spread. Liability should not automatically be assumed merely because content was forwarded; knowledge, intent and the applicable statutory requirements matter. At the same time, deliberate amplification of known false or unlawful material can increase the seriousness of the conduct.

8.3 Online Platforms and Intermediaries

Platforms occupy a special position because they can facilitate rapid dissemination while also possessing technical tools for reporting, detection and removal. Indian intermediary law therefore places due-diligence obligations on platforms. The challenge is to require effective systems without turning platforms into unrestricted private censors of lawful speech.

8.4 AI Developers and Service Providers

Questions may arise concerning the role of AI developers and providers whose tools can generate synthetic media. A balanced framework should distinguish between general-purpose technology and deliberate or reckless facilitation of unlawful conduct. Product safeguards, provenance tools, user reporting and appropriate terms of service can reduce risk without eliminating legitimate uses of generative technology.

9. Evidentiary Challenges

Deepfakes challenge traditional assumptions about audio-visual evidence. A recording may look genuine while being fabricated, while a genuine recording may be falsely labelled as a deepfake. Courts and investigators therefore need reliable methods of authentication. Digital forensic examination, metadata, source verification, device records, chain of custody and expert evidence may become increasingly important.

A further difficulty is that deepfake detection tools are not infallible. Detection systems can produce false positives or become less effective as generation technology improves. Consequently, courts should avoid treating a single automated detector as conclusive proof. Authentication should be based on a combination of technical evidence and surrounding circumstances.

10. Challenges in Enforcement

First, synthetic content can cross jurisdictions rapidly, making investigation difficult. Second, anonymous or pseudonymous accounts can complicate identification of offenders. Third, victims may face repeated reposting even after one copy is removed. Fourth, technology changes faster than legislation, creating gaps between new forms of harm and existing legal categories. Fifth, victims may not know which legal remedy or reporting mechanism is appropriate.

These challenges show that legal reform alone is insufficient. Effective enforcement requires cooperation between law-enforcement agencies, courts, platforms, forensic experts, regulators and affected individuals. Clear procedures for preservation of evidence and rapid response can be as important as the substantive law itself.

11. Need for a Balanced Regulatory Approach

A strong regulatory model should avoid two extremes. The first is under-regulation, in which victims are left without effective remedies while harmful synthetic content spreads rapidly. The second is over-regulation, in which lawful creative expression and technological innovation are unnecessarily restricted. A balanced approach should focus on the nature of the harm, the role of the actor, the level of deception, consent, intent and the public interest. Labelling can be useful where content is synthetic but lawful. Provenance and authenticity technologies can help users identify the origin or history of media. At the same time, labelling should not be treated as a substitute for removal where content is independently unlawful. The legal system should also provide accessible complaint mechanisms, especially for individuals whose identity has been misused.

12. Recommendations

- Develop clear and technology-neutral rules that specifically address harmful synthetic media while preserving lawful expression.
- Strengthen platform-level reporting and grievance mechanisms for impersonation, privacy violations and unlawful synthetic content.
- Promote clear labelling or provenance mechanisms for synthetic content where appropriate, while recognising that labels cannot replace legal remedies.
- Create rapid-response procedures for serious cases involving identity misuse, fraud, intimate synthetic content or threats to safety.

- Improve digital-forensics capacity and training for police, prosecutors and courts so that authenticity disputes can be assessed scientifically.
- Encourage preservation of original files, metadata and other digital evidence to support investigation and judicial proceedings.
- Promote public digital literacy so that users understand that realistic audio and video are not necessarily authentic.
- Require meaningful safeguards in AI systems that generate or manipulate realistic images, audio and video, especially where impersonation is possible.
- Maintain constitutional safeguards for freedom of speech, satire, artistic expression and legitimate criticism.
- Encourage cooperation among regulators, technology companies, civil society, researchers and law-enforcement agencies to respond to emerging forms of synthetic abuse.

13. CONCLUSION

Deepfakes and AI-generated content represent a major development in the digital environment because they weaken the traditional assumption that an apparently authentic photograph, recording or video is necessarily genuine. The resulting legal problems involve privacy, dignity, reputation, identity, fraud, intellectual property, intermediary responsibility and freedom of expression. India's existing legal framework already provides several routes for addressing harmful conduct, particularly through the Information Technology Act, intermediary rules, constitutional rights and civil remedies such as personality-right protection.

Nevertheless, the rapid evolution of generative technology makes continuous legal and institutional adaptation necessary. The objective should not be to prohibit artificial or synthetic content as such. Instead, the law should identify and address harmful uses while preserving legitimate innovation and expression. Clear rules, effective grievance mechanisms, reliable digital forensics, responsible platform practices and constitutional safeguards can together provide a workable response. Ultimately, the central principle should be that technological sophistication does not remove legal accountability: when AI is used to deceive, impersonate, exploit or unlawfully harm another person, the availability of advanced technology should not become a shield against responsibility.

14. REFERENCES

1. Constitution of India, Articles 14, 19, 21 and 32.
2. Information Technology Act, 2000, Government of India.
3. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended.
4. Digital Personal Data Protection Act, 2023, Government of India.
5. K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
6. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
7. Anil Kapoor v. Simply Life India & Ors., CS(COMM) 652/2023, Delhi High Court, order dated 20 September 2023.
8. Ministry of Electronics and Information Technology, Government of India, materials and advisories concerning the Information Technology Rules and synthetically generated information.
9. India Code, Information Technology Act, 2000.
10. Government of India, Gazette of India, Digital Personal Data Protection Act, 2023.