



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

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.

AI-GENERATED DEEPPAKES AND THE INDIAN LEGAL FRAMEWORK: A LEGAL ANALYSIS

Srabanti Biswas

ABSTRACT

Artificial Intelligence has changed the way digital content is produced and shared, making it possible to create images, videos and audio that can appear remarkably real. Deepfakes are one such development, where a person's face, voice or actions can be digitally created or altered. While this technology can be used for legitimate purposes in fields such as education, entertainment and media, its misuse can cause serious harm through impersonation, fraud, harassment, misinformation, privacy violations and non-consensual intimate content. These developments have created new legal concerns in India, particularly because many existing laws were framed before such advanced forms of synthetic media became common. This article examines how the Indian legal system deals with deepfake-related harms through constitutional protections, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Rules, 2021. It also looks at important judicial decisions concerning privacy and personality rights, along with recent regulatory measures relating to Synthetically Generated Information. The article further considers difficulties in detecting deepfakes, securing their timely removal and providing effective remedies to victims. It concludes that India needs a practical and balanced legal approach that protects individuals from harmful uses of deepfakes while allowing legitimate expression, creativity and technological development.

Keywords: *Artificial Intelligence, Deepfakes, Cybercrime, Privacy, Indian Legal Framework.*

I. INTRODUCTION

Artificial intelligence is perhaps one of the most significant technological innovations of our time and has transformed the ways in which data is produced, changed, and disseminated. The

advent of generative AI has enabled the production of highly realistic synthetic images, videos, and sounds, termed deepfakes. While the use of this technology can be beneficial in disciplines like education, entertainment, healthcare and digital media, the potential harm of such technology cannot be ignored in terms of privacy, cybersecurity, and access to justice. Since the availability of AI tools and social media has made the production and distribution of misleading content easy and simple in countries like India, instances of deepfakes occurring for purposes like identity theft, cyber stalking, harassment, extortion, and non-consensual production of personal content can cause great damage to an individual's right to privacy and personal security as well as dignity and reputation. Hence, it is imperative to ask an important legal question in this context: are India's laws adequate to deal with AI-based cybercrimes.¹

II. MEANING AND DEVELOPMENT OF ARTIFICIAL INTELLIGENCE

The term artificial intelligence was introduced in the mid-20th century, when John McCarthy used it in his 1956 paper. Even though there is no single formal definition of AI in law, the meaning of AI in practice is clear. It suggests the machines' ability to perform actions that usually require the human brain. Such functions may include reasoning, learning, perception, making decisions and processing language. Thus, AI has moved from the domain of the theory of computer science to the realm of technology that produces sophisticated forms of digital information.²

III. DEEPFAKES: MEANING, NATURE AND DEVELOPMENT

Deepfakes are one of the most contentious uses of contemporary AI as they may generate digital content that seems authentic even when it has been artificially produced or altered. Deepfake systems may mimic voices, substitute faces, and change video content in ways that could be hard for a regular viewer to notice by using algorithms such as machine learning and neural network approaches. Virtual reality, teaching, movie production, and other artistic endeavours are all acceptable uses for the technology. However, the accessibility of harmful usage has also increased because to the availability of low-cost and user-friendly AI technologies. Deepfakes may be used for fake appearances, scams, assault, disinformation, and the production of illicit sexual content. Certain types of deepfake exploitation, such as distorted personal photos, are especially dangerous for all individuals. The rapidity and extent of online

¹ Bhawya Prajapati and Dr Surbhi Dadhich, *AI-Generated Deepfakes and Cyber Violence Against Women in India: Legal Challenges and Policy Response*, 14 INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT) c 579, c 580 (2026).

² V. K. Ahuja, *Artificial Intelligence and Copyright: Issues and Challenges*, ILI LAW REVIEW, WINTER ISSUE 2020 (Sep. 19, 2026, 10.40 A.M.), <https://ili.ac.in/pdf/vka.pdf>.

engagement exacerbate the issue in the Indian setting. Although many types of deepfake abuse can be covered by current cyber and criminal laws, these regulations were mostly created before to the broad accessibility of current artificial intelligence generative systems. This makes it more challenging to recognize criminals, preserve proof, and give survivors speedy compensation.³

IV. HOW DEEPPFAKE TECHNOLOGY WORKS

Deepfake algorithms may change both image and sound features using methods including facial image morphing, facial switching, recreation, speech creation, and vocal copying. Facial gestures can be manipulated to make an individual seem to be expressing sentiments or doing acts that didn't happen. In the same way, an artificial face may be created or a natural face transplanted to a different individual's physique. Voice replication technology may recreate patterns of speech and voice features, allowing for the creation of authentic but fake audio. Such abilities raise legal issues with permission, identification, confidentiality, reputation, deception, proprietary information, and data security. The law must consequently distinguish between legal digital media uses and scenarios in which this type of technology is exploited to conceal or injure. Since this type of technology has some beneficial aspects, deepfake and artificially generated media technologies should not be classified as illegal by default because they have some valid uses. AI-generated voices and personalized digital resources may help people with impairments in terms of easy access. Artificial multimedia material in education has the potential to make classes more engaging and facilitate distance learning. Digital synthesizing is used in the media industry for graphical effects, dubbing, personality replication, and other creative applications. Virtual assistants, autonomous customer support platforms, and other corporate applications may also make use of similar technologies. However, nowadays individuals exploit this technology incorrectly. The legal difficulty is thus to prohibit harmful behaviour without unduly impeding proper technical advancement.⁴

V. TYPES OF DEEPPFAKES

Deepfakes can take several shapes.

- a. Appearance switching technologically swaps one person's face with another, potentially resulting in a false impression of identification.

³ Shreya Kothari and Sohail Malik et. al., *Regulation of deepfake content under cyber law*, 13. TIJER – INTERNATIONAL RESEARCH JOURNAL c660, c660 (2026).

⁴ Mr. Chitranshu Bhaska and Ms. Nisha Kumari Agarwal et.al., *Artificial Intelligence and Deepfakes Media: Challenges Before Law*, VII. INDIAN JOURNAL OF LAW AND LEGAL RESEARCH 4842, 4844-4847 (2025).

- b. Voice replication and synthesis of speech recreate an individual's voice and are capable of making it look as if the individual uttered remarks that have never actually occurred.
- c. Completely manipulated media may provide a completely fabricated individual, incident, or circumstance.
- d. Lip-syncing and face mirroring can enhance a person's voice and gestures.

These fake mediums can be used for benign artistic objectives, but they may also help in scams, extortion, disinformation, damage to reputation, and public sentiment influence. Their seeming legitimacy makes such abuse extremely difficult to counteract.⁵

VI. LEGAL CHALLENGES CREATED BY DEEPPFAKES

Deepfake identification remains challenging since realistic artificial content can elude normal human inspection, whilst automated systems are not always reliable and may need human confirmation. Because generating techniques are rapidly evolving, detection instruments must likewise be constantly upgraded. As a result, public consciousness and media literacy are vital. Technology alone can't fix the issue; effective regulation necessitates a mix of analytical techniques, legal approaches, software platform responsibility, and user knowledge. Regulation must also strike a delicate equilibrium between privacy breaches, scams, assault, and reputational injury, as well as fundamental rights including happiness, artistic expression, press, and education. The emphasis should thus be on harmful applications and their effects, rather than classifying all AI-generated material as illegal. The production of non-consensual sexual images through the manipulation of deepfake technology poses a significant risk for women, as is the use of deepfakes sexually to criminalise women and girls⁶.

VII. INDIAN LEGAL FRAMEWORK

a. THE CONSTITUTION OF INDIA: RIGHT TO PRIVACY

Deepfakes can misuse a person's face, identity, voice or other personal features without consent, raising serious concerns under Article 21 of the Constitution⁷, which protects the right to life and personal liberty. The Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017)⁸ recognized privacy as a fundamental right, extending beyond physical privacy to

⁵ Mr. Chitranshu Bhaska and Ms. Nisha Kumari Agarwal et.al., *Artificial Intelligence and Deepfakes Media: Challenges Before Law*, VII. INDIAN JOURNAL OF LAW AND LEGAL RESEARCH 4842, 4847-4848 (2025).

⁶ Mr. Chitranshu Bhaska and Ms. Nisha Kumari Agarwal et.al., *Artificial Intelligence and Deepfakes Media: Challenges Before Law*, VII. INDIAN JOURNAL OF LAW AND LEGAL RESEARCH 4842, 4848-4850 (2025).

⁷ INDIA CONST. art. 21.

⁸ *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.

personal autonomy, dignity and control over personal information. This constitutional protection is particularly relevant to deepfakes involving identity manipulation, sexual content, harassment or unauthorized use of personal data. Indian courts have started addressing the issue of the misuse of personality traits through new technologies.' In *Anil Kapoor v. Simply Life India & Ors*⁹, granted injunctive relief to the actor's name, image, voice, and likeness through unauthorised commercial use of AI-related content by the Delhi High Court. Similarly, in *Amitabh Bachchan case*¹⁰, The Delhi High Court granted a protection against the unauthorised commercial use of an actor's name, image, voice, and likeness in *Rajat Negi & Ors.* by the court. These cases show the willingness of Indian courts to apply established principles concerning privacy and personality rights to novel forms of technological identity manipulation¹¹.

“Deepfake has deep roots in India, where it is majorly used in politics, the film industry, pornography, and even in cases of revenge- defamation. From the cases ranging from deepfake depicting Mr. Manoj Tiwari insulting the state government of Delhi, the Aam Aadmi Party speaking English and Haryanvi, to the generation of pornographic content, example being that of Ms. Rana Ayyub, it is pertinent that the deepfake can cause major harm to the person himself or herself being targeted as well as the society, by injuring sentiments, thoughts, and perspectives of the people. In another case a corporate company named Rephrase.ai made a deepfake of Mr. Hrithik Roshan, showing him congratulating his fans. However, Mr. Hrithik had licensed Rephrase.ai to use his face and make him say anything for confectionery Cadbury. Even if the acts done are legal, there is still a requirement of Laws governing the use of deepfakes.”¹²

b. STATUTES

The law of defamation can cause reputational harm in cases related to fake news and deepfakes. Section 356 of the 2023 BNS¹³ outlines punishments for defamation, under which there will be (subject to) imprisonment as punishment; fine or both; or community service as prescribed by law. Civil remedies for defamation may be available in appropriate situations.

⁹ *Anil Kapoor v. Simply Life India & Ors.*, CS(COMM) 652/2023.

¹⁰ *Amitabh Bachchan v. Rajat Nagi*, CS(COMM) 819/2022.

¹¹ Mr. Chitranshu Bhaska and Ms. Nisha Kumari Agarwal et.al., *Artificial Intelligence and Deepfakes Media: Challenges Before Law*, VII. INDIAN JOURNAL OF LAW AND LEGAL RESEARCH 4842, 4852-4856 (2025).

¹² *Is Indian law equipped enough to deal with deepfakes*, I.PLEADERS (Sep. 20, 2026, 12.38 P.M.), <https://blog.ipleaders.in/is-the-indian-law-equipped-enough-to-deal-with-deepfakes/>.

¹³ The Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code.

The current legal basis for cyber defamation should not be attributed to Section 66A of the IT Act¹⁴. Section 66A was declared unconstitutional by the Supreme Court in the Shreya Singhal case¹⁵, as determined by recent legal developments. Union of India. Therefore, defamation resulting from deepfakes should be investigated within the scope of what remains legally applicable (including criminal law and other relevant legal remedies).

In cases of personation, forgery or false electronic records, and certain types of harmful false information, the BNS¹⁶ may be applicable¹⁷.

VIII. GOVERNMENT AND MEITY RESPONSE TO AI-GENERATED DEEPFAKES

- i. **IT ACT, 2000:** Sections 43, 66, 66C, 66D, 66E, 67 and 67A address computer-related offences, identity theft, impersonation, privacy violations and obscene or sexually explicit content. Sections 69A and 79 provide mechanisms concerning blocking and intermediary liability.
- ii. **BHARATIYA NYAYA SANHITA, 2023:** Sections 319, 336, 353 and 111 may apply to cheating by personation, forgery, harmful false information and organised cybercrime.
- iii. **IT RULES, 2021:** Intermediaries must exercise due diligence against unlawful, misleading, privacy-invasive and impersonating content, including AI-based impersonation. SSIMs have additional compliance and grievance-redressal duties.
- iv. **2026 SGI AMENDMENTS:** The February 2026 amendments introduced specific safeguards for Synthetically Generated Information (SGI), including deepfakes. They require clear labelling of permissible AI-generated content and technical measures against unlawful synthetic content, including CSAM, NCII and deceptive impersonation. Certain takedown and grievance timelines were also shortened.
- v. **AI GOVERNANCE:** The India AI Governance Guidelines, released on 5 November 2025, promote a risk-based and proportionate approach to safe and responsible AI.
- vi. **DEEPFAKE DETECTION:** Under the Safe & Trusted AI pillar of the IndiaAI Mission, initiatives such as Saakshya, AI Vishleshak and IIT Kharagpur's real-time voice-deepfake detection project support technological responses to deepfakes.

¹⁴ The Information Technology Act, No. 21 of 2000, India Code.

¹⁵ Shreya Singhal v. Union of India (2015) 5 SCC 1.

¹⁶ The Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code.

¹⁷ Mr. Chitranshu Bhaska and Ms. Nisha Kumari Agarwal et.al., *Artificial Intelligence and Deepfakes Media: Challenges Before Law*, VII. INDIAN JOURNAL OF LAW AND LEGAL RESEARCH 4842, 4853-4855 (2025).

- vii. **CYBERCRIME ENFORCEMENT:** I4C, the SAHYOG Portal and the National Cyber Crime Reporting Portal support reporting, investigation and removal of unlawful online content. The 1930 helpline is also available for cybercrime complaints.
- viii. **GRIEVANCE REDRESSAL:** Intermediaries must provide grievance mechanisms, while the Grievance Appellate Committee (GAC) provides an appellate avenue against specified intermediary decisions.
- ix. **NCII PROTECTION:** A Government SOP issued on 11 November 2025 provides guidance for dealing with non-consensual intimate and morphed images.
- x. **AWARENESS AND CERT-IN:** MeitY conducts cyber-awareness programmes, while CERT-In issues guidance on AI-related threats, including deepfakes.¹⁸ etc.

IX. CONCLUSION

Deepfakes have become a serious challenge in the digital age because they can be used to manipulate a person's identity, invade privacy, spread false information, commit fraud and cause lasting personal and reputational harm. Indian law already provides several remedies through the Constitution, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and the IT Rules. The 2026 amendments relating to Synthetically Generated Information have further strengthened the regulatory approach towards AI-generated content. However, technology is developing much faster than traditional legal mechanisms, making detection, attribution and enforcement difficult. Dealing with deepfakes therefore requires not only stronger laws but also responsible platforms, effective investigation, technological safeguards and greater public awareness.

X. SUGGESTIONS

- **IMPROVE DETECTION:** Investment should be made in reliable and regularly updated tools for detecting AI-generated and manipulated content.
- **PROVIDE QUICK REMEDIES:** Victims should have simple and speedy procedures for reporting and removing harmful deepfakes, especially intimate or impersonating content.

¹⁸ Ministry of Electronics & IT, Gov't of India, *Government Strengthens Regulatory Framework to Address AI-Generated Deepfakes* (Sep.21, 2026, 4:26 PM) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2295500®=48&lang=2>.

- **CLARIFY THE LAW:** India should develop adequate legal provisions for serious deepfake-related offences while protecting legitimate speech, satire, journalism and creativity.
- **INCREASE PLATFORM RESPONSIBILITY:** Online platforms should strengthen systems for detection, labelling, reporting and removal of unlawful synthetic content.
- **SUPPORT VICTIMS:** Victims should have access to legal assistance, privacy protection and appropriate support services.
- **PROMOTE DIGITAL AWARENESS:** Public education should encourage users to verify suspicious images, videos and audio before sharing them.
- **STRENGTHEN COOPERATION:** Law-enforcement agencies, technology companies and governments should cooperate, particularly in cases involving cross-border circulation of deepfakes.
- **KEEP LAWS UPDATED:** Legal and regulatory frameworks should be reviewed regularly so that they remain effective as AI technology continues to evolve.