

International Journal Research Publication Analysis

Page: 01-10

DEEPFAKES AND CYBER CRIMES IN INDIA: LEGAL CHALLENGES AND REMEDIES

***Mahima Sagar Chaudhri**

LL.B. Cyber Law / Criminal Law / Technology Law.

Article Received: 01 August 2026

*Corresponding Author: Mahima Sagar Chaudhri

Article Revised: 21 August 2026

LL.B. Cyber Law / Criminal Law / Technology Law.

Published on: 11 September 2026

DOI: <https://doi-doi.org/101555/ijrpa.4503>

ABSTRACT

The rapid development of Artificial Intelligence (AI) and machine-learning technologies has resulted in the emergence of deepfakes, which are digitally manipulated audio, video, images or other forms of media that can realistically imitate or replace the identity, appearance or voice of an individual. Although such technology may have legitimate applications in entertainment, education and creative industries, its malicious use has created serious legal and social concerns. Deepfakes may be used for identity theft, financial fraud, impersonation, defamation, misinformation, sexual exploitation, harassment and manipulation of electronic evidence.

In India, there is presently no single comprehensive legislation specifically dedicated to deepfakes. Instead, different aspects of deepfake-related conduct may be addressed through existing provisions of the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023 and rules governing intermediaries. The legal framework therefore faces difficulties relating to identification of offenders, attribution, jurisdiction, preservation of digital evidence, intermediary responsibility and protection of victims.

This paper examines the nature of deepfakes, their relationship with cyber crimes, the existing Indian legal framework and the major challenges faced by law-enforcement agencies and courts. It also proposes legal and technological remedies including stronger intermediary accountability, rapid takedown mechanisms, digital watermarking, public awareness, specialised investigation mechanisms and clearer legislative provisions.

KEYWORDS: Deepfake, Artificial Intelligence, Cyber Crime, Cyber Law, Digital Evidence, Identity Theft, Online Harassment, India.

1. INTRODUCTION

Artificial Intelligence has transformed the way digital content is created, modified and distributed. One of the most significant developments in this field is the emergence of deepfake technology. Deepfakes are synthetic or manipulated digital content created with the assistance of artificial intelligence and machine-learning techniques. They can make an individual appear to say or do something that the person never actually said or did.

The increasing availability of AI-based tools has made sophisticated digital manipulation accessible to ordinary users. As a result, deepfake technology has moved beyond entertainment and experimentation and has become a potential instrument for cyber criminals.

Deepfakes can be misused to impersonate individuals, manipulate photographs and videos, conduct financial scams, spread false information, damage reputations and create non-consensual sexually explicit content. The harm becomes particularly serious when the victim is a woman, child, public figure or professional whose reputation is essential to their personal or professional life.

The legal challenge is that deepfake technology develops much faster than legislation. Existing laws may apply to particular consequences of a deepfake, but they do not necessarily address every aspect of the creation, distribution and amplification of synthetic content.

Therefore, there is a need to examine whether India's existing cyber and criminal laws are sufficient to address deepfake-related offences and what additional legal and technological measures may be required.

2. Objectives of the Study

The major objectives of this research are:

1. To understand the concept and nature of deepfake technology.
2. To examine the relationship between deepfakes and cyber crimes.
3. To analyse the existing Indian legal framework applicable to deepfake-related offences.
4. To identify the difficulties faced by victims and law-enforcement agencies.
5. To examine issues concerning digital evidence and attribution of cyber offenders.

6. To analyse the responsibility of online intermediaries and digital platforms.
7. To suggest effective legal, technological and institutional remedies.

3. Research Questions

This study seeks to answer the following questions:

1. What are deepfakes and how can they be used to commit cyber crimes?
2. Is the existing Indian legal framework sufficient to deal with deepfake-related offences?
3. What provisions of Indian cyber and criminal law can be applied to malicious deepfakes?
4. What challenges arise in identifying and prosecuting perpetrators?
5. What legal and technological remedies can effectively protect victims?

4. Research Methodology

The present research follows a doctrinal research methodology. The study is primarily based on secondary sources, including statutes, government materials, judicial decisions, research articles, books, reports and reliable online legal resources.

The principal legislation examined includes the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023.

The study adopts an analytical approach to understand the existing legal framework and identify gaps in relation to deepfake-related cyber crimes.

5. Understanding Deepfakes

The term "deepfake" is derived from deep learning and fake content. Deep learning is a branch of artificial intelligence that enables computer systems to learn patterns from large quantities of data.

Deepfake technology can be used to manipulate:

- photographs;
- videos;
- audio recordings;
- facial expressions;
- voices; and
- other forms of digital media.

For example, a person's face may be digitally inserted into another person's video, or artificial intelligence may be used to imitate a person's voice. The resulting content may appear authentic to an ordinary viewer.

The primary concern is not merely the existence of manipulated content but its malicious use. When a deepfake is created and distributed with the intention of deceiving, exploiting, threatening or harming another person, it may become connected with one or more existing criminal offences.

6. Deepfakes as a Tool for Cyber Crime

Deepfake technology can facilitate several forms of cyber crime.

6.1 Identity Theft and Impersonation

A criminal may use another person's photograph, video or voice to create an artificial identity. Such identity can then be used for fraudulent communications, financial scams or social-media impersonation.

The Information Technology Act, 2000 contains provisions dealing with identity theft and cheating by personation using computer resources. Sections 66C and 66D are therefore particularly relevant to certain deepfake-based activities.

6.2 Financial Fraud

AI-generated voice or video can be used to impersonate a family member, employer, company executive or other trusted person. A victim may consequently be persuaded to transfer money or disclose confidential information.

Where the conduct involves deception and dishonest inducement, relevant criminal provisions may become applicable.

6.3 Sexual Exploitation

One of the most harmful applications of deepfakes is the creation of non-consensual sexually explicit material. A person's face may be digitally placed on sexually explicit content without their consent.

The Information Technology Act contains provisions relating to publication or transmission of obscene and sexually explicit material in electronic form.

Where children are involved, the legal consequences become significantly more serious.

6.4 Defamation and Reputation Damage

A fabricated video may falsely depict an individual making offensive, illegal or immoral statements. If widely circulated, such content can seriously damage the person's reputation.

Deepfakes therefore create a difficult intersection between technology, freedom of expression, privacy and protection of reputation.

6.5 Misinformation and Public Manipulation

Deepfakes may also be used to create false statements attributed to politicians, public officials, celebrities or other public figures. During elections or public emergencies, such content may influence public opinion and create social unrest.

7. Existing Legal Framework in India

India does not currently have one comprehensive statute exclusively dealing with deepfakes. Instead, different laws may apply depending upon the nature and consequences of the conduct.

7.1 Information Technology Act, 2000

The Information Technology Act, 2000 remains an important statute for addressing cyber offences. It contains provisions concerning identity theft, cheating by personation through computer resources, violation of privacy and publication or transmission of certain categories of unlawful electronic material.

Section 66C deals with punishment for identity theft, while Section 66D deals with cheating by personation using a computer resource. Section 66E addresses violation of privacy. Sections 67, 67A and 67B deal with specified categories of unlawful electronic content.

These provisions may be relevant where a deepfake is used as an instrument for committing an underlying offence.

However, the provisions were not drafted specifically for modern generative-AI technology. Consequently, their application may depend upon the facts and the nature of the harmful conduct.

7.2 Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 replaced the Indian Penal Code framework from 1 July 2024. It contains provisions that can be relevant to deepfake-related conduct.

Section 319 deals with cheating by personation, including pretending to be another person or representing another person as someone they are not.

The BNS also addresses forged documents or electronic records. Section 340 deals with forged documents or electronic records and their use as genuine.

These provisions demonstrate that existing criminal law can address some forms of harmful synthetic media, particularly where the deepfake involves impersonation, deception or fraudulent use of an electronic record.

Nevertheless, deepfake technology presents new factual situations that may not fit neatly within traditional concepts of forgery or personation.

7.3 Bharatiya Sakshya Adhiniyam, 2023

Digital evidence is central to deepfake investigations. The Bharatiya Sakshya Adhiniyam, 2023 contains specific provisions concerning electronic or digital records, including their admissibility and proof. Sections 61, 62 and 63 are particularly relevant to electronic evidence.

This is important because a deepfake case may involve questions such as:

- Is the video authentic?
- Who created it?
- Has the original file been altered?
- Where was it first uploaded?
- Can metadata establish its origin?
- Can forensic examination establish manipulation?

Therefore, proper collection and preservation of electronic evidence is essential.

8. Major Legal Challenges

8.1 Absence of a Specific Deepfake Law

The absence of a dedicated deepfake offence creates uncertainty. Existing laws can address particular forms of harm, but they do not create a unified legal framework covering the creation, manipulation, distribution and intentional amplification of harmful synthetic media.

8.2 Difficulty in Identifying the Perpetrator

Cyber criminals can use anonymous accounts, fake identities, encrypted services and foreign platforms. The person who creates the deepfake may be different from the person who initially uploads it or the users who subsequently distribute it.

This creates difficulties in establishing individual criminal responsibility.

8.3 Cross-Border Jurisdiction

A deepfake may be created in one country, uploaded through a server in another country and distributed to victims in India.

The BNS contains provisions dealing with offences committed outside India, including offences targeting a computer resource located in India.

However, practical investigation and enforcement across jurisdictions remain difficult.

8.4 Digital Evidence

Deepfake cases heavily depend upon electronic evidence. However, synthetic media can be extremely difficult to distinguish from authentic content.

Courts may therefore require reliable technical and forensic evidence before determining whether a particular recording has been manipulated.

8.5 Victim Identification and Reporting

Victims may hesitate to report deepfake-related offences because of social stigma, fear of humiliation or concern about further circulation of the content.

In cases involving intimate or sexually explicit deepfakes, the harm may continue even after the original content is removed because copies may already have been downloaded and redistributed.

8.6 Balancing Regulation and Freedom of Expression

Not every manipulated or AI-generated image is unlawful. Satire, parody, artistic expression, education and entertainment may involve altered media.

Therefore, regulation must distinguish between legitimate synthetic content and content created or distributed with unlawful intent or harmful consequences.

9. Remedies and Preventive Measures

9.1 Specific Legislative Framework

India should consider developing a clearer legal framework specifically addressing malicious deepfakes. The law should define deepfake or synthetic media and identify prohibited conduct such as malicious impersonation, non-consensual intimate deepfakes, fraudulent use and deliberate dissemination of harmful synthetic content.

9.2 Stronger Platform Responsibility

Social-media platforms and other intermediaries should establish effective mechanisms for reporting and removing harmful deepfake content.

Platforms should maintain transparent procedures for:

- receiving complaints;
- verifying reported content;
- preserving relevant evidence;
- removing unlawful material;
- preventing repeated uploads; and
- informing affected users about available remedies.

9.3 Technological Detection

Technology should be used alongside law. AI-based detection systems, digital watermarking and provenance technologies can assist in identifying synthetic content.

However, detection tools should not be treated as infallible. Human review and forensic examination may still be necessary.

9.4 Digital Forensics

Cyber-crime units should receive specialised training in AI-generated content and digital forensics. Investigators should be capable of examining metadata, source files, device

information, platform records and other digital traces.

9.5 Victim-Centred Remedies

Victims should have simple and accessible mechanisms for reporting harmful content. In sensitive cases, authorities should prioritise confidentiality and prevent unnecessary exposure of the victim.

9.6 Public Awareness

Digital literacy should include awareness of AI-generated misinformation. Individuals should be encouraged to verify suspicious videos, images and audio before sharing them.

Schools, colleges and universities can play an important role in developing responsible digital behaviour.

10. Role of Courts and Law-Enforcement Agencies

Courts will increasingly encounter cases where the authenticity of digital material is disputed. Judicial officers may therefore require assistance from qualified forensic experts.

Law-enforcement agencies should develop specialised cyber-crime teams capable of handling AI-generated content. Cooperation between police, forensic laboratories, technology companies and legal professionals is necessary.

The investigation should focus not only on the visible content but also on its source, creation process, distribution chain and associated digital evidence.

11. Suggestions

The following measures may strengthen India's response to deepfake-related cyber crimes:

1. Enact clear legal provisions specifically addressing malicious deepfakes.
2. Establish a uniform definition of deepfake or harmful synthetic media.
3. Introduce faster complaint and takedown mechanisms for victims.
4. Strengthen cyber-forensic infrastructure.
5. Train police officers and judicial officers in AI-related crimes.
6. Encourage digital watermarking and content-provenance systems.
7. Establish stronger cooperation between Indian authorities and international platforms.
8. Create awareness programmes regarding AI-generated misinformation.
9. Provide special protection and speedy remedies to victims of non-consensual intimate

deepfakes.

10. Ensure that regulation does not unnecessarily restrict legitimate satire, art, research or free expression.

12. CONCLUSION

Deepfake technology represents one of the most significant emerging challenges in the field of cyber law. While artificial intelligence provides considerable benefits to society, its misuse can facilitate identity theft, fraud, harassment, sexual exploitation, misinformation and reputational harm.

India's existing legal framework provides several provisions that can potentially address different forms of deepfake-related conduct. The Information Technology Act addresses identity theft, personation, privacy violations and unlawful electronic content, while the Bharatiya Nyaya Sanhita contains provisions concerning personation and forged electronic records. The Bharatiya Sakshya Adhiniyam provides a framework for electronic and digital evidence.

However, the fragmented nature of these provisions creates challenges when dealing with sophisticated AI-generated content. The law must therefore evolve alongside technology.

A comprehensive response should not depend solely upon criminal punishment. It should combine legislation, digital forensics, intermediary responsibility, technological detection, victim protection and public awareness.

Ultimately, the objective should be to ensure that technological innovation remains beneficial to society while preventing artificial intelligence from becoming an instrument of deception, exploitation and cyber crime.

REFERENCES

1. Information Technology Act, 2000, India Code, Government of India.
2. Bharatiya Nyaya Sanhita, 2023, India Code, Government of India.
3. Bharatiya Sakshya Adhiniyam, 2023, India Code, Government of India.
4. Bharatiya Nagarik Suraksha Sanhita, 2023, India Code, Government of India.
5. Ministry of Electronics and Information Technology, Government of India, materials concerning intermediary regulation and online safety.
6. Research literature concerning Artificial Intelligence, synthetic media, deepfakes and cyber crime.