

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 3
2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any **suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Deepfake Crimes in India: Issues and Challenges

DR. SUDARSHAN NIMMA*

ABSTRACT

This paper examines the legal challenges posed by deepfake crimes in India. Artificial intelligence has transformed digital communication and content creation, and one of its most controversial applications is deepfake technology, which enables the creation of highly realistic but fabricated audio, video, and image content. While deepfakes have legitimate uses in entertainment, education, and research, they have increasingly become instruments of cybercrime, identity theft, online fraud, non-consensual intimate imagery, political misinformation, and reputational harm. India presently lacks dedicated legislation governing deepfake crimes, compelling law enforcement agencies and courts to rely on the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, and the Bharatiya Sakshya Adhiniyam, 2023 for prosecution and evidentiary assessment. This paper critically examines the nature of deepfake crimes, the criminal liability of accused persons, the admissibility of artificial-intelligence-generated evidence, the constitutional implications, and the challenges confronting investigators and courts in addressing this emerging technological threat.

Keywords: Deepfake, Artificial Intelligence, Bharatiya Nyaya Sanhita, Digital Evidence, Cyber Forensics, Privacy, Criminal Liability, Bharatiya Sakshya Adhiniyam.

I. INTRODUCTION

The rapid progress of artificial intelligence has transformed the manner in which information is created, stored, and disseminated. Among the most significant technological innovations of recent years is deepfake technology, which uses machine-learning algorithms and neural networks to create synthetic media capable of imitating the appearance, voice, and actions of real individuals. The term "deepfake" is derived from the combination of "deep learning" and "fake," reflecting the use of sophisticated artificial-intelligence models to produce realistic, artificially created content.¹

* Author is an Associate Professor at Department of Law, Kakatiya University, Telangana, India.

¹ Mika Westerlund, The Emergence of Deepfake Technology: A Review, 9 TECH. INNOVATION MGMT. REV. 39, 40 (2019).

Deepfake technology was initially developed for research and entertainment purposes. Over time, however, it has gradually evolved into a tool for criminal activity that is now rampant. The creation of false videos depicting public figures making defamatory statements, artificial-intelligence-generated voice clones used in financial fraud, and the manipulation of intimate images, which mostly targets vulnerable women, raises serious concerns regarding privacy and dignity. Such artificial fabrication poses unprecedented challenges to legal systems across the globe.²

In India, the increasing accessibility of generative artificial-intelligence platforms has heightened the risk of misuse. The absence of a specific statutory framework regulating deepfakes has created uncertainty regarding criminal liability, evidentiary standards, and victim protection. Consequently, existing criminal laws must be interpreted and applied to address offences committed through synthetic media.

II. THE CONCEPT OF DEEPPFAKE TECHNOLOGY

Deepfake technology refers to artificial-intelligence-generated synthetic media in which an individual's likeness, voice, or actions are manipulated to create a realistic but false representation. The technology primarily relies upon Generative Adversarial Networks (GANs), a machine-learning framework that enables computers to generate highly convincing digital content.³ Deepfakes now take different forms, including manipulated videos, cloned voices, fabricated photographs, and hybrid multimedia content. While some applications serve legitimate and lawful purposes, such as film production and educational simulations, criminals use deepfakes to deceive and exploit innocent victims, influence public opinion, perpetrate financial fraud, and spread false information.⁴

The increasing sophistication of artificial-intelligence tools has drastically reduced the technical expertise required to produce deepfakes, thereby expanding the scope for their misuse. As a result, legal systems are confronted with the difficult task of regulating a technology that evolves faster than legislative responses can address.

² Robert Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1758 (2019).

³ Ian Goodfellow et al., *Generative Adversarial Networks*, 27 ADVANCES IN NEURAL INFO. PROCESSING SYS. 2672 (2014).

⁴ Chesney & Citron, *supra* note 2, at 1769.

III. CRIMINAL LIABILITY UNDER THE BHARATIYA NYAYA SANHITA, 2023

Although the Bharatiya Nyaya Sanhita, 2023 does not expressly define "deepfake crimes," several of its provisions can be effectively invoked depending upon the nature of the offender's conduct.

A. Cheating and personation

Where a deepfake is used to induce a victim to transfer money, disclose confidential information, or act under false pretences, the accused may incur liability for cheating and personation.⁵ Artificial-intelligence-generated voice cloning has increasingly been employed in financial scams in which offenders impersonate family members, corporate executives, or government officials. The essential elements of deception, dishonest intention, and wrongful gain remain applicable regardless of whether the fraudulent representation is made physically or through artificial-intelligence-generated media.

B. Forgery and fabrication of electronic records

Deepfakes often involve the manipulation of electronic records and digital content. Where fabricated videos, images, or documents are created with the intention of causing damage, supporting false claims, or misleading authorities, criminal liability may arise under the provisions relating to forgery and the falsification of electronic records.⁶

C. Defamation

The circulation of manipulated videos portraying an individual engaging in unlawful or immoral conduct may seriously damage personal and professional reputation. Deepfakes targeting celebrities, politicians, journalists, and private citizens may attract both criminal and civil liability for the offence of defamation.⁷

D. Extortion and criminal intimidation

Deepfake content is increasingly used as a means of blackmail and coercion. Criminals may create artificially fabricated compromising videos and threaten their publication unless money or favours are provided. Such conduct would amount to criminal intimidation and extortion under the Bharatiya Nyaya Sanhita, 2023.⁸

⁵ The Bharatiya Nyaya Sanhita, 2023, § 318, No. 45, Acts of Parliament, 2023 (India).

⁶ The Bharatiya Nyaya Sanhita, 2023, § 336, No. 45, Acts of Parliament, 2023 (India).

⁷ The Bharatiya Nyaya Sanhita, 2023, § 356, No. 45, Acts of Parliament, 2023 (India).

⁸ The Bharatiya Nyaya Sanhita, 2023, §§ 308, 351, No. 45, Acts of Parliament, 2023 (India).

E. Women as a targeted group

One of the most alarming applications of deepfake technology is the creation of non-consensual sexually explicit content. Women are disproportionately targeted through artificial-intelligence-generated pornography and manipulated intimate imagery. Such acts violate their dignity, privacy, and bodily autonomy. These acts attract liability under the provisions dealing with obscenity, sexual harassment, and outraging the modesty of a woman.

IV. CRIMINAL LIABILITY UNDER THE INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000 continues to play a significant role in regulating cybercrimes involving deepfakes. Section 66C criminalises identity theft, which involves the fraudulent use of another person's digital identity, and artificial-intelligence-generated impersonation frequently falls within its ambit. Section 66D penalises cheating by personation through computer resources and may apply where deepfakes facilitate financial fraud.⁹

Similarly, Sections 67 and 67A prohibit the publication and transmission of obscene and sexually explicit material in electronic form. These provisions become particularly relevant where deepfake pornography is disseminated online, while Section 66E penalises the capturing and transmission of images of a person's private area in violation of privacy.¹⁰ The Act therefore provides an important supplementary framework for prosecuting deepfake-related misconduct, notwithstanding the absence of a dedicated deepfake statute.

V. ISSUES AND CHALLENGES

A. Evidentiary challenges

The emergence of deepfakes presents profound challenges for evidentiary law. Traditionally, photographs, audio recordings, and videos have been regarded as reliable forms of evidence. However, artificial-intelligence-generated content has significantly undermined this assumption.

The Bharatiya Sakshya Adhiniyam, 2023 recognises electronic records as admissible evidence subject to prescribed conditions. Nevertheless, courts must increasingly determine whether the digital content presented before them is authentic or artificially manipulated.¹¹

Cyber-forensic experts consequently assume a critical role in criminal proceedings. Their expertise is required to identify metadata inconsistencies, detect algorithmic manipulation,

⁹ The Information Technology Act, 2000, §§ 66C, 66D, No. 21, Acts of Parliament, 2000 (India).

¹⁰ The Information Technology Act, 2000, §§ 66E, 67, 67A, No. 21, Acts of Parliament, 2000 (India).

¹¹ The Bharatiya Sakshya Adhiniyam, 2023, §§ 61, 63, No. 47, Acts of Parliament, 2023 (India).

verify the chain of custody, and authenticate digital evidence. Without robust forensic verification mechanisms, courts risk relying upon fabricated evidence or rejecting genuine evidence on account of uncertainty.

B. Infringement of constitutionally guaranteed rights

Deepfake technology violates some of the most significant fundamental constitutional rights, which include the following.

C. Right to privacy

In *K.S. Puttaswamy v. Union of India*, the Supreme Court of India recognised privacy as an intrinsic component of Article 21 of the Constitution.¹² Deepfake pornography, unauthorised voice cloning, and synthetic impersonation directly violate informational privacy and personal autonomy.

D. Right to reputation

The Supreme Court has repeatedly recognised reputation as an essential component of the right to life and dignity under Article 21.¹³ Deepfakes can irreparably damage the reputation of individuals by spreading false and misleading representations.

E. Right to freedom of speech and expression

Efforts to regulate deepfakes must also respect the constitutional guarantee of free speech under Article 19(1)(a).¹⁴ Excessive restrictions may impede legitimate artistic, journalistic, and educational uses of artificial-intelligence-generated content. Legislators therefore face the difficult task of balancing innovation and freedom with accountability and victim protection.

F. Challenges in prosecuting deepfake crimes

Notwithstanding the legal provisions discussed above, several significant challenges continue to impede effective prosecution.

The first challenge is the absence of a comprehensive statutory definition of deepfakes. The existing provisions were drafted before the emergence of generative artificial intelligence and do not adequately address the unique nature of synthetic media.

¹² Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

¹³ Subramanian Swamy v. Union of India, (2016) 7 SCC 221 (India).

¹⁴ INDIA CONST. art. 19, cl. 1(a).

Secondly, offenders often operate anonymously, using encrypted networks and virtual private networks routed through foreign servers. Identifying the original creator of deepfake content is therefore a difficult task that frequently necessitates international cooperation.

Thirdly, deepfakes spread rapidly across social-media platforms. Even where the content is subsequently removed, the damage to reputation and privacy may by then be irreversible.

Fourthly, India faces a severe shortage of trained cyber-forensic experts with the capacity to detect sophisticated artificial-intelligence-generated content. The growing complexity of deepfake technology demands continuous technological upgrades and specialised training.

India must adopt a comprehensive legislative framework specifically addressing deepfake crimes. Such legislation should clearly define deepfakes, prescribe graded penalties based on the severity of the harm, and establish mandatory obligations for digital intermediaries.

VI. CONCLUSION

Deepfake technology represents one of the most significant challenges confronting contemporary criminal-justice systems. While the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, and the Bharatiya Sakshya Adhiniyam, 2023 provide certain mechanisms for addressing deepfake-related misconduct, they do not comprehensively regulate the unique risks posed by synthetic media. The increasing sophistication of artificial-intelligence-generated content threatens privacy, reputation, democratic institutions, and the integrity of judicial proceedings. A combination of legislative reform, cyber-forensic innovation, institutional capacity building, and international cooperation is therefore necessary to ensure that technological advancement does not undermine the rule of law.

The Government should establish specialised artificial-intelligence forensic laboratories capable of detecting synthetic media and assisting investigative agencies. Mandatory watermarking and provenance-tracking mechanisms for artificial-intelligence-generated content should also be considered. Training programmes for judges, prosecutors, police officers, and forensic experts are essential to ensure effective enforcement. Furthermore, large-scale international cooperation is necessary because deepfake offences are, in most cases, cross-border offences. Public-awareness initiatives should be conducted to educate citizens about the dangers of artificial-intelligence-generated misinformation and to inform them of methods for identifying manipulated content.

VII. BIBLIOGRAPHY

1. The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).

2. The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India).
3. The Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
4. The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
5. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
6. Apar Gupta & Smriti Parsheera, Privacy and Technology in India, 12 INDIAN J.L. & TECH. 1 (2016).
7. Robert Chesney & Danielle Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 CALIF. L. REV. 1753 (2019).
8. Ian Goodfellow et al., Generative Adversarial Networks, 27 ADVANCES IN NEURAL INFO. PROCESSING SYS. 2672 (2014).
9. Mika Westerlund, The Emergence of Deepfake Technology: A Review, 9 TECH. INNOVATION MGMT. REV. 39 (2019).
10. NANDAN KAMATH, LAW RELATING TO COMPUTERS, INTERNET AND E-COMMERCE (Universal Law Publishing).
11. N.V. PARANJAPE, CRIMINOLOGY AND PENOLOGY (Central Law Publications).
12. BILL NELSON, AMELIA PHILLIPS & CHRISTOPHER STEUART, GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS (Cengage Learning).
13. TALAT FATIMA, CYBER LAW IN INDIA (Eastern Book Company).
