

DEEPPAKES AND INDIAN LAW: IS THE CURRENT LEGAL FRAMEWORK ENOUGH?

By Author¹

INTRODUCTION

Artificial Intelligence (AI) has rapidly transformed the digital landscape, making content creation faster, more accessible, and increasingly sophisticated. Among its most controversial developments is the emergence of deepfakes—AI-generated videos, images, or audio recordings that convincingly imitate a person's appearance or voice. Although the technology has legitimate applications in filmmaking, education, accessibility, and entertainment, its misuse has created significant legal and ethical concerns.²

The increasing availability of AI tools has enabled individuals to create highly realistic fake content with minimal technical knowledge. Deepfakes have been used for identity theft, financial fraud, political misinformation, cyberbullying, revenge pornography, and defamation. Such misuse not only harms individuals but also undermines public trust in digital information. In India, the circulation of manipulated videos involving public figures and private individuals has highlighted the limitations of the current legal framework in addressing AI-generated deception.³

Unlike several emerging technologies, deepfakes are not regulated by a dedicated statute in India. Instead, existing legal remedies are scattered across different laws, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 (BNS), and the Digital Personal Data Protection Act, 2023 (DPDP Act). While these laws provide certain protections, they were not enacted specifically to deal with synthetic media generated by artificial intelligence. Consequently, important legal gaps remain regarding prevention, detection, and victim protection.

This article examines the concept of deepfakes, analyses the existing legal framework governing their misuse in India, identifies the shortcomings of the current legal regime, and suggests

¹ Udaynidhi Ramakrishnan

² Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107(6) California Law Review 1753.

³ Ministry of Electronics and Information Technology, 'MeitY Issues Advisory to All Intermediaries to Comply with Existing IT Rules' (Press Information Bureau, 26 December 2023) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1990542> accessed 21 July 2026.

reforms that can balance technological innovation with the protection of privacy, dignity, and public trust.

Understanding Deepfakes

The term deepfake combines the words deep learning and fake. Deep learning is a branch of artificial intelligence that enables computers to learn patterns from vast amounts of data. By analysing thousands of photographs, videos, or voice recordings, AI systems can generate realistic content that closely resembles an existing individual.⁴

Initially, deepfake technology was developed for research and creative purposes. Today, it is widely used in cinema for visual effects, language dubbing, digital restoration of historical footage, and educational simulations. However, the same technology has also become a powerful tool for malicious activities. Criminals have used deepfakes to impersonate business executives during financial transactions, create non-consensual intimate images, spread false political information, and deceive the public through fabricated news reports. These incidents demonstrate that the primary concern is not the technology itself but its misuse.⁵

The rapid advancement of generative AI has made deepfake software affordable and easily accessible. As a result, distinguishing authentic content from manipulated media has become increasingly difficult. This creates challenges for law enforcement agencies, courts, digital platforms, and ordinary citizens, all of whom must determine the authenticity of digital evidence in an increasingly AI-driven environment.⁶

EXISTING INDIAN LEGAL FRAMEWORK

Although India does not have a dedicated law specifically regulating deepfakes, several existing statutes provide remedies against their misuse. The primary legal framework consists of the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 (BNS), and the Digital Personal Data Protection Act, 2023 (DPDP Act).⁷

⁴ Chesney and Citron (n 1) 1755.

⁵ Chesney and Citron (n 1) 1758.

⁶ Ministry of Electronics and Information Technology (n 2).

⁷ Information Technology Act 2000; Bharatiya Nyaya Sanhita 2023; Digital Personal Data Protection Act 2023.

The Information Technology Act, 2000 is India's principal cyber law. It addresses offences such as identity theft, cheating by personation using computer resources, and the publication or transmission of obscene material in electronic form. Where a deepfake is created to impersonate another person, commit fraud, or circulate obscene content, the relevant provisions of the Act may be invoked.⁸

The Bharatiya Nyaya Sanhita, 2023 also provides legal remedies where deepfakes are used for criminal purposes. Depending on the nature of the offence, provisions relating to cheating, defamation, forgery, criminal intimidation, or offences affecting reputation may become applicable. Although the legislation does not specifically refer to artificial intelligence, its provisions are broad enough to address many harmful consequences arising from the misuse of deepfake technology.⁹

The Digital Personal Data Protection Act, 2023 represents another important development in India's digital governance framework. Since many deepfakes are created using photographs, videos, or voice recordings of identifiable individuals, the unauthorized processing of such personal data may attract obligations and liabilities under the Act.¹⁰

Despite these legal protections, India's current framework remains fragmented. None of these statutes specifically defines "deepfake" or establishes a comprehensive regulatory mechanism for AI-generated synthetic media. As a result, enforcement agencies often rely on general legal provisions that were enacted before the emergence of advanced generative AI technologies.

CHALLENGES AND THE WAY FORWARD

One of the greatest challenges posed by deepfakes is the speed at which manipulated content spreads through social media platforms. Once a deepfake becomes viral, the resulting damage to

⁸ Information Technology Act 2000, ss 66C, 66D and 67.

⁹ Bharatiya Nyaya Sanhita 2023.

¹⁰ Digital Personal Data Protection Act 2023, ss 4 and 5.

an individual's reputation, privacy, or public confidence may be difficult to reverse, even if the content is subsequently removed.¹¹

To address these concerns, India should consider introducing dedicated legislation governing AI-generated synthetic media. Such legislation should clearly define deepfakes, distinguish legitimate uses from malicious misuse, impose proportionate penalties, and establish obligations for digital platforms to remove harmful content promptly. Greater public awareness, investment in AI-detection technologies, and specialized training for law enforcement agencies would also strengthen the country's ability to combat deepfake-related offences.

CONCLUSION

Artificial intelligence has created remarkable opportunities for innovation, but it has also introduced new legal challenges that existing laws were not designed to address. While the Information Technology Act, the Bharatiya Nyaya Sanhita, and the Digital Personal Data Protection Act provide partial remedies, they do not comprehensively regulate deepfakes. India must therefore adopt a balanced legal framework that promotes technological development while protecting privacy, dignity, and public trust. A combination of targeted legislation, effective enforcement, responsible platform governance, and public awareness will be essential to ensure that artificial intelligence is used ethically and responsibly.

¹¹ Ministry of Electronics and Information Technology, 'MeitY Issues Advisory to All Intermediaries to Comply with Existing IT Rules' (Press Information Bureau, 26 December 2023) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1990542> accessed 21 July 2026.