



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

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.

DEEPPAKES AND INDIAN LAWS: IS INDIA READY FOR THE NEXT DIGITAL THREAT?

- PRAKRITI TYAGI

INTRODUCTION

Artificial Intelligence has transformed the way people communicate, create content, and interact in the digital world. From virtual assistants to AI-generated art and automated customer services, technological innovation has made life more efficient than ever before. However, the same technology has also given rise to one of the most alarming digital threats of the modern era of deepfakes. Deepfakes are AI-generated or AI-manipulated images, videos, or audio recordings that imitate a person's appearance, voice, or expressions so convincingly that they often appear genuine. While this technology has legitimate applications in filmmaking, education, accessibility, and entertainment, its misuse has created serious legal, ethical, and cybersecurity concerns.

In recent years, India has witnessed a rapid increase in deepfake-related incidents involving celebrities, politicians, journalists, and ordinary citizens. The viral deepfake video of actress Rashmika Mandanna in 2023 highlighted the dangers of AI-generated content and sparked nationwide discussions on digital safety and legal accountability. Such incidents demonstrate that deepfakes are no longer merely a technological innovation but a growing threat to privacy, reputation, democracy, and public trust. Although India has introduced new data protection legislation and strengthened cyber laws, the absence of a dedicated legal framework specifically regulating deepfakes continues to create significant challenges.

UNDERSTANDING DEEPPAKES AND THEIR WORKING

The term "deepfake" combines the words "deep learning" and "fake." It refers to synthetic media generated using advanced artificial intelligence techniques, particularly deep learning algorithms and Generative Adversarial Networks (GANs). In simple terms, the technology studies thousands of photographs, videos, and voice samples of an individual to recreate realistic facial expressions, lip movements, and speech patterns. As a result, a fabricated video or audio clip can appear almost indistinguishable from authentic content. Deepfake technology itself is not inherently unlawful. It is

increasingly used in cinema, gaming, language translation, education, medical training, and digital accessibility. However, the same technology becomes dangerous when it is used without consent to deceive the public, spread misinformation, commit financial fraud, impersonate individuals, or create non-consensual explicit content.

IMPACT OF DEEPPAKES ON SOCIETY

The misuse of deepfake technology has significant social, legal, and economic consequences. One of the most serious concerns is misinformation and fake news. Manipulated videos can influence public opinion, disrupt elections, incite communal tensions, and damage democratic institutions. In the age of social media, false information spreads rapidly, making it difficult to distinguish truth from fabrication.

Deepfakes also facilitate identity theft and impersonation. Criminals may clone an individual's voice or face to deceive family members, financial institutions, or employers into transferring money or disclosing confidential information. Another disturbing consequence is the rise of non-consensual explicit content, particularly targeting women. AI-generated intimate images or videos can cause severe psychological trauma, reputational damage, and long-term emotional distress despite being entirely fabricated.

EXISTING INDIAN LEGAL FRAMEWORK

India presently does not have a standalone law specifically regulating deepfakes. Nevertheless, several existing statutes provide partial protection against their misuse. The Information Technology Act, 2000 remains the primary legislation governing cyber offences. Various provisions address identity theft, cheating through computer resources, violation of privacy, and publication or transmission of obscene material in electronic form. Intermediaries are also expected to exercise due diligence while responding to unlawful online content.

The Digital Personal Data Protection Act, 2023 represents a significant step toward protecting individuals' personal data. Since deepfakes frequently involve unauthorized collection and processing of personal images, videos, and voice recordings, the Act reinforces the importance of lawful consent and responsible data processing. The Bharatiya Nyaya Sanhita, 2023 also becomes relevant where deepfakes involve cheating, forgery, personation, criminal intimidation, defamation, or publication of obscene material. Depending upon the facts, perpetrators may incur both civil and criminal liability. Further protection is available under the Copyright Act, 1957, the Trade Marks Act, 1999, and the common law doctrine of personality rights. Moreover, the constitutional right to privacy recognised under Article 21 provides an important safeguard against unauthorized digital exploitation.

JUDICIAL DEVELOPMENTS AND RECENT INCIDENTS

A significant judicial development is *Amitabh Bachchan v Rajat Nagi* ¹, where the Delhi High Court recognised the need to protect celebrity personality rights from unauthorized commercial exploitation. Although the case did not exclusively concern deepfakes, its reasoning has become increasingly relevant in addressing AI-generated impersonation and identity misuse. During 2025 and 2026, discussions surrounding AI governance intensified worldwide. Governments, technology companies, and regulators increasingly focused on watermarking AI-generated content, improving detection technologies, strengthening intermediary accountability, and developing ethical AI standards. India has also indicated its intention to encourage responsible AI innovation while ensuring that technological advancement does not compromise citizens' rights.

CHALLENGES IN ENFORCEMENT

Despite the availability of multiple legal provisions, enforcement remains difficult. First, India lacks a dedicated statute defining and regulating deepfakes. Existing laws apply only indirectly, resulting in legal uncertainty. Secondly, identifying the creators of deepfakes is technically challenging because such content may originate from anonymous accounts or foreign jurisdictions.

Thirdly, social media platforms often struggle to remove manipulated content before it spreads widely. Once viral, reputational damage becomes almost irreversible. Another challenge is the lack of public awareness. Many individuals remain unable to distinguish authentic media from AI-generated content, making them vulnerable to deception. Finally, lawmakers must carefully balance freedom of speech and technological innovation with the need to protect privacy, dignity, and public order.

CONCLUSION

Deepfake technology represents one of the most significant legal and technological challenges of the digital era. While its beneficial applications cannot be ignored, its misuse threatens privacy, democratic values, financial security, and public confidence in digital information. India has made important progress through the Digital Personal Data Protection Act, strengthened cyber governance, and judicial recognition of personality rights.

However, these measures remain insufficient to comprehensively regulate AI-generated deception. India possesses a strong constitutional foundation and several relevant statutory protections, but it still lacks a dedicated legal framework specifically addressing deepfakes. Future reforms should focus on AI-specific legislation, technical standards, rapid enforcement mechanisms and improved digital literacy.

1. Amitabh Bachchan v Rajat Nagi and others (2022) 6 H.C.C (Del) 641, 2022 SCC Online Del 4110