



# 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.

---

## Legal Aspects of Deepfake Technology in India: The Looming Threat to Privacy and Reputation

*Bhanushali Jignesh Arvind*

### **Introduction:**

In the era of artificial intelligence and rapid digital transformation, deepfake technology has emerged as a serious challenge to individual privacy, public trust, and information integrity. Deepfakes use AI to manipulate audio, video, and images in ways that make it nearly impossible to distinguish between real and fake content. While the innovation behind this technology is noteworthy, its misuse has led to serious legal, ethical, and social concerns - especially in India, where laws struggle to keep pace with technological disruption.

### **What are Deepfakes?**

Deepfakes are typically created using machine learning techniques like Generative Adversarial Networks (GANs) to manipulate media content. Deepfakes are synthetic media created using artificial intelligence, where a person's facial features, voice, or expressions are digitally altered to depict actions or statements they never actually made. Although originally developed for entertainment and innovation, deepfakes have been used maliciously to commit fraud, circulate revenge porn, impersonate public figures, and spread misinformation. What began as harmless experimentation has now escalated into a tool for defamation, misinformation, identity theft, and even blackmail.

### **Legal landscapes in India:**

At present, there is no specific legislation in India that directly governs the creation and dissemination of deepfake content. Still, some existing legal provisions provide only restricted means for seeking redress:

**1. Information Technology Act, 2000 (IT Act):**

Section 66E punishes violation of privacy through electronic means, while Section 67 penalizes publishing or transmitting obscene material online. These can apply if deepfakes are used to produce non-consensual content, particularly of a sexual nature<sup>1</sup>.

**2. Bharatiya Nyaya Sanhita, 2023 (BNS):**

Provisions such as Section 356 (Defamation), Section 77 (Voyeurism), and Section 336 (Forgery for harming reputation) may be invoked against deepfake misuse<sup>2</sup>.

**3. Copyright Act, 1957:**

The use of deepfakes can entail the unauthorized appropriation of an individual's voice or image, which may amount to a violation of copyright laws and moral rights<sup>3</sup>.

**Judicial Perspective:**

---

<sup>1</sup> Information Technology Act, No. 21 of 2000, INDIA CODE (2000), <[https://www.indiacode.nic.in/handle/123456789/1999?view\\_type=browse&sam\\_handle=123456789/1362](https://www.indiacode.nic.in/handle/123456789/1999?view_type=browse&sam_handle=123456789/1362)> accessed 12 July 2025.

<sup>2</sup> Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 77, 356, INDIA CODE (2023), <[https://www.indiacode.nic.in/handle/123456789/20062?view\\_type=search&col=123456789/1362](https://www.indiacode.nic.in/handle/123456789/20062?view_type=search&col=123456789/1362)> accessed 12 July 2025.

<sup>3</sup> The Copyright Act, 1957, No. 14, Acts of Parliament, 1957 (India), <[https://www.indiacode.nic.in/handle/123456789/1367?view\\_type=search&col=123456789/1362](https://www.indiacode.nic.in/handle/123456789/1367?view_type=search&col=123456789/1362)> accessed 12 July 2025.

In the landmark case of **K.S. Puttaswamy v. Union of India**,<sup>4</sup> the Supreme Court affirmed that the right to privacy is a fundamental right guaranteed under Article 21 of the Constitution<sup>5</sup>. See *K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India). Deepfakes, especially when non-consensual, infringe upon the individual's autonomy and decisional privacy.

### **The Growing Threat in India:**

India has already seen instances of deepfake content being used to spread political misinformation, defame public figures, and circulate morphed videos of private individuals. In 2023, several female celebrities were targeted through deepfakes, sparking widespread concern. Such incidents highlight the pressing need for regulatory measures to protect individual dignity and digital identity.

### **International Legal Approaches:**

The U.S. has introduced state laws like California's AB 602 (2019)<sup>6</sup>, which criminalizes malicious deepfakes, particularly in pornography and elections. China's Cyberspace Administration requires watermarks and real-identity registration for AI-generated content. Such international models can serve as useful references for India in shaping its own regulatory response<sup>7</sup>.

### **Challenges Ahead:**

---

<sup>4</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India), < <https://indiankanoon.org/doc/91938676/> > accessed 12 July 2025.

<sup>5</sup> INDIA CONST. art. 21.

<sup>6</sup> California A.B. 602, 2019 Leg., Reg. Sess. (Cal. 2019), < [https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill\\_id=201920200AB602](https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602) > accessed 12 July 2025.

<sup>7</sup> Cyberspace Admin. of China, Provisions on the Administration of Deep Synthesis Internet Information Services (2022), < <https://www.loc.gov/item/global-legal-monitor/2023-04-25/china-provisions-on-deep-synthesis-technology-enter-into-effect/> > accessed 12 July 2025.

Key challenges in regulating deepfakes include balancing freedom of expression (Art. 19(1)(a))<sup>8</sup> with the right to reputation, developing AI content detection tools, and empowering victims with accessible legal remedies. Current laws, while helpful, are fragmented and outdated for addressing such advanced technology.

**The way forward: Need for Regulation:**

India must evolve its legal response to tackle this growing digital threat. Some recommendations include:

- Enacting a dedicated law or amendment within the IT Act to criminalize malicious deepfakes.
- Mandating platform-level content checks using AI watermarking or detection tools.
- Establishing swift and effective grievance redressal systems for individuals affected by deepfake-related harm.
- Ensuring legal protections for freedom of expression while balancing individual rights and consent.

**Conclusion:**

Deepfakes represent one of the most dangerous and rapidly evolving forms of AI misuse in the digital era. Their potential to distort truth, infringe on privacy, and cause irreversible harm to individual reputation and societal trust cannot be overstated. With personal safety, professional integrity, and democratic values at stake, it is imperative for India to adopt a robust legal framework that directly addresses the challenges posed by synthetic media. Whether through amendments to the Information Technology Act or the introduction of a dedicated statute, timely legislative intervention is essential. Our laws must evolve in tandem with emerging technologies to uphold fundamental rights and ensure that malicious use of AI is identified, deterred, and effectively punished.

---

<sup>8</sup> INDIA CONST. art. 19(1)(a).