



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.

Deepfakes, Digital identity and Legal Liability: Is Indian Law Ready for the AI Era?

Ekta Sangneria



The pace at which artificial intelligence has been progressing is breathtaking, resulting in what is known as a crisis of authenticity in the digital space. The deepfake technology makes use of neural networks to manipulate audio, video, and visual data in such a realistic manner. This technology, which originated in entertainment, has been transformed into an instrument of deceit and extortion.

The Anatomy of the Threat: Beyond Mere Trickery

Deepfake technology depends on the machine learning models which are known as Generative Adversarial Networks (GANs). These competing models help create hyper-realistic fake content. In India, such powers have revealed serious weaknesses in many areas.

There have been cases where data harvesting from social media and public databases without any consent led to an increase in non-consensual pornographic content and defamation of one's reputation. The landmark decisions clearly state that privacy is a basic right; however, there are no means by which privacy can be protected against digital cloning. The other threat posed is political deepfakes.

There are new security challenges for India's efforts at digital identity ecosystems. The fraudsters have resorted to deepfakes in order to evade facial and voice authentication systems and commit banking scams and digital arrest scams. These are serious challenges in securing the rapidly growing Indian financial system.

The Legislative Gap: Are India's Laws Equipped?

The principal cyber laws in India such as the IT Act of 2000 and the Bharatiya Nyaya Sanhita have difficulty coping with generative AI. Though the old sections deal with general privacy violation cases, they do not address synthetic media. The police have difficulties due to foreign servers and the tough task of showing digital manipulation. Although the 2021 regulatory guidelines demand that harmful content be deleted by the social media sites within a short time, enforcement is patchy due to high internet traffic.

India already has several laws in place that deal with privacy, defamation, and obscenity, including the Information Technology Act and various sections of the Bharatiya Nyaya Sanhita. However, there are no specific measures to address the challenges posed by synthetic media (Aseri, Choudhary, & Kumar, 2025).

Legal scholars emphasize that current regulations face critical challenges. These are generally explored as

- I. Generative AI systems are often deployed internationally. Consequently, enforcement of any kind becomes particularly challenging.

- II. Demonstrating the identity of the perpetrator and proving malicious tampering requires the use of sophisticated forensic technology, which is not always readily available for local authorities.
- III. Any future regulation will have to strike a fine balance between the inhibition of malicious deepfakes and preserving the right to freedom of expression.

It is essential for India to move on from mere stopgap measures and introduce specific laws that explicitly define deepfakes and make the production of such content a punishable offense. The financial sector and the government websites should be able to detect any biometric spoofing through sophisticated means such as liveness detection and cryptographic watermarking.

The need for striking a balance between the innovative power of artificial intelligence and safeguarding basic rights calls for an active partnership between policymakers, technology firms, and civil society organizations. Nothing else will ensure that India retains its integrity in the digital future (Alanazi et al., 2025).

Privacy in the Age of Synthetic Media

The prevalence of deepfakes reveals the critical importance of a rethink on data privacy laws. As biometrics such as facial structure, voice pitch, and stride become easy to capture and edit without one's permission, the concept of "public data" becomes irrelevant.

Protecting individuals from synthetic exploitation demands a multi-layered approach:

1. Technological Countermeasures: Creating powerful detection mechanisms, cryptography-based watermarks, and blockchain-powered provenance tracking for the validation of genuine media.
2. Stricter Consent Frameworks: Requiring that there be clear consent before an individual's biometric likeness is used either commercially or publicly.
3. Institutional Accountability: Placing accountability on social media sites and companies developing generative AI technologies to moderate and reduce the spread of synthetic content.

Conclusion

Deepfake are the two-edged sword of the age that reveal the remarkable possibilities of artificial intelligence and its darkest dangers at the same time. In the face of an increasingly sophisticated form of media which becomes impossible to distinguish from the real world, safeguarding individual identity necessitates a combined effort of forensic tools, legislation and increased digital literacy on the part of citizens.

Context: Agree or Disagree

The project proposal has been completely approved owing to its ability to fill an important cybersecurity gap through an analysis of deepfake manipulations, weaknesses in law, and the privacy threats facing India's digital sphere. The research has proved itself academically and practically useful by presenting empirical evidence based on the latest literature on legal issues, deficiencies in existing regulation under the Information Technology laws, and countermeasures to synthetic identity theft.

References

- I. Alanazi, S., Asif, S., Caird-Daley, A., & Moulitsas, I. (2025). *Unmasking deepfakes: a multidisciplinary examination of social impacts and regulatory responses*. *Human-Intelligent Systems Integration*, 7(1), 131-153. doi: <https://doi.org/10.1007/s42454-025-00060-4>
- II. Aseri, V., Choudhary, S. K., & Kumar, A. (2025). *Intertwined Concept of Cybersecurity, Digital Forensics, and National Security*. In *Cyber Security, Forensics and National Security* (pp. 1-16). CRC Press. Doi: <https://doi.org/10.1201/9781003497868-1>
- III. Infosecurity Magazine. Available at <https://www.infosecurity-magazine.com/>
- IV. Help Net Security. Available at <https://www.helpnetsecurity.com/>
- V. The Hacker News. Available at <https://thehackernews.com/>
- VI. AI Law Blawg. Available at <https://ailawblawg.com/>

