



CYBER LAW

When Seeing Is No Longer Believing: Deepfakes, The Liar's Dividend, And The Crisis Of Digital Evidence In The Legal System

AUTHOR Appurv Bhatia, Priyanshi Dubey

PUBLISHED 13 January 2026

I. Introduction: The Death of Visual Truth

The aphorism “the camera does not lie” once formed the epistemic backbone of modern adjudication. By 2026, that assumption has collapsed. Artificial intelligence has rendered audiovisual evidence radically unstable, enabling the creation of hyper-realistic deepfakes that can fabricate events, speech, and conduct with alarming precision. While public discourse has focused on political misinformation and celebrity exploitation, a quieter and more consequential battle is unfolding within courtrooms, the battle for the integrity of evidence itself.

For legal practitioners, the threat is no longer merely fake news. It is the erosion of trust in probative material. When AI can manufacture reality, the law must confront a foundational question: how does one prove that a digital record is real?

Table of contents

- [I. Introduction: The Death of Visual Truth](#)
- [II. Deepfakes and the Emergence of the “Liar’s Dividend”](#)
- [III. The Indian Legal Response: Personality Rights and the IT Act](#)
 - [A. Judicial Recognition of Personality Rights](#)
 - [B. Statutory Framework under the Information Technology Act, 2000](#)
- [IV. The Courtroom Challenge: Digital Evidence under the Bharatiya Sakshya Adhiniyam, 2023](#)
- [V. Comparative Perspectives: Global Legal Responses to Deepfake Evidence](#)
 - [A. United States](#)
 - [B. European Union](#)
 - [C. China](#)
- [VI. The Way Forward: From Data Hygiene to Forensic Standards](#)
- [VII. Conclusion: Protecting Truth in an Age of Synthetic Reality](#)

II. Deepfakes and the Emergence of the “Liar’s Dividend”

Legal scholars have identified a phenomenon known as the “**Liar’s Dividend**”, a perverse advantage gained by wrongdoers in an era of synthetic media.¹ As deepfakes become commonplace, even genuine evidence is rendered suspect. A defendant confronted with an incriminating video can simply deny its authenticity by invoking AI manipulation.

This defence is no longer speculative. In cases involving sexual harassment, political corruption, or corporate fraud, the mere possibility of deepfake fabrication shifts the evidentiary burden onto the complainant. Courts are forced into prolonged forensic inquiries, delaying justice and increasing litigation costs. Over time, this scepticism risks corroding the judicial process itself, as audiovisual evidence, once considered among the most persuasive forms of proof, loses its presumptive credibility.

III. The Indian Legal Response: Personality Rights and the IT Act

A. Judicial Recognition of Personality Rights

Indian courts have responded swiftly to the creation and dissemination of deepfakes, particularly involving public figures. In *Anil Kapoor v Simply Life India*, the Delhi High Court recognised that an individual’s likeness, voice, and persona constitute enforceable personality rights, restraining unauthorised AI-generated reproductions.² This reasoning was reaffirmed and expanded in *Amitabh Bachchan v Rajat Negi*, where the court granted broad injunctive relief against misuse of the actor’s image and voice across digital platforms.³

These decisions align Indian jurisprudence with international trends recognising identity as a proprietary and dignitary interest, comparable to the right of publicity in the United States.⁴

B. Statutory Framework under the Information Technology Act, 2000

The Information Technology Act, 2000 provides a fragmented but functional toolkit against deepfakes:

- **Section 66D** criminalises cheating by impersonation using computer resources.

- **Section 66E** addresses violations of privacy involving the capture or transmission of private images.
- **Section 79** governs intermediary liability, with recent governmental advisories mandating takedown of reported deepfake content within strict timelines to retain safe-harbour protection.⁵

While these provisions deter creation and circulation, they are ill-equipped to resolve the evidentiary dilemma posed once deepfakes enter the courtroom.

IV. The Courtroom Challenge: Digital Evidence under the Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam (BSA), 2023, successor to the Indian Evidence Act, retains a technology-neutral approach to electronic records. Section 63 (replacing the infamous Section 65B) mandates certification of electronic evidence, focusing on the source and storage device.

However, this framework presumes the integrity of content. A Section 63 certificate can verify that a video originated from a particular device or server, but it cannot certify that the pixels themselves were not altered by a generative adversarial network.

This lacuna raises serious questions of admissibility. Courts may soon need to adopt a gatekeeping function, similar to the Daubert standard in the United States, where judges assess the reliability of scientific and technical evidence before trial.⁶ The authenticity of digital media may thus become a preliminary issue, rather than one left to cross-examination or final argument.

V. Comparative Perspectives: Global Legal Responses to Deepfake Evidence

A. United States

American courts have begun grappling with deepfakes through evidentiary doctrines. Under the Federal Rules of Evidence, authentication under Rule 901 now increasingly relies on expert testimony and metadata analysis.⁷ Scholars argue for mandatory provenance markers and cryptographic watermarking to restore trust in digital media.⁸

B. European Union

The EU's proposed **AI Act** adopts a risk-based framework, imposing transparency obligations for synthetic media and requiring disclosure where content is AI-generated.⁹ While primarily regulatory, such measures indirectly strengthen evidentiary reliability by normalising disclosure norms.

C. China

China has adopted one of the most stringent regimes, mandating clear labelling of synthetic content and imposing liability on platforms for failure to detect deepfakes.¹⁰ This proactive approach reflects a recognition that evidentiary harm is not merely procedural but societal.

VI. The Way Forward: From Data Hygiene to Forensic Standards

For litigants and counsel, the immediate lesson is data hygiene. Digital evidence must be accompanied by an unbroken chain of custody, secure storage, and contemporaneous documentation. Increasingly, parties may need to rely on:

- Cryptographic hashing at the point of recording
- Secure audit trails
- Independent forensic verification

For the legal system, however, the challenge is structural. While existing laws punish creators and distributors of deepfakes, they do not protect the truth once doubt has been injected. Uniform forensic standards, judicial training in AI literacy, and possibly statutory presumptions regarding authenticated media will be essential.

VII. Conclusion: Protecting Truth in an Age of Synthetic Reality

Deepfakes do not merely threaten reputation or privacy; they strike at the epistemic foundations of justice. The "Deepfake Defence" and the resulting Liar's Dividend risk creating a world where truth itself becomes contestable, not on the basis of facts, but on technological plausibility.

Indian law has made commendable strides in protecting identity and punishing misuse. The next frontier lies in safeguarding evidentiary integrity. Courts must evolve from passive arbiters to informed gatekeepers, capable of distinguishing between manufactured illusion and factual reality.

In the age of artificial intelligence, the law's greatest task may be to reaffirm a simple but endangered principle: truth must still be provable.

For more details, write to us at: contact@indialaw.in

References

1. Chesney, Bobby; Citron, Danielle. (2019). Deep Fakes: A Looming Challenge for Privacy. California Law Review. <https://doi.org/10.15779/Z38RV0D15J> ??
2. Anil Kapoor v Simply Life India & Ors 2023 SCC OnLine Del 6914. ??
3. Amitabh Bachchan v Rajat Negi 2022 SCC OnLine Del 4110. ??
4. Zacchini v Scripps-Howard Broadcasting Co 433 US 562 (1977). ??
5. Ministry of Electronics and Information Technology, Advisory on Deepfake Content (2023). ??
6. Daubert v Merrell Dow Pharmaceuticals Inc 509 US 579 (1993). ??
7. Lorraine v Markel American Insurance Co 241 FRD 534 (D Md 2007). ??
8. Hany Farid, 'Digital Image Forensics' (2009) 2 Scientific American 66. ??
9. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on harmonised rules on artificial intelligence, OJ L 1689 (12 July 2024). ??
10. Zhang, L. (2023) China: Provisions on Deep Synthesis Technology Enter into Effect. [Web Page] Retrieved from the Library of Congress, <https://www.loc.gov/item/global-legal-monitor/2023-04-25/china-provisions-on-deep-synthesis-technology-enter-into-effect/>. ??

Related Practice Areas

AI, Blockchain, and Emerging Technologies

Technology Law

Litigation