# 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




## THE LEGAL IMPLICATIONS OF DEEPFAKES AND AI-GENERATED EVIDENCE IN INDIAN COURTS.


- ***PREETI R MUGAD***



### INTRODUCTION

The Courts across various jurisdictions have witnessed the AI-generated evidence in recent years, from deepfake witness testimony to fabricated voice recordings to altered crime scene photographs, each case exposing a gap in how law currently handles synthetic media. For

instance, in the *Mendones v. Cushman & Wakefield,*[1] when the witness's face appeared to be motionless, consisting of strange cuts and repetition of her mannerisms, the California Judge Victoria Kolakowski, reviewed the video, only to realise that the evidence was AI-generated audio and video of a real person.[2] Similarly, in *Mr. Sudhir Chaudhary vs Meta Platforms*[3], the Delhi High Court, highlighted the misuse of AI to create and circulate misleading videos, as such videos result in both misleading the public and hampering the reputation of the individual involved. Such a rise in deepfake technology, synthetic media and AI-generated content has given rise to unprecedented challenges involving legal complexity, judicial truth-finding and most importantly to the distinction between the manipulated reality and the actual reality. Thus, it is no longer as essential to find the source or integrity of the electronic evidence as it is of proving its very authenticity.[4]

## WHAT ARE DEEPFAKES AND TYPES OF AI-GENERATED EVIDENCE?

Deepfake, as the word suggests, is a mixture of two words, deep learning, a branch of artificial intelligence and fake, something which is not real, together it refers to a technology which produces hyper-realistic images, audio recordings and videos using a person's face, voice or likeness by using the machine learning technology.[5] These are artificially generated or altered with an aim to make them look real, as if the person himself is saying or doing these things, when in reality they are completely fake. Such a technology is now widely used in online attacks by generating fake identities, blackmailing or sharing intimate images without permission.[6]

The AI-generated evidence is of two categories. One is acknowledged AI-generated evidence which is openly accepted to be generated or created and modified with the help of AI, thereby highlighting transparency and enabling courts to deal with them in such a manner. Second is the unacknowledged AI-generated evidence which is presented as if it is authentic and not generated by any AI tools, when in reality, such evidence is a product of AI and includes the

[1] Mendones v. Cushman & Wakefield, Inc., No. 23CV028772 (Cal. Super. Ct. Alameda Cnty. Sept. 9, 2025).
[2] Connor Heaton, Shay Cleary & Michael Navin, *AI-Generated Evidence is a Threat to Public Trust in the Courts*, NAT'L CTR. FOR STATE COURTS, https://www.ncsc.org/resources-courts/ai-generated-evidence-threat-public-trust-courts (last visited May 10, 2026).
[3] Mr. Sudhir Chaudhary v. Meta Platforms Inc. & Ors., CS(COMM) 1089/2025 (Delhi H.C. Oct. 10, 2025).
[4] Amar Gupta, *Artificial Intelligence, Deepfakes and the Law: India's Judicial Moment*, FORTUNE INDIA, (May 10, 2026, 7:29 PM) https://www.fortuneindia.com/opinion/artificial-intelligence-deepfakes-and-the-law-indias-judicial-moment/130373.
[5] Pooja Kisan Bhosale, Mannalal R. Pandiya & Vijay Sahadeo Chavan, *Deepfakes and False Digital Evidence in Indian Courts*, 12 INT'L J.L. 378, 378-379 (2026).
[6] Shinu Vig, *Regulating Deepfakes: An Indian Perspective*, 17 J. STRATEGIC SECURITY 70, 70 (2024).

deepfake videos, images, manipulated photographs, etc.[7] It is this type of evidence that pose serious challenge before the courts regarding their detection and authenticity. The mere fact that such evidence generation need not necessarily be done by an expert but by ordinary people with minimal technical knowledge and understanding as well, is alarmingly serious as such an ability affects the fairness in the judicial process. It is an irony that AI tools used by Law enforcement agencies to detect these fake evidences, are the very ones that generate them.[8]

## THE EVIDENTIARY BASELINE: WHAT THE LAW CURRENTLY SAYS

India's existing legal framework governing electronic evidence and synthetic media, consists of several statutes. The Bharatiya Sakshya Adhiniyam, 2023, under Section 63[9], requires a certificate to be attached with the electronic records to show that such a record was generated by a computer, which speaks only about its origin, but not about whether the underlying content is real or not. A deepfake does not tamper with an original file, instead, it generated a new one from scratch, which comes out clean and appears to be real, thus, questioning the role of such a certificate.[10] The Information Technology Act, 2000, through Sections 66C and 66D[11] criminalises identity theft and cheating by impersonation through computer resources, and Section 66E[12], penalises the publication of private images without consent, which makes it

[7] Natalie Runyon, *Deepfakes on Trial: How Judges are Navigating AI Evidence Authentication*, THOMSON REUTERS INST., (May 10, 2026, 8:30 PM) https://www.thomsonreuters.com/en-us/posts/ai-in-courts/deepfakes-evidence-authentication/.
[8] Bhosale, Pandiya & Chavan, supra note 5, at 378.
[9] Bharatiya Sakshya Adhiniyam, 2023, § 63, No. 47, Acts of Parliament, 2023 (India).
[10] Vansh Srivastava & Arvind Kumar Singh, *Legal Status of AI-Generated Evidence in Indian Courts*, 4 LAWFOYER INT'L J. DOCTRINAL LEGAL RES. 2298, 2303-2304 (2026).
[11] Information Technology Act, 2000, §§ 66C, 66D, No. 21, Acts of Parliament, 2000 (India).
[12] Information Technology Act, 2000, § 66E, No. 21, Acts of Parliament, 2000 (India).

directly applicable to non-consensual deepfakes. Sections 67 and 67A[13] further criminalise obscene and sexually explicit electronic content. The Bharatiya Nyaya Sanhita, 2023 supplements this through Section 336[14], which criminalises electronic forgery, and Section 356[15], which extends defamation law to synthetic media. The Digital Personal Data Protection Act, 2023 requires consent for processing personal data, meaning deepfakes created using a person's biometric data without consent can attract penalties of up to Rs. 250 crores.[16] However, all of these were specifically built to tackle the issues involving unauthorised alteration of existing data, not the entire creation of new media.[17]

The most direct regulatory response came in February 2026, when the Ministry of Electronics and Information Technology amended the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[18] The amendment introduced four key changes: a statutory definition of deepfake as content generated using algorithmic or computational techniques to produce sound or visuals convincing enough to pass as authentic representations of real individuals; a drastic reduction in takedown timelines from 36 hours to merely three hours; mandatory technical disclosure and traceability measures requiring intermediaries to embed metadata enabling AI-generated content to be traced back to its source; and expanded compliance and dispute resolution obligations for significant intermediaries, compressing resolution windows from fifteen days to seven. Yet, this amendment focuses on the actions to be taken by platforms when such synthetic content spreads online, but says nothing about what the courts should do when the same content comes before it as evidence.[19]

## LOOKING AHEAD: TRUST, TECHNOLOGY, AND THE COURTROOM

The deepfake problem is at its core. Even the Supreme Court in *Gummadi Usha Rani v. Sure Mallikarjuna Rao*[20] was confronted with a trial court that had relied upon completely non-existent judgments generated using AI. The court observed that such reliance on fake AI-generated judgements will be a misconduct and legal consequences shall follow. It also asked

[13] Information Technology Act, 2000, §§ 67, 67A, No. 21, Acts of Parliament, 2000 (India).
[14] Bharatiya Nyaya Sanhita, 2023, § 336, No. 45, Acts of Parliament, 2023 (India).
[15] Bharatiya Nyaya Sanhita, 2023, § 356, No. 45, Acts of Parliament, 2023 (India).
[16] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[17] Srivastava & Kumar Singh, *supra* note 8, at 2303-2308.
[18] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended Feb. 2026), No. G.S.R. 139(E), Ministry of Electronics and Information Technology (India).
[19] Aayushman Gaikwad & Smruti Mishra, *Three Hours to Comply: India's New Rules for AI-Generated Content and Deepfakes*, LIVE LAW (last visited May 10, 2026), https://www.livelaw.in/articles/ai-generated-content-deepfakes-524064.
[20] Gummadi Usha Rani & Anr. v. Sure Mallikarjuna Rao & Anr., SLP (C) No. 7575 of 2026 (S.C. Feb. 27, 2026).

the Bar Council of India to constitute a committee of experts, in order to examine issues arising from the use of AI in court proceedings, particularly where trial courts rely on such judgments.[21] Even the apex court is now analysing this issue, which shows how unprepared our systems are. Hence the deepfake challenge demands more proactive measures, specifically designed to deal with the evidence generated in the AI-era.

[21] Amisha Shrivastava, *Use of AI-Generated Fake Judgments: Supreme Court Urges BCI to Form Expert Panel to Examine Issue*, LIVE LAW (last visited May 10, 2026), https://www.livelaw.in/top-stories/use-of-ai-generated-fake-judgments-supreme-court-urges-bci-to-form-expert-panel-to-examine-issue-533023.