Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

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.

When Seeing is no Longer Believing: Admissibility of Deepfake Evidence under Indian Evidence Law

P Sakshi Reddy[a]

[a]Christ Academy Institute of Law, Bengaluru, India

Received 02 April 2026; *Accepted* 06 May 2026; *Published* 11 May 2026

The rapid proliferation of deepfake technology, hyper-realistic synthetic media generated through artificial intelligence, poses an unprecedented challenge to the administration of justice in India. Courts have historically treated visual and audio evidence as cogent proof of fact, yet deepfakes undermine this foundational assumption with alarming ease. This article examines the admissibility of deepfake evidence under India's existing evidentiary framework, with particular focus on the Indian Evidence Act 1872, its successor the Bharatiya Sakshya Adhiniyam 2023, and the Information Technology Act 2000. It analyses the doctrinal requirements of authenticity, relevance, and reliability through which electronic evidence must pass before being admitted, and evaluates whether these requirements are adequate to address the technical sophistication of synthetic media. Drawing on judicial precedent, comparative jurisprudence from the United States and the United Kingdom, and emerging international regulatory instruments, the article argues that India's current legal architecture is structurally ill-equipped to either reliably admit authentic deepfake evidence or systematically exclude fabricated deepfake evidence. The article concludes with a set of de lege ferenda recommendations, including the introduction of a mandatory certification protocol for AI-generated media, the establishment of a panel of court-appointed forensic examiners, and targeted legislative amendments to the Bharatiya Sakshya Adhiniyam 2023 to incorporate deepfake-specific disclosure obligations.

Keywords: *deepfake, electronic evidence, admissibility, authenticity, digital forensics, artificial intelligence.*

INTRODUCTION

In 2017, a new word entered the legal lexicon: 'deepfake.'[1] Coined on an internet forum, it described synthetic audiovisual content generated by deep learning algorithms capable of mapping one person's face or voice onto another's with uncanny verisimilitude. Within half a decade, the technology migrated from online subcultures to the mainstream, driven by the commodification of generative adversarial networks (GANs) and diffusion models that now enable any person with a consumer laptop to fabricate convincing video of a political leader confessing to crimes never committed, a corporate executive ordering fraudulent transaction, or an ordinary citizen engaging in conduct they never performed.[2]

The implications for courts of law are profound and immediate. Evidence law, across all major jurisdictions, is premised upon what might be called the *epistemic reliability assumption* the belief that audio-visual recordings, unlike testimony, bear an intrinsic fidelity to reality. A photograph cannot lie in the way a witness can. CCTV footage captures what actually occurred. This assumption underlies both the popular imagination of justice and the technical rules governing the admissibility of electronic evidence. Deepfakes rupture this assumption entirely.[3]

India presents a particularly acute site for examining these challenges. The country has witnessed explosive growth in digital penetration, with over 800 million active internet users as of 2023, yet its evidentiary framework remains anchored in nineteenth-century legislative text. The Indian Evidence Act 1872[4][5], now substantially replaced by the Bharatiya Sakshya Adhiniyam 2023[6] (hereinafter 'BSA'), was not designed with artificial intelligence in contemplation. Judicial decisions have attempted to modernise it incrementally through the interpretation of sections 65A and 65B concerning electronic evidence, but the structural gaps exposed by deepfake technology require more than interpretive gymnastics.

---

[1] Nina Schick, *DEEP FAKES and the infocalypse: What You Urgently Need To Know* (Monoray 2020)
[2] Lingzhi Li et al., 'Advancing High Fidelity Identity Swapping for Forgery Detection' (Conference on Computer Vision and Pattern Recognition, Seattle, WA, USA, 2020)
[3] Robert Chesney & Danielle K Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review <https://scholarship.law.bu.edu/faculty_scholarship/640/> accessed 04 April 2026
[4] Information Technology Act 2000
[5] Indian Evidence Act 1872
[6] Bharatiya Sakshya Adhiniyam 2023

DEEPFAKES: TECHNOLOGY, TAXONOMY, AND LEGAL HARM

The Technical Architecture of Deepfakes: Deepfake generation relies principally upon two deep learning paradigms: generative adversarial networks (GANs) and, more recently, diffusion models. A GAN consists of two competing neural networks a generator that synthesises fake content and a discriminator that attempts to distinguish fake from real. Through iterative adversarial training, the generator learns to produce outputs so realistic that the discriminator can no longer reliably identify them as fabricated. Diffusion models, which underlie systems such as Stable Diffusion and OpenAI's Sora, operate differently: they learn to reverse a noise-injection process, thereby generating photorealistic images or videos from textual prompts with exceptional fidelity.

The resulting synthetic media falls within a broader taxonomy that courts must learn to navigate. At one end lies *face-swap deepfakes*, which replace a target individual's facial features in an existing video with those of another. Next are *voice cloning deepfakes*, which synthesise speech in a target individual's voice from as few as three seconds of reference audio. More sophisticated still are *full-body puppeteering* technologies, which animate a static image or alter body language in a video. Finally, *text-to-video generation* systems create entirely novel footage from textual descriptions, with no source material required at all.[7]

Legal Harms Generated by Deepfakes: The legal harms generated by deepfakes are multidimensional. In criminal proceedings, a fabricated video can be tendered as evidence of a crime never committed or, inversely, a genuine video of an actual crime may be dismissed as a deepfake by a sophisticated defendant. In civil litigation, synthetic audio purporting to record a contract negotiation, a confession of liability, or a defamatory statement can distort the factual record. In the sphere of electoral integrity, deepfake political advertisements create false impressions of candidates' statements with the capacity to influence democratic outcomes.[8]

Of particular urgency in India is the phenomenon of deepfake non-consensual intimate imagery (NCII) fabricated sexually explicit content depicting real individuals. High-profile incidents involving Bollywood actresses and female journalists have brought this harm into

[7] Henry Ajder et al., *THE STATE OF DEEPFAKES: LANDSCAPE, THREATS AND IMPACT* (Deeptrace, 2019)
[8] Danielle Keats Citron, 'Sexual Privacy' (2019) 128 Yale Law Journal <https://yalelawjournal.org/pdf/Citron_q8ew5jjf.pdf> accessed 04 April 2026

sharp public focus. The National Crime Records Bureau has recorded a sharp upward trajectory in cases registered under section 66E of the Information Technology Act[9] and section 67A[10][11] in recent years, though definitional limitations mean that deepfake-specific incidents remain underreported.

THE INDIAN EVIDENTIARY FRAMEWORK FOR ELECTRONIC EVIDENCE

The Indian Evidence Act 1872: Sections 65A and 65B: The Indian Evidence Act 1872, as amended by the Information Technology Act 2000, introduced sections 65A and 65B to provide a dedicated mechanism for the admission of electronic records.[12] Section 65A proclaimed that the contents of electronic records may be proved in accordance with the provisions of section 65B.[13] Section 65B prescribed conditions under which a computer output defined broadly to encompass any document produced by a computer would be deemed admissible: the computer must have been in regular use, the information must have been stored in the ordinary course of activities, the computer must have been functioning properly, and a certificate from a responsible official attesting to these matters must accompany the output.

The Supreme Court's engagement with section 65B has been characterised by doctrinal oscillation. In *Anvar PV v PK Basheer*[14], a Constitution Bench held that a section 65B certificate is a condition precedent to the admissibility of electronic evidence and cannot be substituted by oral evidence under section 65. This overruled earlier decisions that had treated electronic evidence more permissively. However, in *Shafhi Mohammad v State of Himachal Pradesh*[15], a two-judge bench introduced a relaxation, holding that the certificate requirement could be waived in the interest of justice where the electronic device was not in the possession of the party seeking to adduce it.

The conflict between these decisions was finally resolved in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*[16], where a three-judge bench affirmed *Anvar PV* and held that the section

[9] Information Technology (Amendment) Act 2008, s 66E
[10] Information Technology Act 2000, s 67
[11] Information Technology Act 2000, s 67A
[12] Indian Evidence Act 1872, s 65A
[13] Indian Evidence Act 1872, s 65B
[14] *Anvar P V v P K Basheer & Ors* (2014) 10 SCC 473
[15] *Shafhi Mohammad v The State of Himachal Pradesh* (2018) 2 SCC 801
[16] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal & Ors* AIR 2020 SC 4908

65B certificate is mandatory. The Court further clarified that the certificate must identify the device, attest to its proper functioning, and be provided by the person responsible for operating the device at the material time. Critically, the Court also acknowledged that courts retain discretion to call for additional proof of authenticity where circumstances so require a discretion that becomes especially significant in the context of deepfakes.

Expert Opinion: Sections 45 and 47: Beyond certification, the Evidence Act provides for expert opinion under section 45[17], which allows courts to receive the opinions of persons 'especially skilled' in science, art, foreign law, or handwriting where such opinion is relevant. Section 47[18] provides for an opinion on handwriting specifically. Neither provision was drafted with digital forensics in mind, and neither provides any framework for assessing the methodological validity of an expert's approach a gap that becomes critical when courts must evaluate competing claims about whether a video has been algorithmically manipulated.

The Bharatiya Sakshya Adhiniyam 2023: Continuity and Change: The BSA, which came into force on 1 July 2024, substantially re-enacts the architecture of the Indian Evidence Act while introducing some modernising provisions. Section 57 of the BSA corresponds to the erstwhile section 45, preserving the expert opinion framework.[19] Section 63 re-enacts section 65B with minor modifications.[20] Section 61 introduces a new category of 'primary evidence' for electronic records that are stored in a device: where a document is stored exclusively on a digital medium, the electronic record itself is primary evidence.[21]

Most significantly for present purposes, section 22A of the BSA[22], which has no direct antecedent in the Indian Evidence Act, provides that oral admissions as to the contents of electronic records are not relevant unless the genuineness of the electronic record is in question. This provision, read alongside the certification requirements of section 63, creates a gatekeeping function at the threshold of admissibility. However, it does not specify the standards by which 'genuineness' is to be assessed, nor does it address the evidential burden of establishing that an otherwise authentic-looking record is, in fact, synthetically generated.

[17] Indian Evidence Act 1872, s 45
[18] Indian Evidence Act 1872, s 47
[19] Bharatiya Sakshya Adhiniyam 2023, s 57
[20] Bharatiya Sakshya Adhiniyam 2023, s 63
[21] Bharatiya Sakshya Adhiniyam 2023, s 61
[22] Bharatiya Sakshya Adhiniyam 2023, s 22A

These lacunae leave Indian courts largely rudderless when confronted with deepfake evidence.

DEEPFAKES AND THE ADMISSIBILITY INQUIRY: DOCTRINAL CHALLENGES

Authentication: The requirement that a party seeking to adduce a document establish that it is what it purports to be is the first and most fundamental obstacle that deepfake evidence presents. Under the Indian framework, authentication of an electronic record is achieved primarily through the Section 65B/63 BSA certificate. The certificate attests that the output was generated by a computer in regular use that was functioning properly. But this attestation is addressed to the integrity of the output process, not to the authenticity of the content itself.

Consider a scenario in which an authentic CCTV recording of a crime is downloaded, subjected to a face-swap deepfake algorithm to replace the perpetrator's face with that of an innocent person, and then re-encoded onto a storage device. A section 65B certificate issued in relation to this device would truthfully attest that the device was in regular use, that the information was stored in the ordinary course of activities, and that the computer was functioning properly. The certificate is technically accurate, yet it certifies what is, in substance, fabricated evidence. The certification regime, in other words, authenticates the carrier of the record but is structurally incapable of authenticating its content.

This structural gap means that authentication of deepfake-affected evidence necessarily requires forensic analysis beyond certification. Digital forensic examiners employ a range of techniques to detect manipulation: metadata analysis, compression artefact detection, facial landmark inconsistency analysis, blinking frequency anomalies, physiological signal analysis (such as rPPG remote photoplethysmography, which detects the pulse wave absent in synthetic faces), and, most recently, neural network-based deepfake classifiers trained on large corpora of known synthetic media.[23] The reliability of each technique varies, and the adversarial dynamic between detection and generation means that state-of-the-art classifiers are regularly defeated by improved generation models. Indian courts have no established protocol for evaluating the reliability of such methods.

[23] Hany Farid, *Photo Forensics* (MIT Press 2019)

Relevance and Prejudice: Even if an item of evidence clears the authentication threshold, courts must assess its relevance and weigh its probative value against its prejudicial effect. The Indian framework, unlike the US Federal Rules of Evidence (Rule 403) or the English common law doctrine of discretionary exclusion, does not contain an explicit provision authorising exclusion of relevant but unduly prejudicial evidence. The Supreme Court has, however, exercised an analogous discretion in many cases.[24] In *Tomaso Bruno v State of Uttar Pradesh*[25], the Court observed that the admission of evidence whose authenticity is doubtful may cause irreparable prejudice to an accused and that courts must exercise 'judicious care' in such matters.

Deepfakes exacerbate the prejudice dimension of this inquiry in a specific way: the very realism that makes synthetic media technically impressive makes it cognitively dangerous for lay triers of fact. Research in cognitive psychology demonstrates that human beings are remarkably poor at identifying deepfake video even when explicitly alerted to the possibility of manipulation a phenomenon sometimes termed the 'liar's dividend' by reference to the perverse possibility that genuinely authentic footage may be dismissed as deepfake by a technologically literate but methodologically skeptical adjudicator. Courts must therefore be equipped not only to assess the authenticity of specific items of evidence but also to manage the systemic epistemological effects of deepfake technology on the trial process.

The Burden and Standard of Proof: The burden of proof in Indian law is governed by sections 101 and 102 of the Indian Evidence Act (sections 104 and 105 of the BSA).[26][27] The general rule is that the burden of proving a fact lies on the party who asserts it. In the context of deepfakes, a critical ambiguity arises: who bears the burden of establishing that tendered evidence is genuine, or, conversely, that tendered evidence is fabricated?

Where a prosecution tenders a video recording as evidence of a crime, the defence may challenge its authenticity on the ground that it is a deepfake. Does the prosecution then bear the burden of proving authenticity beyond the certification requirements of section 63 BSA? Or does the defence bear the burden of proving inauthenticity? The answer has significant practical consequences. Establishing the positive genuineness of a video recording

[24] *State of Maharashtra v Dr Praful B Desai* (2003) 4 SCC 601
[25] *Tomaso Bruno & Anr v State of Uttar Pradesh* (2015) 7 SCC 178
[26] Indian Evidence Act 1872, s 101
[27] Indian Evidence Act 1872, s 102

demonstrating that it has not been algorithmically manipulated is technically far more demanding than establishing inauthenticity, because detection techniques are inherently reactive to generation techniques. Placing the burden of proving non-manipulation on the prosecution would impose an evidentiary obligation that may exceed the current state of forensic science. The Supreme Court's observation in *Re Dipanwita Roy v Ronobroto Roy*[28] that courts must be slow to draw adverse inferences from the failure to produce electronic evidence is relevant here, as is the principle in *Chitresh Kumar Chopra v State (Govt of NCT of Delhi)*[29] that circumstantial evidence must form a complete chain before an inference of guilt may be drawn. In deepfake cases, the integrity of that chain is precisely what is in question.

COMPARATIVE PERSPECTIVES

The United States: In the United States, evidentiary challenges concerning electronically generated content are governed by the Federal Rules of Evidence, particularly Rule 901 (authentication), Rule 702 (expert testimony), and Rule 403 (exclusion for prejudice). The Supreme Court's decision in *Daubert v Merrell Dow Pharmaceuticals Inc*[30] established a judicial gatekeeping function for scientific expert evidence, requiring courts to assess the testability, peer review, error rate, and general acceptance of the methodology offered. Applied to deepfake detection, the *Daubert* framework would require courts to evaluate whether a proposed forensic deepfake detection method is scientifically valid before admitting expert opinion based upon it.

American courts have begun to grapple with deepfake-adjacent authentication challenges in the context of AI-generated content more broadly.[31] Several state legislatures including California, Texas, and Virginia have enacted specific deepfake legislation addressing electoral manipulation and non-consensual intimate imagery, providing both criminal prohibitions and civil remedies. At the federal level, the proposed Deepfakes Accountability

[28] *Dipanwita Roy v Ronobroto Roy* AIR 2015 SC 418
[29] *Chitresh Kumar Chopra v State (Govt of NCT of Delhi*) (2009) 16 SCC 605
[30] *Daubert v Merrell Dow Pharmaceuticals Inc* [1993] 509 US 579
[31] Ryan Calo, 'Artificial Intelligence Policy: A Primer and Roadmap' (2017) 51 University of California, Davis <https://lawreview.law.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/51-2_Calo.pdf> accessed 04 April 2026

Act[32] and the Malicious Deep Fake Prohibition Act[33] have been introduced but not enacted, leaving a legislative gap that practitioners navigate through existing doctrine.

The United Kingdom: English law approaches electronic evidence through the common law of authenticity and the provisions of the Civil Evidence Act 1995 and the Police and Criminal Evidence Act 1984. The Court of Appeal's decision in *R v Reed and Reed; R v Garmson*[34] established that computer-generated evidence is presumptively reliable but subject to challenge on specific grounds. The Online Safety Act 2023 introduced a specific offence of sharing intimate deepfake images without consent, representing one of the more comprehensive legislative responses to deepfake-related harm in a major common law jurisdiction. The UK's approach is notable for its explicit acknowledgement that the traditional presumption of reliability attaching to electronic evidence must be qualified in light of the capacity for algorithmic manipulation.

The European Union: The EU's Artificial Intelligence Act 2024[35] imposes mandatory transparency obligations on providers of AI systems capable of generating synthetic media: such systems must ensure that outputs are labelled as artificially generated or manipulated in a manner that is detectable by automated means. This 'watermarking' obligation creates an evidentiary artefact, the watermark, that could in principle assist courts in identifying synthetic content. However, the watermark is subject to removal by sophisticated actors, and its absence cannot be taken as proof of non-manipulation. The EU framework is nonetheless instructive as a regulatory model for India to consider adapting.

INDIA'S EMERGING REGULATORY RESPONSE

India's regulatory response to deepfake technology has thus far been predominantly advisory rather than legislative. In November 2023, the Ministry of Electronics and Information Technology (MeitY) issued an advisory directing intermediary to ensure that existing provisions of the IT Act and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 are scrupulously enforced against deepfake

[32] Deepfakes Accountability Act 2019
[33] Malicious Deep Fake Prohibition Act of 2018, s 3805
[34] *R v Reed & Ors* [2009] EWCA Crim 2698
[35] Artificial Intelligence Regulations 2024, art 52

content. The advisory specifically invoked rule 3(1)(b)(vii), which prohibits content that is 'patently false and untrue', and rule 3(1)(b)(ix), which prohibits impersonation.

The Digital Personal Data Protection Act 2023[36] offers a complementary regulatory instrument. By establishing a framework for the consent-based processing of personal data, including biometric data such as facial and voice features, the DPDPA potentially restricts the dataset collection that underpins deepfake generation. However, the DPDPA is directed at data fiduciaries (entities processing data) rather than at the generation of synthetic media per se, and its enforcement mechanisms are not calibrated to address evidentiary challenges in ongoing litigation.

The Law Commission of India has not yet specifically addressed deepfakes, though its earlier work on trial by media[37] and the Srikrishna Committee's foundational analysis of privacy in the digital age provide relevant analytical frameworks. The current legislative environment is characterised by an enforcement gap: existing penal and civil provisions apply to deepfake harms in principle, but the absence of a dedicated statutory framework for deepfake identification and evidentiary management leaves courts without adequate procedural tools.

RECOMMENDATIONS: TOWARDS A DEEPFAKE-RESPONSIVE EVIDENTIARY FRAMEWORK

Mandatory Authenticity Disclosure Obligations: India should amend the BSA to introduce a specific disclosure obligation applicable to any party seeking to adduce audio-visual electronic evidence in proceedings before a court. The obligation should require the disclosing party to specify: (i) the device and software used to generate or record the content; (ii) the chain of custody of the recording from creation to production; (iii) whether any AI-assisted editing, enhancement, or generation tool was applied to the content at any stage; and (iv) the results of any authenticity verification process conducted before production. This disclosure framework would not predetermine admissibility but would provide the opposing party and the court with the information necessary to mount a meaningful challenge.

[36] Digital Personal Data Protection Act 2023
[37] Law Commission of India, *Report No 200: On Trial by Media* (Law Com No 200, 2006)

A Panel of Court-Appointed Forensic Examiners: The current reliance on party-appointed experts creates an adversarial dynamic ill-suited to the technical complexity of deepfake detection. Where authenticity of audio-visual evidence is placed in dispute, courts should have the power and the procedural infrastructure to appoint a neutral forensic examiner from a pre-established panel maintained by the Central Forensic Science Laboratory (CFSL) or a newly constituted National Digital Forensics Institute. Court-appointed examiners should be required to employ a standardised methodology validated by a technical committee, and their reports should be subject to cross-examination by both parties. This approach, drawing on the model of court-appointed experts in complex commercial litigation, would provide a more reliable epistemic foundation for judicial determinations of authenticity.

A Deepfake-Specific Evidentiary Standard: The BSA should be amended to introduce a provision specifying that where a party disputes the authenticity of an audio-visual electronic record on the ground that it may constitute synthetically generated content, the court shall, before admitting the record, be satisfied that reasonable forensic steps have been taken to verify its authenticity. The standard of satisfaction should be calibrated to the gravity of the proceeding: in criminal cases where the electronic record is relied upon as primary evidence of the actus reus, a heightened standard of forensic verification should apply. The provision should further specify that the burden of producing prima facie evidence of manipulation lies with the party alleging it, after which the burden shifts to the tendering party to establish authenticity on the balance of probabilities.

Mandating Provenance Watermarking: Borrowing from the EU AI Act model, India should require that AI systems capable of generating synthetic audio-visual media made available to consumers through app stores or digital platforms subject to Indian jurisdiction incorporate provenance watermarking technology that encodes an invisible but machine-detectable signature identifying the content as AI-generated. The CFSL and its state counterparts should be equipped with watermark-detection tools capable of reading such signatures. While acknowledging that watermarks can be removed by sophisticated actors, mandatory watermarking would raise the evidential cost of fabrication and provide courts with an additional detection layer in the substantial proportion of cases involving less technically sophisticated fabricators.

Judicial Training and Specialised Benches: Technical literacy among the judiciary is a prerequisite for the effective implementation of any deepfake-responsive evidentiary framework. The National Judicial Academy and state judicial academies should develop dedicated modules on artificial intelligence and digital forensics, equipping judges to assess the methodological validity of forensic expert evidence and to recognise the cognitive risks posed by hyper-realistic synthetic media. In High Courts and the Supreme Court, it may be desirable to constitute specialised intellectual property and technology benches whose members receive advanced training in digital forensics, analogous to the practice in specialist commercial courts.

CONCLUSION

The admissibility of deepfake evidence under Indian evidence law presents a challenge that is simultaneously technical, doctrinal, and institutional. Technically, the sophistication of current generative models means that synthetic media can defeat all but the most advanced forensic detection methods, and the adversarial dynamic between generation and detection ensures that the evidentiary landscape will continue to evolve. Doctrinally, the existing framework anchored in the certification regime of section 63 BSA and the expert opinion provisions of section 57 is structurally misaligned with the nature of deepfake manipulation: it authenticates the carrier of a record but is silent on the authenticity of its content, and it provides no standards for evaluating competing forensic methodologies.

Institutionally, the gap is perhaps most significant. Courts in India lack the forensic infrastructure, the procedural tools, and, as yet, the judicial training to reliably distinguish authentic from synthetic evidence in the context of a determined and well-resourced fabricator. The ‘liar's dividend’, the perverse epistemic benefit that deepfake technology confers upon those who seek to discredit genuine evidence, threatens to undermine the integrity of the adjudicative process just as much as the direct admission of fabricated evidence.

The reforms proposed in this article mandatory authenticity disclosure, court-appointed forensic panels, a deepfake-specific evidentiary standard, provenance watermarking, and judicial training do not offer a technological solution to what is ultimately a social and legal challenge. No forensic tool can guarantee the infallibility of authenticity determinations, and

no legislative provision can anticipate every future configuration of synthetic media technology. What the law can do, however, is create a structured framework of incentives and procedural safeguards that raises the cost and risk of tendering fabricated evidence, equips courts with the institutional resources to make reasoned authenticity determinations, and restores a measure of epistemic trust to an evidentiary system that the deepfake revolution is in the process of destabilising.[38]

When seeing is no longer believing, the law must ensure that courts retain the institutional capacity to know the difference.

[38] Bharatiya Sakshya Adhiniyam 2023