
ARTIFICIAL INTELLIGENCE-GENERATED EVIDENCE AND DEEPFAKES UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023: RETHINKING ADMISSIBILITY AND AUTHENTICATION IN INDIAN COURTS

Varshita A, BA LLB, MKPM RV Institute of Legal Studies

ABSTRACT

The Bharatiya Sakshya Adhiniyam, 2023 ("BSA") replaced the Indian Evidence Act, 1872 with effect from 1 July 2024, and in doing so modernised the statutory treatment of electronic records through Sections 61 to 63. These provisions were, however, drafted against the backdrop of conventional electronic evidence such as emails, call records and CCTV footage, and not against a landscape increasingly populated by generative artificial intelligence and deepfakes. This paper undertakes a doctrinal examination of the BSA's electronic evidence framework, traces its evolution from Section 65B of the erstwhile Evidence Act through the landmark decisions in *Navjot Sandhu*, *Anvar P.V.* and *Arjun Panditrao*, and evaluates whether the certificate-based authentication model under Section 63(4) is adequate to test the veracity of AI-generated content. Using the 2023 Rashmika Mandanna deepfake incident as an illustrative reference point, the paper argues that the BSA authenticates the process of production of an electronic record but not the truth of what that record depicts, leaving a doctrinal gap that ordinary criminal law provisions were not designed to close. The paper concludes with recommendations for statutory amendment, the creation of a dedicated forensic authority, a burden-shifting evidentiary rule, and judicial capacity building.

Keywords: Bharatiya Sakshya Adhiniyam 2023; Electronic Evidence; Artificial Intelligence; Deepfake; Admissibility; Digital Forensics.

1. Introduction

The manner in which Indian courts encounter and evaluate evidence has been transformed by the pervasive use of digital technology. Emails, WhatsApp conversations, CCTV recordings, call detail records, GPS data and social media posts now routinely form the evidentiary backbone of both civil and criminal proceedings. Recognising this shift, Parliament enacted the Bharatiya Sakshya Adhiniyam, 2023, which came into force on 1 July 2024 and replaced the Indian Evidence Act, 1872 in its entirety, updating the statutory architecture governing the admissibility of electronic records.

At the same time, the rapid diffusion of generative artificial intelligence has introduced an entirely new category of digital material into circulation: synthetic audio, video and images that are visually and aurally indistinguishable from authentic recordings, commonly referred to as deepfakes. Unlike earlier forms of digital manipulation, which typically left detectable traces, contemporary generative models can fabricate a person's voice, face and mannerisms with a degree of realism that challenges even trained observers.¹

India received an early demonstration of this risk in November 2023, when a fabricated video of the actress Rashmika Mandanna, generated using AI-based imaging techniques, circulated widely on social media. The individual responsible was eventually identified and prosecuted, but the episode was resolved through general provisions of the Information Technology Act, 2000 and the Indian Penal Code, 1860 rather than through any evidentiary or criminal provision specifically designed for synthetic media.²

The stakes of getting this analysis right are not merely academic. Electronic evidence now touches nearly every category of litigation before Indian courts -- criminal trials involving fabricated confessions or alibi footage, matrimonial disputes turning on intercepted messages, employment litigation resting on recorded conversations, and commercial disputes decided on the strength of digital transaction records. A framework that cannot reliably distinguish authentic digital material from convincingly fabricated synthetic media therefore places at risk the epistemic foundation on which adjudication itself depends.

¹Sakshi Tripathi, 'AI-Generated Evidence in Indian Courts: Admissibility and Legal Challenges' (Law Jurist, 2 July 2025).

²The deepfake video of actress Rashmika Mandanna surfaced in November 2023; the creator was subsequently traced and charged under provisions of the Information Technology Act, 2000 and the Indian Penal Code, 1860.

This paper asks a narrower but pressing question: does the electronic evidence framework introduced by the BSA 2023 possess the doctrinal tools necessary to test the authenticity of AI-generated content, or does it merely re-enact, in updated language, a model of authentication that was designed for a pre-generative-AI world? The paper proceeds in eight further parts. Part 2 sets out the objectives and methodology. Part 3 traces the evolution of electronic evidence law in India. Part 4 analyses the statutory framework under the BSA 2023. Part 5 surveys the relevant judicial trajectory. Part 6 examines the specific challenge posed by deepfakes. Part 7 identifies the resulting gaps, and Part 8 offers recommendations, before Part 9 concludes.

2. Research Objectives and Methodology

This study adopts a doctrinal and analytical method, relying on primary sources such as the Bharatiya Sakshya Adhiniyam, 2023, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and relevant judicial decisions, supplemented by secondary literature including law journal articles, legal commentary and contemporaneous news reporting up to mid-2026. The specific objectives of the paper are: (i) to trace the statutory evolution of electronic evidence law in India from the Indian Evidence Act, 1872 to the BSA 2023; (ii) to analyse the certification-based authentication model contained in Sections 61 to 63 of the BSA; (iii) to examine the judicial approach to electronic evidence, including the most recent pronouncement in *Pune Bar Association v Union of India*; (iv) to assess the specific doctrinal and practical challenges posed by AI-generated evidence and deepfakes; and (v) to propose legislative, institutional and procedural reforms capable of addressing the identified gaps.

3. From the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023

The admissibility of electronic records in Indian courts was first placed on a statutory footing through the Information Technology Act, 2000, which inserted Section 65B into the Indian Evidence Act, 1872. Section 65B permitted a "computer output" to be treated as a document, provided that specified conditions relating to the regular use and proper functioning of the computer were satisfied, and provided further that the output was accompanied by a certificate identifying the record and the device used to produce it.³

The interpretation of Section 65B generated over a decade of judicial disagreement. In *State*

³Information Technology Act 2000, s 92, inserting s 65B into the Indian Evidence Act, 1872.

(NCT of Delhi) v Navjot Sandhu, the Supreme Court permitted electronic records to be proved through the general provisions on secondary evidence even without a Section 65B certificate, effectively creating an alternative route to admissibility. This position was overruled in Anvar P.V. v P.K. Basheer, where the Court held that Section 65B constituted a complete code and that compliance with its certification requirement was mandatory wherever a party sought to rely on a computer output rather than the original device.⁴

The rigidity of this position produced its own practical difficulties, particularly where the certifying custodian of the device was unwilling or unavailable to furnish a certificate. In Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal, a three-judge bench reaffirmed the mandatory nature of the certificate but clarified that it could be produced at any stage of the proceedings, including during trial, thereby offering some procedural relief without disturbing the substantive requirement.⁵

It is against this jurisprudential backdrop that the Bharatiya Sakshya Adhiniyam, 2023 was enacted, alongside the Bharatiya Nyaya Sanhita, 2023 and the Bharatiya Nagarik Suraksha Sanhita, 2023, as part of a wider recodification of India's criminal law statutes. The BSA came into force on 1 July 2024 and replaced the 1872 Act in its entirety, retaining the broad architecture of the erstwhile Section 65B while introducing refinements addressed to contemporary forms of digital communication.⁶

4. Statutory Framework Governing Electronic Records under the BSA 2023

Section 57 of the BSA recognises electronic and digital records as falling within the definition of "document", placing them on the same footing as paper records for evidentiary purposes. Section 61 goes further, providing that nothing in the Adhiniyam shall be used to deny the admissibility of an electronic or digital record merely on the ground of its electronic character, and that such a record shall, subject to Section 63, carry the same legal effect, validity and enforceability as any other document.⁷

Section 62 provides that the contents of an electronic record may be proved in accordance with

⁴State (NCT of Delhi) v Navjot Sandhu alias Afsan Guru (2005) 11 SCC 600; Anvar P.V. v P.K. Basheer (2014) 10 SCC 473.

⁵Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1.

⁶The Bharatiya Sakshya Adhiniyam, 2023 was enacted together with the Bharatiya Nyaya Sanhita, 2023 and the Bharatiya Nagarik Suraksha Sanhita, 2023 as part of the recodification of India's criminal law statutes.

⁷Bharatiya Sakshya Adhiniyam 2023, ss 57 and 61.

Section 63, which sets out the operative conditions for admissibility. A "computer output" is admissible without production of the original device where it is shown that the output was produced by a computer or communication device that was in regular use, that the relevant information was fed into it in the ordinary course of activities, that the device was operating properly, and that the output accurately reproduces the information so fed.

Notably, Section 63 expands the scope of the erstwhile Section 65B by extending coverage to information stored in semiconductor memory, in addition to optical and magnetic media, and by explicitly bringing "any communication device" -- including smartphones -- within its ambit. This is a meaningful modernisation given the centrality of mobile messaging platforms to contemporary litigation.⁸

The most significant refinement, however, lies in Section 63(4), which mandates a dual certification process. The certificate accompanying the electronic record must now be furnished in two parts, as prescribed in the Schedule to the Act: Part A, to be completed by the person in charge of the device, and Part B, to be completed by an expert. In addition, the certificate must specify a hash value -- a unique numeric identifier generated through a cryptographic algorithm -- to demonstrate that the record has not been altered since its creation.⁹

Commentators have observed that Section 61 was deliberately inserted to correct what many considered an overly rigid reading of Section 65B in *Arjun Panditrao*, by clarifying that a copy of an electronic record may also be proved through the ordinary modes available for proving any other document, and that the certificate-based route under Section 63 is an enabling mechanism rather than the sole permissible pathway to admissibility.¹⁰

5. Judicial Trajectory: Consolidating Procedural Safeguards

The most recent significant pronouncement on this framework is the Supreme Court's decision in *Pune Bar Association v Union of India*, decided in May 2026, in which the constitutional validity of Section 63(4) was upheld. The Court emphasised that the requirement of hash-value disclosure is not a mere technicality but a substantive safeguard against manipulation, cloning

⁸Bharatiya Sakshya Adhiniyam 2023, s 63(1)-(3).

⁹Bharatiya Sakshya Adhiniyam 2023, s 63(4) and the Schedule (Certificate, Parts A and B).

¹⁰Saji Koduvath, "Nothing In This Adhiniyam Shall Apply To Deny The Admissibility" - New Provision (s 61, BSA)' (Indian Law Live, 5 April 2026).

and fabrication of digital records, a category of risk that the Court recognised as being magnified by sophisticated AI-generated content. The Court further clarified that persons notified as Examiners of Electronic Evidence under Section 79A of the Information Technology Act, 2000 are not the only competent experts capable of testifying to the authenticity of electronic records; courts retain discretion to rely on other qualified experts, provided their methodology withstands judicial scrutiny.¹¹

Lower courts, too, have signalled caution in the treatment of electronic material. In *Virender Kumar v State of Himachal Pradesh*, the High Court cautioned against relying on electronic evidence without independent corroboration, holding that such evidence must be critically scrutinised and its authenticity affirmatively established before it can found a conviction.¹²

What emerges from this trajectory is a consistent judicial emphasis on tightening the procedural safeguards surrounding the production and certification of electronic records. What has not yet emerged, however, is any authoritative pronouncement that squarely addresses the admissibility of AI-generated or synthetic media as a distinct evidentiary category, leaving a doctrinal vacuum precisely where the risk of fabrication is most acute.¹³

6. The Deepfake Dilemma: A Content-Authenticity Gap

A deepfake may be understood as synthetic audio-visual content, typically generated using generative adversarial networks or diffusion models, that simulates the appearance, voice or actions of a real individual with a degree of realism sufficient to mislead an ordinary viewer or listener. What makes deepfakes analytically distinct from earlier forms of digital evidence is the nature of the risk they pose: conventional electronic evidence law is preoccupied with establishing that a record has not been tampered with after its creation, whereas a deepfake may be entirely "untampered" in this technical sense -- the file itself may never have been altered -- while nonetheless depicting events that never occurred.

This distinction exposes a structural limitation in the BSA's certificate-based model. The certificate under Section 63(4) authenticates the regularity of the device and the integrity of the process by which the record was produced; it does not, and was never designed to, authenticate

¹¹*Pune Bar Association v Union of India* (Supreme Court of India, May 2026).

¹²*Virender Kumar v State of Himachal Pradesh* (2019) HPHC.

¹³See generally, 'Admissibility and Authentication of Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023' (Mondaq, June 2026).

the veracity of the underlying events that the record purports to depict. A deepfake video generated on a properly functioning device and transmitted without subsequent alteration could, in principle, satisfy every condition of Section 63 while still constituting a wholly fabricated account of reality.¹⁴

The 2023 Rashmika Mandanna episode remains instructive precisely because of how it was resolved: the perpetrator was prosecuted under general provisions of the Information Technology Act and the Indian Penal Code, and not under any provision purpose-built to address the fabrication or evidentiary misuse of AI-generated media. This illustrates the broader pattern whereby India's legal response to deepfakes has, thus far, been reactive and dependent on statutes never drafted with generative AI in contemplation.¹⁵

Within the criminal law, Section 192 of the Bharatiya Nyaya Sanhita, 2023 punishes the fabrication of false evidence, but this provision predates the era of synthetic media and does not specifically criminalise the creation of a deepfake for the purpose of deceiving a court.¹⁶

Similarly, Sections 66C, 66D, 66E, 67 and 67A of the Information Technology Act, 2000 -- addressing identity theft, impersonation, privacy violations and obscene or sexually explicit content respectively -- can be stretched to cover some instances of deepfake misuse, but each was framed for a pre-deepfake technological environment and addresses only fragments of the harm that synthetic media can cause.¹⁷

A further regulatory layer has emerged through the Information Technology (Intermediary Guidelines) Rules, 2026, which impose labelling and traceability obligations on synthetic and AI-generated content circulated through online platforms. While primarily conceived as a content-moderation measure, these obligations carry direct evidentiary significance, since compliant labelling and traceability metadata could, in principle, assist courts and litigants in testing the provenance of digital material tendered as evidence.¹⁸

At a practical level, the detection of sophisticated deepfakes requires specialised capabilities -

¹⁴Bharatiya Sakshya Adhiniyam 2023, s 63(4); the certificate attests to the regularity of the device and the process of production, not to the veracity of the events recorded.

¹⁵See note 3 above.

¹⁶Bharatiya Nyaya Sanhita 2023, s 192 (fabricating false evidence).

¹⁷Information Technology Act 2000, ss 66C, 66D, 66E, 67 and 67A.

¹⁸Information Technology (Intermediary Guidelines) Rules 2026, labelling and traceability obligations for synthetic and AI-generated content.

- frame-level inconsistency analysis, biometric liveness detection and metadata forensics -- that are not uniformly available across India's forensic science laboratories, nor are they capabilities that judicial officers can be expected to independently evaluate without expert assistance.¹⁹

6.1 A Brief Comparative Note

India is not alone in confronting this challenge. Several jurisdictions have begun experimenting with disclosure obligations for AI-generated content in litigation, and with mandatory labelling of synthetic media at the point of creation or publication, rather than relying solely on after-the-fact forensic detection at trial. The underlying regulatory instinct in these approaches is to shift part of the authentication burden upstream -- to the platforms and tools that generate or host synthetic content -- rather than leaving courts to reconstruct provenance long after a deepfake has entered circulation. India's own Information Technology (Intermediary Guidelines) Rules, 2026 move in this direction for content moderation purposes, but, as noted above, have not yet been formally linked to the evidentiary provisions of the BSA. A more deliberate alignment between platform-level labelling obligations and courtroom authentication standards would allow India to draw on this emerging international practice without requiring wholesale statutory redesign.

7. Gaps in the Current Framework

Drawing together the analysis above, at least four distinct gaps may be identified. First, the BSA contains no provision addressing the allocation of the burden of proof once the authenticity of AI-generated content is credibly challenged; it remains unclear whether the burden should fall on the party tendering the evidence to affirmatively establish its authenticity, or on the challenger to demonstrate fabrication. Second, the certificate contemplated under Section 63(4) verifies the integrity of the recording process and the device used, but does not require any independent forensic verification of the content itself, leaving a category of evidence that is procedurally compliant yet substantively unreliable. Third, neither the BSA, the Information Technology Act, nor the Bharatiya Nyaya Sanhita contains a statutory definition of "deepfake" or "synthetic media", a definitional vacuum that complicates both prosecution and adjudication. Fourth, institutional capacity remains uneven: although the Supreme Court in *Pune Bar Association* widened the pool of experts competent to testify on

¹⁹Deepfake detection ordinarily requires frame-level inconsistency analysis, biometric liveness detection and metadata forensics, capacities that remain unevenly distributed across Indian forensic laboratories.

electronic evidence, no minimum technical standards for AI-forensic competence have yet been prescribed.

It may also be noted that while the National Forensic Sciences University Act, 2020 established a dedicated institution for forensic science education and research, no equivalent statutory authority currently exists with a specific mandate to standardise the certification of AI-generated or synthetic content.²⁰

8. Recommendations

Four sets of reforms are proposed. First, at the legislative level, Section 63 of the BSA could be supplemented with a dedicated sub-provision governing electronic records suspected or alleged to be AI-generated or synthetically altered, requiring an additional layer of forensic certification distinct from the existing device-based certificate under Section 63(4). Second, at the institutional level, the establishment of a dedicated national authority -- whether as a wing of an existing forensic institution or as a freestanding body -- tasked with standardising deepfake-detection protocols and accrediting examiners would address the current absence of uniform technical benchmarks.

Third, at the procedural level, a rebuttable-presumption model is worth considering: where a credible, evidence-based challenge to the authenticity of digital content is raised, the burden could shift to the party tendering the evidence to affirmatively establish its authenticity through forensic means, rather than requiring the challenging party to prove fabrication from a position of informational disadvantage.²¹

Fourth, sustained judicial capacity building is required. Judicial officers need not become technologists, but structured training on the capabilities and limitations of generative AI and deepfake-detection tools would materially improve courts' ability to evaluate expert testimony critically. Finally, the labelling and traceability obligations introduced under the Information Technology (Intermediary Guidelines) Rules, 2026 should be formally integrated into the evidentiary framework, so that compliance or non-compliance with these obligations becomes a recognised factor in assessing the authenticity of digital material tendered in court.

²⁰National Forensic Sciences University Act 2020 established a dedicated forensic-science university, but no equivalent statutory authority currently exists for AI-content certification.

9. Conclusion

The Bharatiya Sakshya Adhiniyam, 2023 represents a genuine modernisation of India's electronic evidence law, consolidating decades of judicial disagreement over Section 65B into a clearer statutory scheme and introducing meaningful safeguards such as dual certification and mandatory hash-value disclosure. Yet this framework remains, at its core, a device-centric model of authentication: it is designed to verify that a record was produced by a properly functioning device through a regular process, not to verify the truth of what that record depicts. Generative artificial intelligence exposes precisely this limitation, since a deepfake may satisfy every procedural safeguard the BSA prescribes while remaining entirely fabricated in substance. Bridging this gap will require coordinated action across three fronts -- legislative amendment to address content-level authenticity, institutional investment in forensic capacity, and procedural innovation in the allocation of the burden of proof -- failing which Indian courts risk confronting deepfake-driven miscarriages of justice without the doctrinal tools necessary to guard against them.

References

Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

Bharatiya Nyaya Sanhita, 2023 (India).

Bharatiya Sakshya Adhiniyam, 2023 (India).

Information Technology Act, 2000 (India).

Information Technology (Intermediary Guidelines) Rules, 2026 (India).

Koduvath, S. (2026, April 5). "Nothing in this Adhiniyam shall apply to deny the admissibility" -- New provision (s 61, BSA). Indian Law Live. <https://indianlawlive.net>

Mondaq. (2026, June). Admissibility and authentication of electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023: Legal framework and emerging challenges. <https://www.mondaq.com>

Mondaq. (2026, March 24). Deepfakes as evidence: Authenticity, chain of custody and Section 65B in the age of IT Rules 2026. <https://www.mondaq.com>

National Forensic Sciences University Act, 2020 (India).

Pune Bar Association v. Union of India (Supreme Court of India, May 2026).

State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru, (2005) 11 SCC 600.

Tripathi, S. (2025, July 2). AI-generated evidence in Indian courts: Admissibility and legal challenges. Law Jurist. <https://lawjurist.com>

Virender Kumar v. State of Himachal Pradesh (2019) HPHC.