ARTIFICIAL INTELLIGENCE AS EVIDENCE IN INDIAN COURTS: CHALLENGES UNDER THE BHARATIYA SAKSHYA ADHINIYAM 2023

Ruposri Biswas*

"sākṣya — 'that which is seen with one's own eyes' — and the evidentiary problem of a witness with no eyes."

ABSTRACT

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) replaced the Indian Evidence Act, 1872 from 1 July 2024, with the stated goal of bringing India's evidence law into the digital age. But when you look closely at its key innovations, especially the dual-certification system for electronic records under Section 63, it becomes clear they were built with CDs, emails, call records, and CCTV footage in mind, not the challenges that generative AI has now, like deepfakes, cloned voices, algorithmic risk-scoring tools, and AI-generated transcripts or translations. This paper argues that Section 63 (on electronic evidence) and Section 39 (on expert opinion) offer a useful doctrinal starting point for dealing with AI-generated evidence, but they fall short. Both provisions assume a fairly straightforward recording process, with a real person who can vouch for its accuracy. That assumption doesn't hold for generative AI outputs, which have no original 'ground truth' to compare them against.

To make this case, the paper traces how Indian courts have handled electronic evidence so far, looks at the newer but conceptually separate body of deepfake personality-rights injunctions, and draws comparisons with reliability-gatekeeping frameworks used in the US, UK, and EU. It highlights a real doctrinal gap between how India treats deepfakes as a tort issue versus as an evidentiary one, and proposes concrete reforms: a dedicated AI-content certification clause under Section 63(4), formal recognition of "AI Forensic Examiners" under Section 39, and a

*BBA LLB (HONS), THIRD YEAR, PRESIDENCY UNIVERSITY, BANGALORE.

structured reliability framework inspired by the Daubert standard and the bias-audit reasoning in R (Bridges) v Chief Constable of South Wales Police.

Keywords: Electronic Evidence, Deepfakes, Expert Evidence, Forensic Examiners.

INTRODUCTION

The Bharatiya Sakshya Adhiniyam 2023 came into force on 1 July 2024, replacing the Indian Evidence Act 1872 in its entirety, alongside the Bharatiya Nyaya Sanhita, 2023 and the Bharatiya Nagarik Suraksha Sanhita 2023.[1] The Statement of Objects and Reasons accompanying the BSA situates the reform in the need to account for electronic and digital records, and the Act's drafting reflects a genuine, if incremental, attempt to modernise the evidentiary architecture inherited from 1872.

That modernisation, however, was conceived before generative artificial intelligence deepfakes, synthetic voice cloning, large-language-model-generated text, and algorithmic risk-assessment tools entered the legislative and judicial conversation in India. This is the central claim this paper develops: the BSA's admissibility architecture, principally section 63, was built to authenticate *records of things that happened,* like a call, a message, a document, a photograph. AI evidence frequently involves *inferences or generations*, content that never corresponded to any real-world event (a deepfake), or a probabilistic output with no single identifiable operator who can meaningfully certify its accuracy (a machine-learning risk score). This doctrinal mismatch between a certification model built for deterministic recording devices and the probabilistic, generative nature of AI output is the structural problem this paper surfaces and seeks to address.

The etymology of the statute's own name is instructive. ‘Sakshya’ derives from the Sanskrit *sākṣin*, one who sees with one's own eyes; a term that captures the perception-based foundation of classical evidence law. Generative AI, by contrast, has no eyes: it does not perceive and report an event but manufactures an output whose relationship to any underlying reality may be tenuous or absent. A legal architecture built around the credibility of a perceiving witness or a mechanically recording device is necessarily strained when the thing being evaluated was never perceived by anyone or anything at all.

[1] Bharatiya Sakshya Adhiniyam 2023, s 1.

This paper proceeds in six further parts. Part 2 develops a working typology of AI-generated evidence. Part 3 maps the relevant BSA provisions- sections 63 and 39- against the fifteen-year trajectory of Indian case law on electronic evidence. Part 4 identifies three distinct failure points: authenticity, admissibility and reliability at which the existing framework strains under AI evidence. Part 5 surveys comparative reliability-gatekeeping models in the United States, the United Kingdom and the European Union. Part 6 argues for dedicated AI forensic standards in India and Part 7 sets out concrete recommendations for legislative and judicial reform.

UNDERSTANDING AI-GENERATED EVIDENCE: A TYPOLOGY

"AI evidence" is not a single doctrinal category; it names at least four distinct phenomena, each raising a different evidentiary problem, and any analysis that treats them as interchangeable risks conflating problems that require different legal responses.

First, AI-generated content offered as evidence: deepfake video or audio, synthetic images, AI-written text, and voice clones raises what may be called the fabrication problem: the content purports to depict or record something that did not occur.

Second, AI-assisted analysis of evidence: facial-recognition matching, gait analysis, predictive-policing outputs, and AI forensic tools that authenticate or interpret other evidence, raising the reliability or "black-box" problem: the output may be accurate, but its underlying process is often opaque even to its own developers, and its error rate may be unknown or unknowable to the court.

Third, AI as a record-keeping or transcription tool: AI transcription of hearings, AI-translated documents, AI-drafted contracts raises an accuracy and hearsay problem: the tool intermediates between an original utterance or document and the record tendered in court, and any errors it introduces may go undetected precisely because the tool is presumed neutral.

Fourth, adversarial AI evidence: material tampered with or generated specifically to defeat detection raises an authentication-burden problem, since the very techniques used to verify digital evidence (hash comparison, metadata analysis) can themselves be spoofed by a sufficiently capable adversary.

For comparative definitional rigour, the European Union's Artificial Intelligence Act supplies a horizontal definition of an "AI system" as software developed with machine-learning or logic- and knowledge-based approaches that can, for a given set of human-defined objectives,

generate outputs such as content, predictions, recommendations or decisions influencing the environments they interact with.[2] While not binding on Indian courts, this definition is a useful anchor because it makes explicit what Indian law does not yet define at all: there is presently no statutory definition of "artificial intelligence," "deepfake" or "synthetic media" anywhere in the BSA, the Information Technology Act 2000, or the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 a gap addressed further in Part 6.

LEGAL FRAMEWORK UNDER THE BHARATIYA SAKSHYA ADHINIYAM 2023

The Electronic Evidence Gateway: Section 63: Section 63(1) BSA deems the output of a computer or communication device to be a "document," admissible without production of the original, provided the conditions specified in the section are satisfied as a *non obstante* clause carried over, with modification, from section 65B(1) of the Indian Evidence Act, 1872.[3] Sections 63(2)–(3) restate the old conditions of regular use and proper functioning of the device, with the express addition of "communication device" alongside "computer," placing beyond doubt that mobile telephones fall within the gateway without requiring the interpretive stretching that characterised litigation under the 1872 Act.

The most significant textual departure is section 63(4), which introduces a dual-certification requirement: a Part A certificate from the person in charge of the device, and a Part B certificate from an expert.[4] This is a meaningful advance on section 65B(4) of the 1872 Act, which required only a single operator certificate, and it is the strongest textual indication that the BSA already contemplates a role for technical scrutiny of digital evidence, a foundation this paper argues should be extended explicitly to AI-content authentication. Relatedly, the Schedule requires a hash value to be furnished with the certificate, a more rigorous requirement than the pre-2023 regime. A hash value, however, can only establish that a file has not been altered *after* creation; it says nothing about whether the file's content was itself synthetically generated in the first place. This limitation is central to the authenticity problem discussed in Part 4.

[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 2024/1689, art 3(1).
[3] Bharatiya Sakshya Adhiniyam 2023, s 63(1); Indian Evidence Act 1872, s 65B(1) (as repealed).
[4] Bharatiya Sakshya Adhiniyam 2023, s 63(4) and Schedule.

Expert Opinion: Section 39: Section 39 BSA carries forward the mechanism of the "Examiner of Electronic Evidence," linked to section 79A of the Information Technology Act, 2000, whose opinion on electronic or digital records is treated as a relevant fact.[5] There is presently no statutorily recognised category of expert specifically tasked with AI-content forensic examination, for instance, of a notified deepfake-detection specialist. Section 39 could in principle be read purposively to include AI-forensic examiners within its existing language, but the safer and more durable route, developed in Part 7, is an express amendment or fresh notification creating that category by name.

The Case Law Baseline: Although decided under section 65B of the 1872 Act, the following line of Supreme Court authority establishes the interpretive baseline that will, by continuity of drafting, carry over to section 63 of the BSA, and any account of AI evidence in India must begin from it.

In *State (NCT of Delhi) v Navjot Sandhu alias Afsan Guru*, the Supreme Court held that electronic records could be proved by secondary evidence under sections 63 and 65 of the 1872 Act even in the absence of a section 65B certificate, a position subsequently overruled.[6] In *Anvar PV v PK Basheer*, a three-judge bench overruled *Navjot Sandhu* on this point, holding that sections 65A–65B constitute a complete code and that, applying the maxim *generalia specialibus non derogant*, the special provisions governing electronic records displace the general law of secondary evidence.[7] A division bench in *Shafhi Mohammad v State of Himachal Pradesh* purported to relax the certification requirement where a party had no control over the relevant device, a position later held to be per incuriam.[8] The matter was authoritatively resolved by a three-judge bench in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, which reaffirmed *Anvar* as correctly decided, overruled *Shafhi Mohammad*, and clarified that a section 65B(4) certificate is a condition precedent to admissibility of an electronic record led as secondary evidence, save where the original device itself is produced and proved as primary evidence.[9]

This fifteen-year doctrinal struggle over who must certify an electronic record, and when, will reopen with AI evidence but on harder terms. An operator can certify that a device functioned

[5] Bharatiya Sakshya Adhiniyam 2023, s 39; Information Technology Act 2000, s 79A.
[6] State (NCT of Delhi) v Navjot Sandhu alias Afsan Guru (2005) 11 SCC 600 (SC) [150].
[7] Anvar PV v PK Basheer (2014) 10 SCC 473 (SC) [19]–[24] (Kurian Joseph J).
[8] Shafhi Mohammad v State of Himachal Pradesh (2018) 2 SCC 801 (SC).
[9] Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1 (SC).

properly; no one can meaningfully certify that a generative model's output is *accurate*, because there is no ground truth against which to check it. The section 63(4) certification model assumes a deterministic recording process; generative AI does not fit that assumption, and this is the doctrinal mismatch this paper treats as its central analytical claim.

CHALLENGES OF AUTHENTICITY, ADMISSIBILITY, AND RELIABILITY

Authenticity: Deepfakes are, by design, engineered to defeat precisely the test that sections 63(2)–(3) BSA pose: whether the device was functioning properly. A deepfake may be recorded on a perfectly functioning device; the falsity lies entirely in the content, not in the recording process. This is a structural blind spot in the certification model, not a mere evidentiary gap that better forensic tools alone can close.

Indian courts have, in a distinct civil register, already begun grappling with the harm side of this problem. In *Anil Kapoor v Simply Life India*, the Delhi High Court restrained the unauthorised use of the plaintiff's persona through deepfake and AI-based tools, expressly identifying face-swap technology as a distinct category of harm to personality rights.[10] In *Ankur Warikoo v John Doe*, the Delhi High Court granted a John Doe injunction against AI-generated deepfake videos and voice clones used to perpetrate investment fraud, directing takedown and disclosure of identifying user data.[11] Personality-rights orders obtained by Aishwarya Rai Bachchan and Abhishek Bachchan in September 2025 similarly restrained AI and deepfake manipulation of image and likeness, grounding protection in Article 21 of the Constitution.[12] Most recently, in May 2026, the Delhi High Court granted an interim injunction restraining AI-generated deepfakes falsely attributing political statements to Shashi Tharoor.[13]

It bears emphasis that every one of these orders is a civil, interim injunction granted on a prima facie/balance-of-convenience standard, protecting personality and dignity rights under Article 21. Not one of them is a ruling on the evidentiary admissibility of a deepfake tendered as substantive proof in a criminal trial, or as documentary evidence going to the merits of a civil

[10] Anil Kapoor v Simply Life India CS(COMM) 652/2023, Delhi HC, order dated 20 September 2023 (Prathiba M Singh J).
[11] Ankur Warikoo v John Doe, Delhi HC (2024) (precise CS(COMM) number to be confirmed from the Delhi High Court e-filing portal before final submission).
[12] Aishwarya Rai Bachchan and Abhishek Bachchan personality-rights orders, Delhi HC, September 2025 (Tejas Karia J) (CS(COMM) numbers to be confirmed before final submission).
[13] Shashi Tharoor v [Defendants], Delhi HC, May 2026 (Mini Pushkarna J) (CS(COMM) number to be confirmed before final submission).

suit. This distinction is the central doctrinal gap this paper identifies: Indian courts presently possess a body of deepfake *tort* jurisprudence, but no deepfake *evidence* jurisprudence.

Admissibility: Applying *Anvar* and *Arjun Panditrao* by analogy, AI-generated content tendered as an electronic record must satisfy the dual certification demanded by section 63(4). But the provision presupposes an identifiable "person in charge of the computer," a category that maps poorly onto a cloud-hosted generative model operated by a third-party AI company with no meaningful presence or record-keeping obligation within the jurisdiction. This mirrors, in sharper form, the unresolved cloud-server certification problem that commentators had already flagged in relation to call-data records even before generative AI entered the picture. A separate and arguably more coherent path is to route AI output through the expert-opinion gateway in section 39, treating a model's output the way DNA or forensic scientific evidence is treated as expert opinion requiring an independent foundation of reliability, rather than as a self-authenticating "document" under section 63.

Reliability: Even where AI-derived material clears the admissibility gateway, Indian evidence law presently has no codified reliability-gatekeeping test analogous to the four-factor test developed in the United States. Weight is assessed largely through the expert-opinion provision in section 39 without any structured threshold inquiry into testability, error rate, peer review or general acceptance, discussed further in Part 5.

Two further Supreme Court decisions bear on the reliability and integrity of digital evidence generally, and their reasoning extends naturally to unauthenticated AI evidence. In *Tomaso Bruno v State of Uttar Pradesh*, the Court considered the evidentiary value of CCTV footage and the consequences of its non-production, illustrating a judicial willingness to draw adverse inferences from missing or unreliable digital evidence.[14] In *P Gopalkrishnan v State of Kerala*, the Court addressed the need to maintain the integrity of electronic records during storage and production, a principle directly relevant to chain-of-custody arguments for AI evidence, where provenance tracking from generation to production is at least as important as the more familiar question of storage integrity.[15]

[14] Tomaso Bruno v State of Uttar Pradesh (2015) 7 SCC 178 (SC).
[15] P Gopalkrishnan v State of Kerala (2020) 9 SCC 161 (SC).

COMPARATIVE APPROACHES

United States: The Reliability-Gatekeeping Model: The United States has developed the most fully worked-out reliability-gatekeeping model among comparable jurisdictions. *Frye v United States* established a "general acceptance" test, admitting expert scientific evidence only where the underlying technique had gained general acceptance in the relevant scientific community.[16] The Federal Rules of Evidence subsequently displaced *Frye*, and in *Daubert v Merrell Dow Pharmaceuticals Inc* the Supreme Court laid down a flexible, multi-factor reliability inquiry, testability or falsifiability, peer review and publication, known or potential error rate, the existence of standards controlling the technique's operation, and general acceptance for trial judges acting as gatekeepers under Federal Rule of Evidence 702.[17] In *Kumho Tire Co Ltd v Carmichael*, the Court extended this gatekeeping function from purely scientific testimony to all expert testimony, including technical or specialised testimony, a holding directly analogous to expert testimony concerning an AI system's operation.[18] The *Daubert* factors of error rate and testability map with unusual precision onto what a workable "AI forensic standard" should demand of a deepfake-detection tool or an algorithmic risk-assessment system before a court relies upon it, and this paper treats *Daubert* as the primary comparative template for Part 7's recommendations.

United Kingdom: English law has no single codified reliability test equivalent to *Daubert*; admissibility of computer-derived evidence was historically governed by common-law principles and by section 69 of the Police and Criminal Evidence Act 1984, which created a presumption that computer evidence had functioned correctly, a provision repealed in 1999 as unworkable in practice.[19] This is a cautionary comparative precedent: the BSA's section 63 certification model bears a structural resemblance to the pre-1999 UK approach that Britain itself abandoned as unadministrable, and India would do well to learn from that history rather than repeat it. The Law Commission of England and Wales subsequently recommended a more structured reliability test for expert evidence in criminal proceedings, considerably closer to *Daubert* than to unstructured common-law admissibility, and offers a workable comparative model for reforming section 39 BSA.[20] More directly relevant to AI evidence specifically, the

[16] Frye v United States 293 F 1013 (DC Cir 1923) 1014.
[17] Daubert v Merrell Dow Pharmaceuticals Inc 509 US 579 (1993) 592–595.
[18] Kumho Tire Co Ltd v Carmichael 526 US 137 (1999).
[19] Police and Criminal Evidence Act 1984, s 69 (repealed by Youth Justice and Criminal Evidence Act 1999, s 60).
[20] Law Commission, Expert Evidence in Criminal Proceedings in England and Wales (Law Com No 325, 2011).

Court of Appeal in *R (Bridges) v Chief Constable of South Wales Police* held that police deployment of live automated facial recognition breached Article 8 of the European Convention on Human Rights and associated data-protection duties, in part because the force could not demonstrate it had taken reasonable steps to satisfy itself that the software was free of racial or gender bias.[21] This reasoning supplies a directly transplantable model for judicially mandated bias and reliability audits as a precondition to reliance on any AI tool's output.

European Union: The EU's Artificial Intelligence Act classifies AI systems by risk tier, and systems used in the administration of justice and democratic processes, including evidence evaluation and judicial research assistance, are categorised as high-risk AI systems, triggering conformity-assessment, transparency, human-oversight and logging or traceability obligations before deployment.[22] Separately, Article 22 of the General Data Protection Regulation confers a right not to be subject to a decision based solely on automated processing that produces legal effects, a useful comparator for algorithmic evidence used to found adverse legal consequences, such as a risk score influencing a bail or sentencing determination.[23]

THE NEED FOR AI FORENSIC STANDARDS IN INDIA

India presently relies on the network of Central Forensic Science Laboratories and the Information Technology Act's Examiner of Electronic Evidence framework under section 79A. Neither is equipped with a notified, court-recognised protocol for deepfake or synthetic-media detection comparable to, for instance, a forensic science regulator's codes of practice for digital forensics in a comparable jurisdiction.

Four concrete gaps follow from the analysis above. First, there is no statutory definition of "synthetic media" or "deepfake" anywhere in the BSA or the Information Technology Rules. Second, there is no notified AI-forensic examiner category under section 39 of the BSA or section 79A of the IT Act. Third, there is no mandatory disclosure requirement for the error rates or validation studies of an AI-detection tool before a court relies on it, of the kind that *Daubert* and *Bridges* together suggest is achievable. Fourth, there is no chain-of-custody protocol specific to hash-based provenance tracking, of the kind offered by existing technical

[21] R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058, [2020] 1 WLR 5037 [199]–[201].
[22] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 2024/1689, Annex III (pinpoint sub-paragraph to be confirmed against the consolidated EUR-Lex text before final submission).
[23] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, art 22.

content-provenance standards such as the Coalition for Content Provenance and Authenticity (C2PA) framework, which could be referenced or adapted by rule rather than invented afresh.

On the executive side, the Ministry of Electronics and Information Technology has issued advisories to intermediaries concerning deepfake labelling and removal obligations under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[24] These advisories are the executive-side counterpart to the evidentiary gap diagnosed in this paper: they regulate the *publication* of synthetic content, but say nothing about its treatment once tendered as *proof* in a court of law.

RECOMMENDATIONS FOR LEGISLATIVE AND JUDICIAL REFORM

1. Amend section 63(4) BSA to add a third certification limb specific to AI-generated or AI-processed content, distinct from the existing device-operator and technical-expert dual certificate, and calibrated to the fact that no operator can certify the accuracy of a generative output.

2. Statutorily recognise "AI Forensic Examiners" as a defined sub-category of expert under section 39 BSA, with notified qualification criteria, on the model of the Examiner of Electronic Evidence under section 79A of the Information Technology Act 2000.

3. Adopt a structured judicial reliability-assessment framework for AI-tool-derived evidence, drawing on the four Daubert factors of testability, peer review, known error rate, and general acceptance, to be applied at the admissibility stage and not merely as a matter going to weight.

4. Mandate disclosure of training-data provenance, validation error rates, and known bias audits for any AI tool whose output a party seeks to rely upon as evidence, modelled on the reasoning in R (Bridges) v Chief Constable of South Wales Police.

5. Extend the existing deepfake-injunction jurisprudence: the Anil Kapoor, Warikoo, Bachchan and Tharoor line of orders into a dedicated Supreme Court or High Court practice direction on the interim preservation and forensic imaging of AI-related digital evidence pending trial.

[24] Ministry of Electronics and Information Technology, advisory to intermediaries on deepfakes and synthetic content under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (exact advisory reference and rule number to be confirmed against MeitY's website before final submission).

6. Consider whether India requires an EU AI Act-style risk-tiering specifically for AI tools used within the justice system itself translation tools, predictive-policing tools, and AI transcription of testimony- given the EU's classification of comparable uses as high-risk.

CONCLUSION

The Bharatiya Sakshya Adhiniyam, 2023 modernised India's electronic-evidence gateway to dual certification, mandatory hash values, and express coverage of communication devices, but it did so looking backwards at the CD, CCTV and email problem that Indian courts had already spent a decade and a half litigating through *Navjot Sandhu*, *Anvar*, *Shafhi Mohammad* and *Arjun Panditrao*, not forward at generative artificial intelligence. The doctrinal tools formally exist in sections 39, 61, 62 and 63 of the BSA, but they were not built for content that has no ground-truth original against which it can be certified.

Comparative law offers transplantable models: the United States' Daubert reliability-gatekeeping factors, the United Kingdom's bias-audit reasoning in Bridges (and its own cautionary experience with an unworkable certification presumption under the repealed section 69 of the Police and Criminal Evidence Act 1984), and the European Union's risk-tiering of AI systems used in the administration of justice. India's own emerging deepfake-injunction case law demonstrates real judicial appetite to engage with the underlying problem but, to date, only on the harm side of the ledger, through personality-rights injunctions, and not yet on the evidence side, through a ruling that squarely addresses the admissibility of an AI-generated output tendered as substantive proof. Closing that gap, through the concrete reforms proposed in Part 7, is the task this paper commends to Parliament and to the higher judiciary alike.