ARTIFICIAL INTELLIGENCE, MACHINE LEARNING OUTPUTS AND FUTURE SCIENTIFIC EVIDENCE UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

Md Irtifa Ur Rahman, B.A.LL.B., School of Law Justice & Governance,
Gautam Buddha University, Greater Noida, U.P.

ABSTRACT

The Bharatiya Sakshya Adhiniyam, 2023 (BSA), in force since 1 July 2024, modernised Indian evidence law by placing electronic and digital records on an equal footing with paper documents. Yet the statute was drafted for records that machines store, not for conclusions that machines generate. Outputs of artificial intelligence (AI) and machine learning (ML) systems, such as facial recognition matches, predictive risk scores, voice identification, automated transcription and synthetic media detection, are probabilistic inferences produced by models whose internal reasoning is often opaque. This article examines whether, and on what terms, such outputs can be admitted and weighed under the BSA. It analyses the definitional provisions on documents and evidence, the primary evidence explanations in Section 57, the certification regime in Section 63 as upheld by the Supreme Court in Pune Bar Association v. Union of India (2026), and the expert opinion provisions in Section 39. It argues that the Section 63 certificate secures the integrity of a record but says nothing about the reliability of an algorithmic inference. Drawing on comparative jurisprudence and the literature on explainable AI, the article proposes a layered approach combining authentication, a reliability inquiry modelled on scientific-validity standards, disclosure obligations, and safeguards for the accused under Article 21 of the Constitution. It concludes with recommendations for legislative rules, forensic standards, and judicial training so that future scientific evidence strengthens rather than distorts the search for truth.

Keywords: Bharatiya Sakshya Adhiniyam 2023; artificial intelligence; machine learning; electronic evidence; expert opinion; Section 63 certificate; algorithmic reliability; deepfakes; explainability; fair trial.

Introduction

Courts have always depended on science to settle disputed facts. Fingerprints, blood grouping, ballistics and DNA profiling each entered the courtroom after a period of judicial caution. Artificial intelligence represents the next and arguably most difficult stage of this journey. Unlike earlier forensic techniques, an ML system does not apply a fixed rule devised by a human expert. It learns statistical patterns from training data and produces outputs that even its designers may be unable to fully explain (Burrell, 2016).

Indian investigating agencies already use automated facial recognition, call-data analytics and speech-to-text tools. Litigants increasingly rely on AI-generated summaries, translations and enhanced images. At the same time, generative AI can fabricate convincing audio and video, a phenomenon widely termed "deepfakes" (Chesney & Citron, 2019). Courts therefore face two linked problems: how to evaluate genuine machine inferences, and how to detect fabricated machine content.

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) replaced the Indian Evidence Act, 1872 (IEA) as part of a wider overhaul of criminal law. It expanded the treatment of electronic records but did not expressly mention AI, algorithms or machine learning. This article asks three questions. First, how do AI and ML outputs fit within the BSA's categories of evidence? Second, are the existing tools of authentication and expert opinion adequate to test their reliability? Third, what reforms are needed so that future scientific evidence is both admissible and trustworthy?

The Statutory Framework for Electronic Records under the BSA

The BSA treats electronic information as a mainstream form of proof. Section 2(1)(d) defines "document" to include electronic and digital records, and Section 2(1)(e) extends "evidence" to information given electronically (Bharatiya Sakshya Adhiniyam, 2023). Section 61 further provides that an electronic or digital record shall not be denied admissibility merely because it is in electronic form.

Section 57, through its Explanations, treats an electronic record as primary evidence when it is stored or produced from proper custody, including records stored simultaneously or sequentially in multiple files. Section 63 carries forward and tightens the old Section 65B of the IEA. Under Section 63(4), a party tendering an electronic record must file a certificate in

the form prescribed in the Schedule. Part A is signed by the person in charge of the device, while Part B is signed by an expert, and the certificate must disclose the hash value of the record.

The jurisprudence on Section 65B shaped this design. In *Anvar P.V. v. P.K. Basheer* (2014), the Supreme Court held that the certificate was a mandatory condition for admitting secondary electronic evidence. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) reaffirmed that position. Under the BSA, commentators note that the certificate has effectively become necessary for every electronic record, making the regime stricter than before (LiveLaw, n.d.).

In 2026, a three-judge bench of the Supreme Court upheld the validity of Section 63(4) in *Pune Bar Association v. Union of India*. The Court treated the hash value as an electronic fingerprint that protects integrity. It also read Sections 39(1) and 39(2) together and held that Part B need not be signed only by an Examiner of Electronic Evidence notified under Section 79A of the Information Technology Act, 2000; other qualified experts may sign it (SCC Online, 2026). This framework is a significant achievement for authenticating stored data. Whether it suffices for machine-generated inferences is the central question of this article.

The Nature of AI and ML Outputs as Evidence

Not all machine outputs raise the same evidentiary concerns. It is useful to distinguish three categories.

1. **Recorded data.** A CCTV clip, a GPS log or a server timestamp captures an event with minimal interpretation. These fit comfortably within the electronic record provisions.

2. **Processed outputs.** Automated transcription, translation or image enhancement transforms recorded data. The output is still anchored to an original, but the transformation can introduce errors.

3. **Inferential outputs.** A facial recognition "match", a voice identification score, a predicted risk level or a deepfake-detection verdict is a probabilistic conclusion. It functions much like an expert opinion, yet no human expert formed it.

Roth (2017) describes the third category as "machine testimony" because it conveys an

assertion about the world that depends on the credibility of the system. The difficulty is that the BSA has no witness to cross-examine. The Section 63 certificate confirms that the output file has not been altered after creation. It does not confirm that the model was accurate, that its training data were representative, or that it was used within its validated limits.

The opacity of ML compounds the problem. Burrell (2016) identifies three sources of opacity: corporate secrecy, technical illiteracy among users, and the inherent complexity of high-dimensional models. Rudin (2019) argues that for high-stakes decisions, inherently interpretable models should be preferred over post-hoc explanations of black boxes. These insights suggest that inferential outputs require a reliability inquiry distinct from authentication.

Admissibility and Authentication Challenges

Admissibility under the BSA turns on relevance and on compliance with the rules of proof. An AI output that tends to prove a fact in issue is relevant. If it is stored as an electronic record, it can be proved with a Section 63 certificate. On a literal reading, therefore, a facial recognition match report could be admitted on the same footing as a CCTV clip. This literal reading risks collapsing an important distinction between admissibility and weight.

Three practical gaps emerge. First, the certificate attests to the device and the hash value, not to the algorithm. A model can be poorly trained, biased or used beyond its tested conditions, and the output will still carry an accurate hash. Second, AI systems change over time. Models are retrained and updated, so the same input may yield a different result next month. Unless the model version, parameters and thresholds are recorded, the output cannot be reproduced, and the opposing party cannot test it. Third, many tools used by investigators are proprietary. Vendors may claim trade-secret protection over source code and training data, which prevents meaningful scrutiny.

The Supreme Court's reasoning in *Pune Bar Association* (2026) helps here. By recognising that qualified private experts may sign Part B, the Court widened the pool of persons who can attest to electronic evidence. The same logic can support a broader role for independent AI auditors. However, the attestation must extend beyond integrity to cover the model's identity, version, validation record and known error rates. Without this, the certificate offers false reassurance for inferential outputs.

Expert Opinion and Reliability Standards

Section 39(1) of the BSA makes relevant the opinions of persons especially skilled in foreign law, science, art or "any other field". This open phrase can accommodate data scientists and AI forensic specialists. Section 39(2) deems the Examiner of Electronic Evidence an expert for electronic records. In practice, inferential AI outputs should be introduced through such experts, who can explain how the system works, how it was validated and what its limitations are.

Indian law, however, lacks a codified test for the reliability of scientific methods. Courts generally assess expert evidence by its reasoning and corroboration rather than by a formal gatekeeping standard. The United States Supreme Court in *Daubert v. Merrell Dow Pharmaceuticals, Inc.* (1993) asked whether a technique can be tested, has been peer reviewed, has a known error rate, has operational standards, and enjoys general acceptance. These factors map well onto ML systems. A model's error rate, its performance across demographic groups and its validation on independent datasets are measurable.

Empirical research shows why such inquiry matters. Buolamwini and Gebru (2018) found that commercial gender-classification systems had markedly higher error rates for darker-skinned women than for lighter-skinned men. The ProPublica analysis of the COMPAS risk tool reported racial disparities in false-positive rates (Angwin et al., 2016). In *State v. Loomis* (2016), the Wisconsin Supreme Court allowed the use of a proprietary risk score in sentencing but required cautionary warnings about its limits. These experiences counsel that Indian courts should demand disclosure of error rates and bias testing before relying on algorithmic conclusions.

Psychological research adds a further concern. Decisionmakers tend to over-trust automated outputs, a pattern known as automation bias (Skitka et al., 1999). Judges and juries may treat a numerical score as more objective than it is. Expert testimony must therefore communicate uncertainty clearly, and courts should treat AI outputs as corroborative rather than conclusive.

Deepfakes, Fairness and the Rights of the Accused

Generative AI threatens the evidentiary value of audio-visual records themselves. Chesney and Citron (2019) warn of a "liar's dividend": once fabricated media become common, genuine

recordings can be dismissed as fake. A hash value proves that a file has not changed since certification, but it cannot prove that the file captured a real event in the first place. Courts will increasingly need provenance evidence, such as device metadata, chain of custody and content-credential standards, together with expert analysis of synthetic artefacts.

The use of AI evidence also engages constitutional rights. Article 21 guarantees a fair trial, which includes a meaningful opportunity to challenge the prosecution's evidence. In *Selvi v. State of Karnataka* (2010), the Supreme Court refused to admit compelled narco-analysis, polygraph and brain-mapping results, stressing both their doubtful reliability and the accused's right against self-incrimination. Although AI tools differ from those techniques, *Selvi* shows that courts will scrutinize novel scientific methods for both reliability and constitutional compliance.

The right to privacy recognized in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) is equally relevant. Mass facial recognition and data-mining tools process personal data on a large scale. Evidence gathered through such tools must satisfy the tests of legality, necessity and proportionality. Further, if the accused cannot access the model, its training data or its error rates, the right to cross-examination becomes illusory. Equality of arms requires that defence experts receive adequate access, under protective orders where commercial secrecy is genuinely at stake.

Recommendations

A layered approach can integrate AI evidence into the BSA without weakening its safeguards.

1. **Separate authentication from reliability.** The Section 63 certificate should continue to establish integrity. For inferential outputs, courts should additionally require a reliability showing through a Section 39 expert.

2. **Expand the certificate schedule for AI outputs.** Part B could require disclosure of the system name, model version, date of use, input data, decision thresholds and documented error rates.

3. **Adopt structured reliability factors.** Guidelines issued by the Supreme Court or through rules could list factors similar to *Daubert*: testability, validation, error rates, bias audits, peer review and acceptance in the relevant field.

4. **Ensure disclosure to the defence.** Courts should permit defence experts to examine models and validation data under protective orders, so that trade secrets do not defeat the right to a fair trial.

5. **Notify and accredit AI forensic laboratories.** The Central Government can extend Section 79A notifications to laboratories with demonstrated competence in ML validation and deepfake detection.

6. **Treat AI outputs as corroborative.** Absent strong validation, an algorithmic conclusion should not by itself sustain a conviction.

7. **Train judges and lawyers.** Judicial academies should offer modules on statistics, ML basics and automation bias, so that courts can evaluate expert testimony critically (Doshi-Velez & Kim, 2017; Gless, 2020).

Conclusion

The BSA has given India a modern framework for electronic records, and the Supreme Court's decision in *Pune Bar Association* (2026) has strengthened its integrity safeguards. Yet AI and ML outputs are not merely stored data; they are machine-made inferences. The certificate under Section 63 tells a court that a file is unchanged, not that its conclusion is correct. Reliability must therefore be tested separately, through qualified experts, transparent validation and respect for the rights of the accused. If Indian evidence law adopts this layered approach, AI can become a valuable source of future scientific evidence. If it does not, courts risk replacing human error with automated error that is harder to see and harder to challenge.

REFERENCES:

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016, May 23). *Machine bias*. ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (Supreme Court of India).

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (Supreme Court of India).

Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research, 81*, 77–91.

Burrell, J. (2016). How the machine "thinks": Understanding opacity in machine learning algorithms. *Big Data & Society, 3*(1), 1–12. https://doi.org/10.1177/2053951715622512

Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753–1820.

Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

Doshi-Velez, F., & Kim, B. (2017). *Towards a rigorous science of interpretable machine learning* (arXiv:1702.08608). arXiv. https://doi.org/10.48550/arXiv.1702.08608

Gless, S. (2020). AI in the courtroom: A comparative analysis of machine evidence in criminal trials. *Georgetown Journal of International Law, 51*(2), 195–253.

Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India).

LiveLaw. (n.d.). *How Bharatiya Sakshya Adhiniyam has transformed digital evidence*. https://www.livelaw.in/articles/bharatiya-sakshya-adhiniyam-transformed-digital-evidence-552681

Pune Bar Association v. Union of India, Writ Petition (Civil) (Supreme Court of India, 2026).

Roth, A. (2017). Machine testimony. *Yale Law Journal, 126*(7), 1972–2053.

Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence, 1*(5), 206–215. https://doi.org/10.1038/s42256-019-0048-x

SCC Online. (2026, July 8). *Hash value is an electronic fingerprint; Section 63(4) BSA certificate requirement is valid: Supreme Court*. https://www.scconline.com/blog/post/2026/07/08/sc-upholds-admissibility-of-electronic-evidence-under-section-63-4-bsa/

Selvi v. State of Karnataka, (2010) 7 SCC 263 (Supreme Court of India).

Skitka, L. J., Mosier, K. L., & Burdick, M. (1999). Does automation bias decision-making? *International Journal of Human-Computer Studies, 51*(5), 991–1006. https://doi.org/10.1006/ijhc.1999.0252

State v. Loomis, 881 N.W.2d 749 (Wis. 2016).