JOURNAL OF CYBER GOVERNANCE AND INTELLECTUAL PROPERTY

Volume 1, Issue 2 Article 6

Examining the Legal Recognition of AI-Generated Evidence in Civil Proceedings

Haarika Nadimpalli

School of Law, Mahindra University

Recommended Citation:

Nadimpalli (2026) "Examining the Legal Recognition of AI-Generated Evidence in Civil Proceedings" Journal of Cyber Governance and Intellectual Property, Vol. 1, Issue 2, Article 6. (DOI)

ABSTRACT

The use of AI in commercial, financial and interpersonal communication has made evidentiary issues in civil litigation more complicated. Traditional legal frameworks, which were designed for assessing static documents and human testimonies, are hard to process when evaluating machine-generated dynamic outputs, deepfake synthesis, predictive algorithmic reports and data compilations. The present research paper critically analyzes the legal status and admissibility of AI-generated evidence in civil proceedings, particularly the provisions of Bharatiya Sakshya Adhiniyam, 2023 (BSA) and the provisions of the Indian Evidence Act, 1872 (IEA). The study addresses the procedural issues of authentication, hearsay exceptions, opacity of algorithms (the "black box" problem), and the chain of custody. The paper examines whether the existing statutory certifications (e.g., Section 63 of the BSA, which is known by the name Section 65B of the IEA) are adequate to provide validation for machine-generated evidence without human validation. Finally, the paper suggests a special judicial procedure, new legislation that incorporates specific authentication requirements, and judicial panels of algorithmic experts to guarantee procedural fairness and protect the integrity of the evidence in civil cases.

KEYWORDS

AI-Generated Evidence, Civil Litigation, Bharatiya Sakshya Adhiniyam 2023, Authenticity, Deepfakes, Algorithmic Transparency.

INTRODUCTION

The old law of civil evidence has two tenets: materiality and personhood. The admissibility of documentary evidence has depended on finding the author of the document, tracing the chain of custody, and questioning the veracity of the document. But, with the rise of generative artificial intelligence, machine-learning analytics, and automated decision-making systems, the type of digital proof that is submitted to civil courts has changed. In today's civil actions, from loss assessment reports created by algorithms in insurance cases to audio recordings produced by AI in family law cases, or financial models created by AI in corporate valuation disputes, evidence produced in part or fully by algorithms is commonplace.

The traditional rules of evidence come into conflict with the products of the algorithms. AI-generated outputs are distinguishable from traditional electronic documents like e-mails, SMS or scanned PDFs, which are just digital depository of human thought, as they are produced autonomously, processed probabilistically and opaque system-wise. Where a deepfake is created that is convincing and completely fake, or where an AI tool is analyzing unstructured data to produce a forensic summary, the judicial system is now faced with challenges on an unprecedented scale to decide whether it is real or produced by an AI tool or malicious intent.

Indian law had envisioned the transformation of the evidentiary regime from the pre-digital era to digital era with the replacing of the old Indian Evidence Act, 1872 (IEA) by the Bharatiya Sakshya Adhiniyam, 2023 (BSA). Although the BSA expressly expands the definition of "electronic and digital records," it still deals with the output of automated and algorithmic processes with a statutory framework that is still applicable to static electronic documents. The principle of mandatory certification for electronic outputs controlled by Section 63 of the BSA (the new Section 65B of the IEA) is that electronic outputs are created by normal computers used by humans in the normal course of business. This assumption fails in the case of generative algorithms which work without explicit user guidance, or deterministic processing.

So these are questions that precede civil courts: What about “data” created by a machine that is not identifiable to a human author can it be legally deemed a “document” or “electronic record”? When the algorithms used in the underlying code are proprietary and opaque, how can a litigant prove the authenticity and reliability of an algorithmic output? What should the

court consider with respect to deepfakes in a civil case where the standard of proof applies is preponderance of the probabilities? In today's technologically-driven world, it is crucial to address these questions to preserve procedural justice, prevent apparent evidence of fraud, and ensure that the civil adjudication system remains efficient and reliable.

LITERATURE REVIEW

The law relating to civil litigation and electronic evidence has passed through various technologic ages. Early scholars gave considerable attention to setting up the fundamentals of static electronic records. Academic literature thereafter focused on the procedural requirements and compulsory certification, following the enactment of the Information Technology Act, 2000 and the insertion of Section 65A and 65B in the Indian Evidence Act, 1872. In Anvar P.V. v. P.K. Basheer[1] and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal[2] The Supreme Court of India put an end to decades of conflicting opinions by holding that the requirement of obtaining a Certificate under Section 65B was a strict condition precedent for the admissibility of secondary electronic evidence. Carnelutti and more recently Indian commentators, Ratanlal and Dhirajlal, made the point that electronic records were "digital extensions of human writing" and that the custodial log and other practices essential for ensuring that those records are not tampered with apply to electronic records as well [3].

But a major problem has emerged in the modern legal literature: traditional principles on digital evidence are based on the assumption that technology is passive. A computer that prints a bank statement, is only a medium to record human transactions. However, the current legal scholarly debate, such as George L. Paul and Stephen Mason, challenges this paradigm by conceiving of a new form of creation, namely, autonomous machine creation [4]. In his work on Electronic Evidence, Mason makes the same point about the machine-generated output: it is not easily considered hearsay and it is not necessarily presumed to be accurate just because it came from a machine [5]. Civil trials present substantial problems for cross-examination and cross-scrutiny when complex machine-learning models are used, because even the software developers may not be able to explain the exact steps in the process linking the data input to the algorithmic output of the model.

[1] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).
[2] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).
[3] Ratanlal Ranchhoddas & Dhirajlal Keshavlal Thakore, The Law of Evidence 345 (26th ed. 2017).
[4] George L. Paul, *Foundations of Digital Evidence,* 88 (2008).
[5] Stephen Mason & Daniel Seng, Electronic Evidence 112 (4th ed. 2017).

The recent academic debates on the Bharatiya Sakshya Adhiniyam, 2023 (BSA) in India's context show that the law has a long-standing oversight. Section 2(1)(t) and Section 63 of the BSA made significant strides to modernize rules for electronic evidence, allowing more types of custodians to sign electronic certificates, but scholars point out that the BSA doesn't differentiate between passive electronic storage and active AI generation [6]. The framework does not distinguish between an automated AI summary and a generative deepfake and both are still governed by the same legal definition as a static PDF or e-mail transcript. With such a statutory blackout, trial courts are left without guidance on litigating claims of algorithmic bias, hallucination or synthetic origin.

Moreover, comparative literature from other jurisdictions shows that a movement toward specialization of evidentiary rules is urgently needed. The concept of standards for "machine testimony" has become a growing point of discussion in the United States in the context of Rule 901 and Rule 702 of the Federal Rules of Evidence (FRE)[7]. Some scholars like Andrea Roth believe that a separate hearsay-adjacent framework should be developed for machine-generated outputs, which should be subjected to a thorough validation process similar to the Daubert standard for expert testimony[8] . In the same way, the EU AI Act (2024) includes requirements for transparency and auditability of high-risk applications of AI that directly inform the court's examination of the reliability of evidence[9] .

The present review suggests that, though there is good existing scholarship on passive digital evidence and overarching electronic certificates, there is a significant gap in research on how the civil courts in common law jurisdictions, such as India, should consider the admissibility, reliability and probative value of evidence created by artificial intelligence. This paper seeks to fill that void by providing a critical assessment of the existing statutory position and then to suggest practical guidelines for judges.

METHODOLOGY

The method of research used in this research is non-empirical (Doctrinal Legal Research) and uses a comparative analytical approach. The doctrinal framework will include an in-depth analysis of primary legal sources such as statutes related to the Bharatiya Sakshya Adhiniyam, 2023 (BSA); Indian Evidence Act, 1872 (BSIA); Information Technology Act,

[6] Bharatiya Sakshya Adhiniyam, 2023, §§ 2(1)(t), 63, No. 47, Acts of Parliament, 2023 (India).
[7] Fed. R. Evid. 901(b)(9).
[8] Andrea Roth, *Machine Testimony*, 98 Iowa L. Rev. 1971, 1985 (2013).
[9] 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), art. 50, 2024 O.J. (L 1689).

2000[10]; and pertinent civil procedural statutes. Precedents from the Supreme Court and High Courts are analyzed on a systematical basis to see the judicial trends and to find the existing ambiguity in the statutes with a view to understanding the existing judicial trends and gaps in the statutes.

The paper utilizes a comparative methodology in addition to the doctrinal analysis. It reviews international legislation, including the United States Federal Rules of Evidence (FRE Rules 901 and 702) and legislation from the last few years, including the European Union's Artificial Intelligence Act (2024). The evidentiary framework in India can provide useful insights into the methods used by foreign courts in matters relating to algorithmic authentication, algorithmic evaluation of complex models, and deepfake verification.

The selected methodology is suitable since the legal nature of AI-generated evidence is a question of norms and legislation. The study, through a textual, judicial and comparative analysis, assesses the current state of the law and proposes a set of well-structured proposals for the reform of the statute and judicial practice.

ANALYSIS

Classification of AI Outputs as Evidence under Evidence Law

The first question to be answered is whether the evidence produced by AI is legally admissible in civil trials. In the traditional principles of evidence, evidence falls into three categories: oral, real (physical) and documentary. A "document" under Section 2(1)(d) of the Bharatiya Sakshya Adhiniyam, 2023 (BSA)[11] has been broadly defined to mean anything expressed or described by means of any substance with the aid of letters, figures or marks, and includes electronic and digital records. Section 2(1)(t) also provides a definition of "electronic record" as data, record or data created, image or sound stored, received or sent in an electronic form.[12]

The technical nature of an "electronic record" presents a significant conceptual conundrum: although an AI-generated output, such as an auto-generated data summary, a predictive financial valuation, or synthetically altered image, may manifest physically as a digital file, it remains technically an "electronic record. The traditional electronic records are deterministic and represent a human representation; an e-mail or a digital record entry is nothing but a human expression, recorded electronically. In contrast, generative AI has probabilistic and

[10] Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).
[11] Bharatiya Sakshya Adhiniyam, 2023, § 2(1)(d), No. 47, Acts of Parliament, 2023 (India).
[12] Bharatiya Sakshya Adhiniyam, 2023, § 2(1)(t), No. 47, Acts of Parliament, 2023 (India).

non-deterministic results; the results are generated with a complex matrix operation and are not directly influenced by the user for this particular result.

This condition introduces a legal dilemma of whether AI generated content is documentary evidence, computer-generated real evidence, or automated expert opinion. When AI derived content is used solely as proof of its existence, there's a risk that the courts will presume this is just a document and that every word in it is accurate, without taking into account algorithmic bias or training data inaccuracies. On the other hand, if it is treated as actual evidence – like a thermometer or speed radar – the party that offers it must prove that it was in proper order and working as it should at the time in question. But the inner workings of a complex generative model are not like that of a simple measuring device, they can be a "black box" even to the model's creators.[13] Thus, simply defining AI-generated outputs as "electronic records" under section 2(1)(t) of BSA does not adequately capture their dynamic and non-deterministic nature.

Procedural Barrier: Statutory Certification under Section 63 BSA vs Section 65B IEA

Statutory certification is the gateway in Indian civil litigation to admit any electronic record as secondary evidence. Where an electronic record is a document and is admissible without any further proof as a result of compliance with certain statutory conditions, it is admissible without further proof when the record is printed on paper, stored, recorded or copied in optical or magnetic media.

The provisions of the core conditions contained in Section 63(2) of the BSA[14] must be met:

a) The computer output was generated by the computer during the period during which the computer was regularly used to store or process information for any activities conducted regularly;
b) In the course of these activities, the information type contained in the electronic record was regularly inputted into the computer during the above period;
c) During this material part, the computer was working as intended, or if it was not, the fact that the computer was not working did not impact the accuracy of the contents; and
d) The data in the record is the reproduction or derivation of such data which is entered into the computer in the normal course of such activities.

[13] Harry Surden, Machine Learning and Law, 89 Wash. L. Rev. 87, 114–18 (2014).
[14] Bharatiya Sakshya Adhiniyam, 2023, § 63(3)-(4), No. 47, Acts of Parliament, 2023 (India).

e) The certificate must be signed by a person in a responsible official position with respect to the operation of the device, or the management of the activities.[15]

Such a regulatory framework brings significant challenges into practice when implemented in the context of generative AI systems. Condition (b) must first be satisfied by information of the type found in the record being regularly fed in the ordinary course of activities. The outputs of generative AI, whether it be a new, synthetic contract draft or a predictive model, are dynamically created from massive amounts of diverse training data, instead of administrative inputs. Second, a requirement to prove that the system was operating properly is required by condition (c). From a software point of view, an algorithm can be functioning perfectly, yet producing a nicely formulated "hallucination" or incorrect output because of the training data or reward-function mismatch.

In addition, there is a structural problem in determining who should sign the Section 63(4) certificate. Is it the end user who entered the prompt, the software developer who created the algorithm, or the cloud-based provider of the model infrastructure? The Supreme Court in Arjun Panditrao Khotkar has laid down a mandatory requirement for certification as it pertains to admissibility [16]. Applying these strict standards for certification to the outputs of AI developed under a distributed cloud system puts civil litigants in an evidentiary bind.[17]

The Challenge of Authenticating of Machine Hearsay, and the "Black Box" Challenge

In addition to procedural certification, civil courts need to establish the authenticity and trustworthiness of the evidence created by AI. When the output from an AI is generated as evidence in civil cases involving breach of contract, intellectual property rights or commercial fraud, the probative value of the output will depend on establishing the output is what its proponent alleges it is.[18]

One of the key evidentiary objections to the outputs of AI is the doctrine of hearsay. Out-of-court statements made for the purpose of establishing the truth of the matter asserted are traditionally not allowed under hearsay rules, because there is no way to cross-examine the original speaker on the matter. If an AI tool provides a report, a diagnosis, or a similar analytical product, is it a "statement" that is subject to the hearsay bar? Modern legal theory makes a difference between what is said by human beings via computers as well as pure machine statements. In common law countries, courts have come to the conclusion that

[15] Bharatiya Sakshya Adhiniyam, 2023, § 63(3)(c) & § 63(4), No. 47, Acts of Parliament, 2023
[16] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1, 52.
[17] Stephen Mason & Daniel Seng, *Electronic Evidence* 284–88 (5th ed. 2021).
[18] Fed. R. Evid. 901(a).

statements made solely by automatic machine processes are not hearsay because a machine is not considered a "person" for proof law purpose[19]].

However, withholding this evidence of reliability is dangerous as it would throw out the hearsay rule. A machine can't lie, but it can fall for a number of reasons to give false, distorted, or fabricated answers:

a) Training Data Bias: Errors or poor sampling of the training data set.
b) Algorithmic Opacity: The 'black box' nature of DNNs, meaning that the decisions made inside the algorithm cannot be audited or explained.
c) Prompt Manipulation: Manipulation of input by a litigant [20]to get a desired output.

The Deepfake Problem in Civil Proceedings and Standard of Proof

From hyper-realistic synthetic video to the cloning of voices and the creation of fake digital signatures, generative deepfake technology is a huge threat to civil trial strategy. In a criminal case, the prosecution must prove guilt beyond reasonable doubt, in a civil case, it is judged on the balance of probabilities. This lower evidentiary standard opens the door to deepfakes becoming particularly endemic in civil cases.

In case of a matrimonial division of the estate or of a commercial contract dispute, for instance, a party may present an audio recording that is claimed to contain an oral admission or corporate promise. When the other side alleges that it's an AI-generated voice clone, the court is confronted with a challenging evidentiary dilemma. Courts may use expert opinions to determine altered media under Section 45 of the IEA (and corresponding Section 39 of the BSA).[21] But the current commercial deepfake detection tools suffer from poor performance[22] in terms of high false positives and false negatives rates compared to generative synthesis tools.

Furthermore, deepfakes bring about the “liar’s dividend,” which is the case where litigants falsely allege that authentic harmful digital evidence is an AI generated deepfake to avoid liability [23]. Pursuant to Section 101 and Section 102 of the BSA (which sets forth the burden of proof), the party alleging the affirmative of a claim has the burden of proving it. The courts' difficulty lies in the fact that, if there is a genuine digital record being disputed as a

[19] United States v. Lizarraga-Tirado, 789 F.3d 1107, 1110 (9th Cir. 2015)
[20] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* 16–23 (2023).
[21] *Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 6914
[22] Hany Farid, *Fake Photos*, MIT Press Essential Knowledge Series 76–82 (2019).
[23] Bobby Chesney & Danielle Citron, *Deepfakes and the New Disinformation Threat*, 105 Minn. L. Rev. 1757, 1785 (2019).

deep fake, the challenger may have to continually convince the court of authenticity, or the participant may have to provide initial technical evidence of a synthetic alteration. This leaves people in doubt, causing procedural delays, escalating litigation expenses, and strategy-driven abuse in civil proceedings.

This course will compare the perspectives of the US Federal Rules of Evidence and the EU AI Act. A review of the foreign legal systems can provide useful insights to help in solving these clearly identified evidentiary hurdles.

Under the U.S. rules of evidence, the admissibility of machine outputs is mostly determined by FRE 901 (Authenticating or Identifying Evidence) and FRE 702 (Testimony by Expert Witnesses). FRE Rule 901(b)(9) makes special mention of evidence that is the product of a "process or system" of which the proponent must produce evidence "describing a process or system used to produce a result and showing that the process or system produces an accurate result." This rule focuses not only on the reliability of the device, but on that of the technical process as a whole. Moreover, in cases of complex predictive analysis, U.S. courts test the underlying technology according to the Daubert standard (Daubert v. Merrell Dow Pharmaceuticals, Inc.) [24]. Daubert rules place the burden on the trial judge to determine if the AI methodology has been empirically tested, peer reviewed, subjected to known error rates and generally accepted in the relevant scientific community.

European Union Artificial Intelligence Act (2024): EU Act on Artificial Intelligence (2024) adopts a risk-based approach with direct implications for the rules of civil evidence in the EU member state [25]. To enhance the legal accountability of high-risk AI systems, under the EU framework, these systems, such as those used in judicial administration, credit scoring, and critical infrastructure, must comply with stringent legal obligations related to data governance, technical documentation, transparent systems[26], automatic logging, and risk management. Article 50 of the EU AI Act explicitly mandates transparency requirements for deployers of Generative AI, including the requirement to label deepfakes and synthetically generated content in machine-readable formats. As for civil litigation in European courts, these transparency and logging requirements offer a straightforward record of the events of the proceedings, which include the generation or modification of a digital record by AI, and this facilitates the verification of the events.

[24] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).
[25] EU AI Act, *supra* note 9, art. 50.
[26] 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), arts. 9–15, 2024 O.J. (L 1689).

DISCUSSION

This analysis shows that the existing rules of civil evidence, including those of the Bharatiya Sakshya Adhiniyam 2023, are not suitable for dealing with the complexities of AI-generated evidence. The approach of treating dynamic, probabilistic algorithmic outputs as "electronic records" under the same procedural framework as static electronic records raises legal uncertainty, risks evidence of fraud in civil trials and imposes impractical certification requirements for litigants.

To fill this legislative void, there is a need for comprehensive reforms of the legal and procedural framework:

a) Legislative change to BSA: The legislature should add a separate category to the BSA for Algorithmic and Synthetic Digital Media. While passive electronic records under section 63 will need a two-step authentication process, AI generated evidence should have a two-step authentication process as well:
b) Technical Process Authentication: Assuring the correctness of the software model, parameters for the training, and execution of the prompt (US FRE 901(b)(9)).
c) System Integrity Certification: Mandating that the entity that provided the AI output shares the specific version of the software or model, the prompts that were used, and the environment in which it was operated to produce the output.

To alleviate the "liar's dividend" and keep the parties safe from synthetic fraud, the framework of rebuttable presumptions should be incorporated into civil procedure. A digital record that has been certified to be initial upon its deposit should be presumed to be genuine until technical evidence (e.g. preliminary forensic audit or metadata) is produced by the opposing party establishing prima facie evidence of synthetic manipulation. Upon the presentation of such prima facie evidence the burden of proof returns to the proponent to prove authenticity on a basis of a preponderance of probability.

Since the technical nature of neural networks, there should be increased use of the court-appointed independent technical expert provided for in the BSA 39. Furthermore, rules of civil procedure should be updated to permit limited "algorithmic discovery" in high-value commercial disputes, allowing court-appointed experts to inspect training logs, system prompts, and model parameters under strict protective confidentiality orders.

CONCLUSION

The use of AI in routine business and legal transactions is a fundamental change in the way civil litigation is conducted and settled. The Bharatiya Sakshya Adhiniyam, 2023 has introduced updates to the rules of static electronic evidence and has the benefit of bringing them into the modern world, but it still does not sufficiently address the autonomous, non-deterministic and synthetic outputs of AI. Evidence created by AI cannot be considered conventional documentary evidence and it is not admissible without proper disclosure of the algorithms involved in its generation.

Civil litigation must be a fair process, and this means that evidence law must be adapted to reflect these technical facts. The law can benefit from legal technology, but the focus on the positive side of legal technology, while protecting truth, transparency, and judicial integrity, can be achieved through the implementation of a reform of Section 63 of the BSA, the introduction of specific process-authentication requirements based on comparable standards such as the US FRE Rule 901(b)(9) and the EU AI Act, setting clear burden-shifting rules for deepfake claims, and the use of court-appointed technical experts.