THE EXAMINER, THE ALGORITHM, AND THE ACCUSED: ASSESSING THE ADEQUACY OF THE BHARATIYA SAKSHYA ADHINIYAM, 2023 FOR AI-GENERATED EVIDENCE

Richelle Nick. S, LLM, Jain University, Bengaluru, Karnataka

ABSTRACT

The Bharatiya Sakshya Adhiniyam, 2023 (BSA), which came into effect from 1st July 2024 and replaced the Indian Evidence Act, 1872, is aimed at modernizing the law of evidence in India to suit the digital age. A major part of this modernization is Section 63, which revises the certificate for electronic records, and Section 39(2), which clearly states that the role of the Examiner of Electronic Evidence is that of an expert when it comes to issues involving information contained in computer resources. While these sections mark a major leap forward, it is pertinent to point out that the BSA was enacted at a time when AI was changing the very nature of evidence, not just its medium of storage. AI evidence includes AI outputs, machine learning outputs, algorithmic forensic tools, facial recognition, decision-support tools, and other autonomous decision-support tools that are being offered without any specific statutory guidelines being laid down regarding its admissibility, its reliability, or the right of parties to challenge it. It is submitted that the BSA, while being a major legislative leap forward, has three structural shortcomings when it comes to AI evidence. Firstly, the requirement of a Section 63(4) Part B certificate was developed for authenticating static electronic evidence and not for assessing the reliability of the underlying process of generation of evidence in AI systems. The question of who could be a competent expert for the purpose of authenticating the outputs of an AI model remains completely unanswered. Secondly, although Section 39(2) specifies the expert for the purpose of electronic evidence as the Examiner of Electronic Evidence, no provision for a reliability inquiry of the underlying AI model upon which the expert evidence was based is made. Thirdly, the right of an accused person under Article 21 of the Constitution of India to challenge evidence of AI systems is structurally flawed in the absence of a requirement for disclosure of the underlying model of the AI evidence. The article concludes with recommendations for a framework for addressing the issues identified based upon a comparative framework of the law in the US and Australia.

Keywords: Bharatiya Sakshya Adhiniyam, AI-generated evidence, Examiner of Electronic Evidence.

INTRODUCTION

The most comprehensive overhaul of the law of evidence in India since its independence is the Bharatiya Sakshya Adhiniyam, 2023 (BSA)[1], replacing the Indian Evidence Act, 1872[2]. With the BSA coming into force on the 1st of July 2024, the law of evidence in India is set to witness a modernization of the rules concerning electronic and digital evidence in its 170 sections. However, even as the Parliament of India was busy enacting legislation concerning electronic mail, CCTV footage, and even encrypted communications, a new form of evidence had begun to emerge in India, one that is the product of artificial intelligence, such as voice spectrogram results obtained through machine learning, facial recognition results, risk assessment results, and even forensic summaries produced by artificial intelligence, in both civil and criminal trials, without the BSA providing any express code for testing the veracity of such evidence, nor vindicating the rights of the parties who would resist such evidence.

This is important because the new kind of electronic evidence is not just electronic evidence in a new form; it is evidence, whose admissibility is not dependent upon the integrity of the electronic file but upon the validity of the process by which it is generated, a process that may be obscure, proprietary, and/or subject to error rates that are unknown to the adversary. The legal question is whether the BSA's system, predicated upon the authentication of electronic evidence and the appointment of Examiners of Electronic Evidence as expert witnesses, is sufficient to the task. This article argues that it is not, that three structural gaps must be addressed by Parliament and the judiciary, and that the analysis will proceed in the following way: in Section II, the BSA's most important provisions will be discussed in the context of AI-generated electronic evidence; in Section III, the three structural gaps will be identified; in Section IV, the experience in the United States and Australia will be explored; and in Section V, recommendations will be offered.

PART I: THE BSA'S FRAMEWORK AND ITS APPLICATION TO AI OUTPUTS

The Definition of 'Document': Section 2(1)(d)

[1] Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India) [hereinafter BSA]. Presidential assent: 25 December 2023; commencement: 1 July 2024.
[2] Indian Evidence Act, 1872, No. 1, Acts of Parliament, 1872 (India), repealed by BSA § 170.

The BSA defines 'document' in Section 2(1)(d) to include 'any matter expressed or described or otherwise recorded upon any substance... and includes electronic and digital records.'[3] This broad definition appears on its face to be broad enough to encompass AI-generated output: the probability score of a machine learning model, a facial recognition report generated algorithmically, or a forensic summary written by AI is a 'matter expressed by means of letters or figures' stored on a device. The real question is not whether such output is included in the definition of 'document,' which appears almost certain – but whether the rules for admissibility under Section 63 and the expert opinion regime under Section 39 are sufficient to address the unique reliability concerns surrounding AI output.

The Certificate Requirement: Section 63

The BSA framework for admissibility of electronic records rests upon a trilogy of provisions. The provisions are as follows: Section 57 of the BSA treats certain electronic records as primary evidence[4]. Section 61 of the BSA provides that digital records shall be admissible as documents and shall have the same legal effect as paper records[5]. Section 63 of the BSA is a codification of the requirement of a certificate for the admissibility of electronic records as settled in a trilogy of decisions of the Supreme Court in Anvar P.V. v. P.K. Basheer[6], Shafhi Mohammad v. State of Himachal Pradesh[7], and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal[8]. Significantly, however, Section 63 of the BSA goes beyond the requirement of a certificate as settled in the above decisions in that the certificate contemplated in Section 63(4) of the BSA shall be in two parts: Part A shall be filled in by the person submitting the evidence,

[3] BSA § 2(1)(d) ('document' means 'any matter expressed or described or otherwise recorded upon any substance by means of letters, figures or marks or by more than one of those means... intended to be used or which may be used for the purpose of recording that matter', and expressly includes electronic and digital records). BSA § 2(1)(e) defines 'evidence' to include all documents, including electronic and digital records, produced for the court's inspection.

[4] BSA § 57 (defining 'primary evidence'; Explanations 4–7 provide that electronic and digital records in proper custody, or stored across multiple devices or simultaneously transmitted, constitute primary evidence).

[5] BSA § 61 (electronic or digital records shall not be excluded from evidence on the ground that they are electronic; they shall have the same legal effect, validity, and enforceability as any other documents, subject to BSA § 63).

[6] Anvar P.V. v. P.K. Basheer & Ors., (2014) 10 SCC 473 (three-Judge Bench holding that secondary electronic evidence is inadmissible unless accompanied by a certificate under § 65B(4) of the Indian Evidence Act, overruling State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600 to that extent).

[7] Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801 (two-Judge Bench, subsequently overruled in Arjun Panditrao Khotkar, holding the certificate requirement could be relaxed when the tendering party was not in possession of the device).

[8] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal & Ors., (2020) 7 SCC 1 (three-Judge Bench, decided 14 July 2020; reaffirming Anvar P.V. and overruling Shafhi Mohammad; holding that the § 65B(4) certificate is a mandatory condition precedent to admissibility of secondary electronic evidence).

and Part B shall be filled in by a qualified expert along with a report of a hash value in the prescribed Schedule[9].

The Part A/Part B construct of the Section 63(4) certificate is an actual improvement in the level of evidentiality over the Section 65B construct. It ensures that the electronic record is verified for integrity and hash by an independent expert. But it does not address the question of the reliability of the process that created the electronic record in the first place. For a static electronic record such as a WhatsApp message or a frame from a CCTV camera, the concern is primarily one of authentication, ensuring that the electronic record is what it is purported to be and has not been interfered with in any way. But for an AI-generated electronic record, the question of the authentication of the output file is the easy part; the much harder question is the reliability, validity, and unbiased nature of the generative model itself.

The Examiner of Electronic Evidence: Section 39(2)

Section 39(2) of the BSA states that "where it is necessary for the court to form an opinion upon 'any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form,' the opinion of the Examiner of Electronic Evidence under Section 79A of the Information Technology Act, 2000 shall be a relevant fact and the said Examiner 'shall be an expert.' This provision of law is of significant importance as it provides a clear basis for admitting the opinions of certified experts in the field of digital forensics in a court of law and eliminates all ambiguity in this regard. A crucial omission in the provisions of Section 39(2) of the BSA, however, relates to the fact that although this provision specifies what expert opinion the court shall consider in admitting evidence of electronic evidence, it fails to specify what standards the court shall use in assessing the reliability of the methodology adopted by the expert. An 'expert' in the field of electronic evidence who uses a commercial AI-based forensic tool and produces a report shall be an 'expert' as per the provisions of Section 39(2) of the BSA.

PART II: THREE STRUCTURAL LACUNAE

The foregoing analysis reveals three structural lacunae that the BSA does not address.

[9] BSA § 63 (admissibility of electronic records; corresponding to former § 65B, IEA; the certificate under § 63(4) is now in two parts: Part A to be completed by the person submitting the evidence; Part B to be completed by an expert, with hash value reports required as per the Schedule).

The first is the absence of a reliability standard for AI generative processes. The BSA's Section 63(4) certificate is a certification of the reliability of the output file, not the reliability of the process used to generate the file. A court admitting an AI-generated forensic report on the basis of a duly certified Section 63(4) certificate and the expert opinion of a Section39(2) Examiner is simply stating affirmatively that the file is authentic and was produced by a certified expert. It is not inquiring in the slightest way into the scientific validity of the AI model used in the generation of the file. There is no framework in Indian law on the reliability gatekeeper obligation established in Daubert v. Merrell Dow Pharmaceuticals[10] in the US, which requires trial courts to make their own determinations about the testability of the evidence and its potential for errors before admitting evidence that is based upon certain scientific methodologies. The Supreme Court of India has recognized the Daubert criteria in the context of scientific evidence, although the BSA does not codify any of this. The courts are left without a basis upon which to question the reliability of AI-generated evidence.

The second lacuna is the infringement of the right to challenge AI evidence under Article 21. In Justice K.S. Puttaswamy (Retd.) v. Union of India, a unanimous decision was rendered by the Supreme Court. It held that a right to privacy demands that an infringement of a person's protected interest is lawful, necessary, and proportionate. When AI evidence is used adversarial in a criminal proceeding against an accused, then a part of their right to a fair trial is their ability to challenge AI evidence. However, under the BSA, no duty is imposed on an individual using AI evidence to disclose their data set used for training their model or their error rate. An accused in a criminal proceeding cannot compel an individual using AI forensic evidence to disclose their model's false positive rate or their demographic data set. Cross-examining the Section 39(2) Examiner is not an alternative to this systemic disclosure because the Examiner themselves may not have knowledge of the internals of the proprietary model.

The third gap is that there is no framework for autonomous AI output. The BSA's definition of 'evidence' under Section 2(1)(e) includes oral statements by witnesses and documents produced for inspection by the Court. This scheme starts with the assumption of a human author or a human-operated device. It does not account for AI system-generated output that has been created without any human involvement—such as a contract analysis created solely by a large

[10] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993) (U.S. Supreme Court, Blackmun J.; establishing that Federal Rule of Evidence 702 requires trial judges to act as evidentiary 'gatekeepers', assessing: (i) testability; (ii) peer review and publication; (iii) known or potential error rate; and (iv) general acceptance in the relevant scientific community).

language model, a crime prediction generated without any human intervention, or an AI-created surveillance report. The precise rationale for admitting evidence in this manner—whether it be considered a document or an expert opinion or something else—remains unclear. This definitional gap has created judicial inconsistencies.

PART III: COMPARATIVE PERSPECTIVES

The United States' Federal Rules of Evidence, at Rule 901(b)(9), provide that evidence can be authenticated by showing that it is of the type that produces an accurate result[11]. When these provisions are considered in conjunction with the requirements of the Daubert framework, it is clear that the American judiciary have taken the view that the scientific validity of the AI forensic evidence needs to be established at a minimum level prior to it being allowed, examining the data used for training the model, the validation methodology employed, the error rates of the model, and the general acceptance of the model within the relevant forensic science community[12]. This is the gatekeeping role of the adversarial system.

Australia's Evidence Act 1995 takes a different approach by providing a rebuttable presumption of accuracy for documents generated by machines. This means that documents generated by machines are presumed to have been generated accurately if they were generated by a normally functioning device at or near the relevant time[13]. This is a pragmatic approach because it does not require proof of technical accuracy, but still allows the opposing party to adduce evidence to rebut this presumption by proving a malfunction or inaccuracies in the device or process. What is noteworthy is that, unlike the BSA's approach, which focuses on authentication, this approach focuses on accuracy, which is a more appropriate concern with AI evidence. What both systems have in common, and what is lacking in the Indian system, is the realization that the product of an algorithm needs to be subjected to a separate inquiry of reliability, not merely the authenticity of the file, but the process. The Standing Committee on Home Affairs, in their report on the Bharatiya Sakshya Bill, did address the need for ensuring the integrity of

[11] Federal Rules of Evidence, r. 901(b)(9) (U.S.) (evidence may be authenticated by 'evidence describing a process or system and showing that it produces an accurate result').
[12] Evidence Act 1995 (Cth) (Austl.) § 48 (documents produced by a device or process presumed accurate if the device was functioning normally; rebuttable by contrary evidence). The Commonwealth and uniform evidence legislation adopted this model to facilitate admission of digital records without requiring technical proof in every case
[13] Evidence Act 1995 (Cth) (Austl.) § 48 (documents produced by a device or process presumed accurate if the device was functioning normally; rebuttable by contrary evidence). The Commonwealth and uniform evidence legislation adopted this model to facilitate admission of digital records without requiring technical proof in every case

electronic evidence. However, they did not go far enough with respect to the reliability of AI generative processes. This was certainly understandable in 2023. However, it is no longer tenable given the pace at which AI evidence is now being introduced in the Indian courtroom.

CONCLUSION AND RECOMMENDATIONS

The BSA represents a significant step forward from the Indian Evidence Act in its approach to electronic evidence. The two-part certificate under Section 63(4), the recognition of the office of the Examiner of Electronic Evidence in Section 39(2), and the wide definition of "document" in Section 2(1)(d) collectively provide a stronger basis for electronic evidence than was previously available. However, the BSA was not developed in response to the particular evidentiary issues created by AI-generated evidence. The three structural defects identified in this article—the lack of a reliability test for generative AI, the undermining of the accused's Article 21 right to challenge AI evidence, and the lack of a framework for autonomous AI evidence—are not ancillary concerns. They are fundamental to the fairness of evidence in an AI-driven litigation environment.

Three specific reforms are recommended to overcome the difficulties that AI-generated evidence is creating in Indian courts. Firstly, the Supreme Court is recommended to issue a set of practice directions that mandate party adducing AI-generated evidence to disclose details of sources used for training the AI model, validation processes followed for the AI model, error rates associated with the AI model, and details of the exact version of the AI model used in the specific instance. Secondly, Parliament is recommended to make amendments to Section 63 of the BSA that mandates a 'reliability declaration' in addition to the authentication certificate. Such a reliability declaration is to affirm that the AI model was validated for use in the exact manner in which it was used in a particular instance and to disclose details of the error rate of the AI model in similar instances. Thirdly, Parliament is recommended to make amendments to Section 2(1)(d) of the BSA to include a specific definition of 'AI-generated records' as a distinct type of electronic records and to subject AI-generated records to a dual test of admissibility under the BSA: one for authentication under Section 63 and another for reliability validation.