AI-GENERATED EVIDENCE IN THE INDIAN LEGAL SYSTEM: NAVIGATING THE EVIDENTIARY VACUUM AND CHARTING A REFORM AGENDA

Ananya Sharma, Amity University, Noida

Dr. Ekta Gupta**,** Amity University, Noida

ABSTRACT

The increasing use of Artificial Intelligence (AI) in the judicial, administrative, and commercial spheres has generated a new form of legally relevant material - AI-generated evidence - that is not structurally suited to the existing evidentiary regime in India. This research paper provides an analysis of the epistemic, doctrinal and institutional aspects of AI-generated evidence in India, including the normative deficiencies of the Bharatiya Sakshya Adhiniyam,[1] 2023 (BSA) - the successor of the Indian Evidence Act,[2] 1872 - and the possible avenues for reform.

This paper begins with a classification of AI-generated evidence - including risk assessment tools generated by algorithms, facial recognition matches, natural language processing (NLP) transcriptions, deepfake video and audio clips, generative AI content, and machine learning predictive analytics - and a discussion of the technological features of such evidence that present novel challenges for judicial assessment, such as the opacity of algorithmic reasoning, lack of a human "author", and risk of systemic bias. It then conducts an analysis of the existing evidentiary regime, mapping the evolution of Section 65B of the Indian Evidence Act and its successor provisions in the BSA with regard to computer-produced documents, and highlights the deficiencies that undermine the efficacy of these provisions for AI-generated evidence.

The paper then engages in a comparative study of the evidentiary frameworks of the United States (Federal Rules of Evidence and Daubert standards), the European Union (the AI Act and its evidentiary implications), the United Kingdom (post-Brexit), and some Asian jurisdictions such as China and Singapore. The paper draws on these insights to recommend a holistic reform framework for India, which includes specific amendments to the BSA, the

[1] Bharatiya Sakshya Adhiniyam, 2023.
[2] Indian Evidence Act, 1872.

creation of a network of AI forensics certification bodies, a framework for transparency and explainability of algorithms used in courts, and a judicial capacity-building initiative.

Keywords: Artificial Intelligence, AI evidence, Bharatiya Sakshya Adhiniyam 2023, Section 65B, electronic evidence, deepfakes, algorithmic evidence, authentication, admissibility, machine learning, Indian Evidence Act, law and technology, algorithmic opacity, explainability.

I. INTRODUCTION

Technology and law have always been in a structural relationship of inequality. The pace of innovation determines the pace at which technology develops; the pace of reasoning and institutional change determines the pace at which the law develops. This asymmetry is most pronounced in the law of evidence, the body of rules which govern the materials on which courts decide matters of fact. In India, normative standards of evidence were codified in the Indian Evidence Act of 1872 - a colonial legislative artifact written at a time when "document" always referred to paper and "author" always to a person. The past 150 years of technological advance, from the invention of audio and visual recording technologies, to the advent of electronic computing, to the creation of the internet, to the development of artificial intelligence, has been matched by increasingly inept normative responses by the law.[3]

Contemporary forms of Artificial Intelligence present the greatest challenge to the normative framework of the law of evidence. Unlike a human witness, whose veracity may be challenged through cross-examination, or an electronic record, which may be authenticated by a certificate issued by a responsible person, AI-generated evidence is the result of intricate statistical calculations applied to extensive data, with no one human author who can be said to know, explain, or certify the specific instance. It is this epistemic novelty, paired with authorial opacity, that makes AI-generated evidence a new type of evidence, not contemplated by today's evidence laws.

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) - which repeals the Indian Evidence Act with effect from July 1 2024, as part of a comprehensive recodification of the Indian criminal law trilogy - is the latest attempt to reform the law of evidence in India. Although the BSA contains a number of enhancements over the previous legislation, such as a reclassification of electronic

[3] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

evidence and digital records, this paper suggests it is still structurally incapable of regulating AI-generated evidence. The normative void in the heart of Indian evidence law, therefore, continues to exist, and its ramifications - in criminal practice, in civil practice, and in commercial arbitration - are increasingly evident each year.[4]

This paper proceeds as follows. Part II offers a conceptual framework for AI-generated evidence and describes its technical features. Part III examines the Indian evidentiary law (from Section 65B of the Indian Evidence Act to the BSA) in relation to AI-generated evidence. Part IV examines the doctrinal deficiencies that amount to the evidentiary gap. Part V conducts an international comparative study. Part VI recommends a reform agenda for India. Part VII concludes.

II. CLASSIFICATIONS AND TECHNICAL FEATURES OF AI-GENERATED EVIDENCE

2.1 Defining AI-Generated Evidence

The focus of this paper is on AI-generated evidence - defined as any material generated, analysed, categorised, or evaluated by an artificial intelligence system and tendered in evidence for the purpose of proving or disproving a fact in issue, or a relevant fact, in a court, tribunal, or other adjudicatory body. This classification is intentionally broad, and includes not just evidence produced by an AI system, but also analyses that are assisted by an AI system in converting raw data into a legal inference.

This definition needs to be separated from two related concepts. First, AI-processed evidence - such as using an algorithm to improve the clarity of a photograph without changing its substance - where AI is used as a technical instrument rather than an epistemic agent. Second, AI-authenticated evidence such as the use of an AI system to authenticate the integrity of a document or the voice of a speaker - where the questions concern the reliability of verification, rather than the authenticity of the evidence.[5]

2.2 Types of AI-Generated Evidence

AI-generated evidence comes in a number of forms, with different technical features and

[4] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[5] Nils J. Nilsson, *Artificial Intelligence: A New Synthesis* (Morgan Kaufmann 1998).

evidentiary implications.

Risk assessment scores generated by algorithms are one of the most important and contentious types of AI-generated evidence in criminal law. Algorithms like COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) in the US, and similar predictive policing and bail risk assessment systems increasingly used by police in India, produce scores or probabilities of future risk based on historical data. These scores and probabilities are presented in court as evidence of risk of future offences in bail, sentencing and parole. The algorithms' lack of transparency, the closed nature of the underlying code, and the potential to embed historical biases in predictive outputs have serious implications for justice.[6]

Biometric evidence from facial recognition systems, which identify a person from CCTV footage or other forms of surveillance by matching the image to a biometric database, is also increasingly being used in criminal investigations in India. The systems' accuracy rates differ among groups of people (known as differential error rates) and studies have shown that rates of error are much higher for darker skinned people, women, and the elderly. The use of facial recognition evidence without a proper consideration of its technical risks may lead to significant wrongful results.

Natural language processing (NLP) transcriptions are created by AI systems from audio and video recordings and are employed in a wide range of proceedings, including criminal and civil fraud, family divorces, and even criminal trials. NLP systems, unlike human transcribers, may be prone to accent, noise and jargon, and may introduce systematic biases that are not immediately discernible by non-technical users.[7]

Deepfakes and synthetic media are perhaps the most pressing evidentiary threat arising from AI. Generative adversarial networks (GANs) and large language models can create synthetic video, audio and image data that look and sound almost identical to real video recordings. With deepfake technology becoming more widely available, the possibility of synthetic media being introduced as authentic evidence in courts of law - and conversely, of genuine video recordings being judged by a court to be deepfakes - is a problem of critical importance to fact-finding in Indian courts.

[6] Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn, Pearson 2021).
[7] European Commission, *Ethics Guidelines for Trustworthy AI* (2019).

2.3 Algorithmic Opacity and Explainability

Many sophisticated AI systems, especially deep learning models, are opaque: it is not possible for any human to explain, in a clear and step-by-step fashion, the reasoning that led to a particular output. This feature - sometimes referred to as the "black box problem" - has a profound effect on the law of evidence.

The adversarial system of evidence, as adopted by Indian law from English common law, is premised on the idea that evidence can be subjected to cross-examination, witnesses can articulate the reasoning behind their statements, and judges and juries can rationally assess the evidence. The opacity of algorithms undermines each of these premises. If the designer of a risk assessment system cannot explain how the system generated a particular risk score for a particular offender, how can the score be tested by the defence? How can a judge assess its weight? How can an appeal court assess the reasonableness of the fact-finder's reliance on it?[8]

The notion of 'explainable' AI - the ability of AI systems to offer explanations of their results - has become a key regulatory priority in several jurisdictions. The European Union's AI Act requires explainability of high-risk AI systems, such as those used in law enforcement and the courts. India's legal framework lacks such requirements, which means that courts lack guidance in determining the admissibility of the output of opaque algorithms as evidence.

III. A CRITIQUE OF INDIA'S EVIDENTIARY LAW

3.1 The Indian Evidence Act, 1872: A Legislation of Empire

The Indian Evidence Act, 1872, authored by Sir James Fitzjames Stephen and passed by the British Parliament, was a codified version of the Anglo-Saxon law of evidence, tailored to the Indian legal system. Its underlying structure - distinguishing facts in issue and relevant facts, the law of evidence dealing with oral and documentary evidence, and the burden of proof - reflected the Victorian conception of evidence that evidence was authored by humans, that documents were material objects, and that expert evidence was the means by which specialised knowledge entered the courtroom.

The increasing use of electronic evidence in court proceedings through the Information

[8] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015)

Technology Act, 2000[9], and the subsequent amendment of the Indian Evidence Act to include Sections 65A and 65B, were a partial and imperfect solution to the problem of electronic evidence. This act introduced a certification process for the admissibility of computer-generated records - requiring a certificate from a person holding a responsible official position in relation to the computer used to prepare the record - but it did not and could not foresee the arrival of AI-generated evidence, which features the absence of a single responsible author.[10]

3.2 The Bharatiya Sakshya Adhiniyam, 2023: An Analysis

The Bharatiya Sakshya Adhiniyam, 2023, a part of India's criminal law reform initiative along with the Bharatiya Nyaya Sanhita and the Bharatiya Nagarik Suraksha Sanhita, introduces a new law that replaces the Indian Evidence Act. The BSA retains the same underlying architecture as its predecessor, but it makes several changes to the law of electronic evidence. Significantly, the BSA alters the two-tiered regime of Sections 65A and 65B with a new regime for 'electronic records', extends the scope of electronic evidence to include communications from 'electronic devices' and 'other electronic forms', and provides for certification.

Despite the proposed changes, the BSA does not address the key problems with AI-generated evidence. The BSA still deals with electronic evidence exclusively in terms of the authenticity of the record (the electronic record has not been tampered with in transit or storage) and not in terms of the reliability and explainability of the generative process. This is an important point: for AIgenerated evidence, it is not just a question of whether the record has been altered since it was generated, but whether the generative process was reliable enough to produce probatively relevant evidence.

The BSA is also silent on the hearsay concerns around machine-generated statements, the admissibility of AI-generated expert testimony, and the procedural rules around the challenge of algorithmic records. These are not mere technical details; they are structural deficiencies that render the Indian courts without a normative framework for assessing AI-generated evidence.[11]

[9] Information Technology Act, 2000.
[10] Law Commission of India, *Report No. 185: Review of the Indian Evidence Act, 1872* (2003).
[11] S.C. Sarkar, *Sarkar on Evidence* (LexisNexis, 18th edn, 2016).

3.3 The Section 65B Jurisprudence

Over the years, the Supreme Court has rendered a large amount of jurisprudence on the certification requirements of Section 65B. In Anvar P.V. v. P.K. Basheer ((2014) 10 SCC 473), the Court ruled that electronic evidence that is inadmissible without the Section 65B certificate cannot be admitted as secondary evidence under any other sections, overturning previous practice and confirming the mandatory nature of the certification. In Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal ((2020) 7 SCC 1), the Court confirmed this stance and considered the issue of whether the court could require the certificate even if it is not provided initially.

These cases, although technically compliant with the legislative provisions, expose the inherent deficiencies of the certification framework in respect of AI-based evidence. The Section 65B certificate certifies the propriety and integrity of the 'computer' system used. But in relation to an AI system, what does it mean to certify that the system was 'running properly'? It is possible that an AI system outputs biased results (biased training data) while functioning technically as it should. The certificate cannot take this into account.[12]

IV. THE EVIDENTIARY VACUUM: PARTICULAR DOCTRINAL DEFICIENCIES

4.1 Authentication of AI-Generated Evidence

Authentication - the process of proving that a document or other evidence is what it is claimed to be is the first step in the admissibility of documentary or electronic evidence. In the context of AI, the process of authentication is more complicated than for other types of electronic evidence. It requires not just establishing the integrity of the evidence (that it has not been tampered with) but also the reliability of the generative process - the data that was used for training, the structure of the model, the methods used for testing, and the environment that was used to generate the evidence.

India does not have a specific framework for authentication of AI-generated evidence. The BSA's framework for electronic evidence prioritises integrity and not reliability; neither the BSA nor any of its related regulations specify technical standards, testing and certification protocols for AI systems generating evidence. This leaves litigation to fall back on the general

[12] Ratanlal & Dhirajlal, *The Law of Evidence* (LexisNexis, 26th edn, 2017).

principles of expert evidence and judicial discretion, which is likely to lead to varied and technically naive outcomes.[13]

4.2 Chain of Custody in Algorithmic Processes

The chain of custody - the chronological documentation of the handling of a piece of evidence - is fundamental to the admissibility of evidence, especially in criminal trials. In the case of evidence produced by an AI system, the chain of custody requirements will apply not only to the physical (or virtual) handling of the evidence output, but also to the data inputs to the AI system, the training data used to create the model, the version of the algorithm used to produce the evidence, and any changes to the system after the evidence was produced.

There is no existing provision in Indian evidence law to address the issue of chain of custody requirements for AI-generated evidence. This is especially problematic in the case of predictive policing and facial recognition systems where evidence is created in the course of law enforcement activities that may not have proper documentation of the algorithms used. In the absence of a chain of custody, the chain of custody of AI-generated evidence cannot be established and the risk of unreliable and manipulated evidence making its way into court is significantly raised.[14]

4.3 Hearsay: Machine Statements and the Author

The hearsay rule - which, in its simple form, bars out-of-court statements offered for the truth of their contents unless they fit within an exception - poses a conceptual challenge for AI evidence. The rule is based on the idea that a "statement" is made by a "person" who may be cross-examined. However, AI systems do not make statements - they generate outputs that result from statistical processing of training data. There is no person who makes a statement and who can be crossexamined.

Indian evidence law, like its common law counterparts, does not offer a clear framework to determine the nature of the machine's output in respect of the hearsay rule. In practice, courts have tended to treat electronically produced records as "documents" rather than "statements", and so avoid the hearsay problem. But this is not satisfactory for AI outputs that are indeed

[13] Avtar Singh, *Principles of the Law of Evidence* (Central Law Publications, 2019).
[14] Stephen Mason, *Electronic Evidence* (5th edn, Institute of Advanced Legal Studies 2021).

inferential in nature - such as a risk score, facial recognition or sentiment analysis - where the output is not a document and the correctness of the inference is the key issue.

4.4 Right to Confront and Algorithmic Transparency

The opacity of AI systems poses a serious challenge to the right to confrontation granted to an accused - a right that is enshrined in the notion of "natural justice" and the right to a fair procedure under Article 21 of the Constitution. If a criminal defendant is convicted on the basis of an algorithmic risk assessment generated by a proprietary system, the workings of which are inexplicable due to it being a trade secret, the defendant has been denied the right to examine the evidence against them.[15]

This is no abstract problem. In the US, the case of State v. Loomis[16] (881 NW 2d 749, Wis 2016) raised this issue with respect to the COMPAS risk assessment system. The Wisconsin Supreme Court validated the COMPAS score, despite the defendant's lack of access to the proprietary algorithm - a decision that drew significant academic criticism. In India, where predictive policing systems and facial recognition technologies are increasingly being used without sufficient regulatory safeguards, similar issues relating to the confrontation right are likely to emerge.

4.5 Deepfakes and the Authenticity Crisis

The rise of deepfakes, computer-simulated audio-visual media produced by AI that looks and sounds like real media, raises an authenticity problem for the law of evidence that goes beyond the traditional methods for scrutinising created or faked evidence. Traditional methods of evidence verification - chain of custody records, forensic examination of video and audio files, and visual analysis - are becoming insufficient to detect deepfakes[17].

The 'liar's dividend' - using deepfake allegations to undermine evidence - is also an issue. With increasing knowledge of deepfake technology, parties may challenge the authenticity of bona fide audio or video evidence by invoking the possibility of deepfake creation. In the absence of a scientifically robust and legally verifiable methodology for detecting deepfakes and

[15] Lorraine v. Markel American Insurance Co., 241 F.R.D. 534 (D. Md. 2007).
[16] *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
[17] Rebecca Wexler, 'Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System' (2018) 70 Stanford Law Review 1343.

authenticating visual and audio evidence, courts will increasingly doubt the veracity of video and audio evidence.

V. INTERNATIONAL COMPARISONS

5.1 The United States: Daubert Standards and Emerging Practice

The rules of the US Federal Rules of Evidence and, in particular, the Daubert standard adopted by the Supreme Court in Daubert v. Merrell Dow Pharmaceuticals Inc.[18] (509 US 579, 1993), offer the most sophisticated standard in the common law system for the admissibility of novel scientific and technical evidence. Daubert requires a federal court to play the role of a "gatekeeper" to determine the admissibility of expert testimony based on novel scientific or technical knowledge: whether the knowledge is scientifically valid, and the opinion reliably applied to the facts of the case. The Daubert test is based on whether the method employed by the expert has been tested, peer reviewed, and accepted as valid within the scientific community.

US courts have started to apply Daubert standards to AI evidence, such as algorithmic risk assessments. A number of federal circuit courts have required the proponent of an algorithmic output to demonstrate the scientific validity of the underlying methodology, the reliability of the particular application, and the credentials of the expert offering the AI output. Others have also demanded access to training data and model documentation to facilitate testing. These experiences offer valuable guidance for India, albeit still in their infancy.

5.2 Europe: The AI Act and its Impact on Evidence

The European Union's Artificial Intelligence Act, which came into effect in 2024, is the most ambitious framework for regulating AI systems to date and has important ramifications for the admissibility of AI-generated evidence in court. The AI Act takes a risk-based approach: it defines prohibited, high-risk and limited-risk AI systems. There are specific requirements for transparency, explainability, human oversight, and accuracy for high-risk AI systems (including those used in law enforcement, criminal justice, and judicial administration) and

[18] *Daubert v. Merrell Dow Pharmaceuticals Inc.*, 509 U.S. 579 (1993).

technical documentation must be maintained.[19]

In the context of AI-generated evidence, the AI Act's requirements for technical documentation, logging and transparency of high-risk AI systems sets a regulatory standard that impacts on the quality of evidence. The fact that high-risk AI systems must be designed to enable human oversight and their operation logged in a way that allows for retrospective review offers a model for the sort of regulatory requirements that should be considered in India's AI policy and regulatory framework.

5.3 Lessons from the United Kingdom and Singapore

Post-Brexit reforms have begun to see the UK develop its own regulatory approach to AI, while the Law Commission of England and Wales is conducting an inquiry into the law of evidence and the use of AI-generated outputs. The Commission's initial consultation has identified issues of authentication, reliability, explainability, and the hearsay rule as the key evidentiary challenges of AI - broadly consistent with the findings in this paper.

Singapore offers valuable comparative lessons for India as a technologically advanced common law jurisdiction with a forward-looking approach to the regulation of legal technology. The Singapore Academy of Law has released comprehensive guidelines on the use of AI in the legal profession, and Singapore's courts have been highly sophisticated in their consideration of issues relating to electronic evidence. Singapore's evidence law - which draws in part on the Indian Evidence Act - has been more quickly updated to accommodate the realities of electronic evidence and AI-generated evidence, offering an example for India to follow.[20]

VI. A REFORM FRAMEWORK FOR INDIA

6.1 Principles for Reform

The reform framework for the governance of AI-generated evidence in India should be premised on the following principles. First, the principle of technological neutrality: the legal framework should be articulated in terms that are not technology-specific to current AI technologies, but also open to future technological advances. Second, the principle of epistemic

[19] Danielle Keats Citron and Robert Chesney, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753.
[20] Andrew D. Selbst, 'Disparate Impact in Big Data Policing' (2017) 52 Georgia Law Review 109.

adequacy: the framework should ensure not only the integrity of AI-generated evidence but also its reliability - the accuracy and validity of the generative process. Third, the principle of confrontation and fairness: the framework must ensure the parties against whom AI-generated evidence is used are afforded a fair chance to test the evidence. Last, the principle of institutional capacity: the law must be complemented by a build-up of the institutional capacity of the judiciary, forensic institutions and regulatory agencies to assess AI-generated evidence.

6.2 Legislative Proposals to BSA

This paper recommends the following amendments to the Bharatiya Sakshya Adhiniyam, 2023, to fill the evidentiary gap in AI-generated evidence:

- A new Chapter on 'AI-Generated Evidence' should be introduced, which establishes a separate definition and admissibility framework for AI-generated evidence. This should be based on a functional definition, emphasising the epistemic properties of the evidence rather than the technology used.

- AI-generated evidence should be subject to a reliability test, similar to the Daubert test, with the proponent of the evidence required to demonstrate that the AI system has been validated through testing, peer review and audit, and that the particular output was generated in conditions of technical reliability.[21]

- A more comprehensive certification framework, to replace the current Section 65B-based regime, should require AI-generated evidence to be accompanied by a technical disclosure document which identifies the AI system, provides details of the data and methods used to train the system, performance metrics, including error rates disaggregated by relevant demographic variables, and certification that the system complies with technical standards.

- A presumption against admissibility of AI evidence generated from unexplainable systems should be created, with a rebuttable presumption that AI-generated evidence is inadmissible unless proponents can demonstrate that the system complies with applicable explainability principles or that the particular AI-generated evidence has been subject to independent forensic certification.

[21] Cary Coglianese and David Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105 Georgetown Law Journal 1147.

- A specific provision on deepfakes and synthetic media should mandate that any party proffering audio-visual evidence certify the evidence's authenticity, and provide forensic certification from an AI forensics laboratory, with courts having the power to engage court experts where authenticity is disputed.

6.3 Institutional Arrangements: AI Forensics and Certification

Law reform is not enough. The use of AI evidence calls for strong institutional measures. The paper recommends the following institutional arrangements.

First, a National AI Evidence Standards Authority (NAESA) should be established as a statutory body with the Ministry of Law and Justice, with the responsibility to develop technical standards for the validation and certification of AI systems used for evidence generation. NAESA should be comprised of a diverse range of computer scientists, forensic scientists, lawyers, and ethicists, with the power to accredit AI forensics laboratories and certify AI systems for use in the courts. Second, a network of accredited AI Forensics Laboratories should be set up in every state, capable of performing forensic investigations of AI evidence, authenticating audio-visual materials and issuing expert reports to the courts. The laboratories should adhere to NAESA's quality standards and should be equally accessible to prosecution and defence parties in criminal court.

Third, NAESA should maintain a mandatory AI Evidence Registry, documenting all AI systems that have been certified for evidentiary purposes, along with the technical specifications, testing and validation data and limitations of each system. Courts should be obliged to check certification of AI-generated evidence from a given system.[22]

6.4 Judicial Capacity Building

If any law or institutional framework on AI evidence is to be applied, it is essential for the judiciary to have the technical capacity to assess AI systems and AI-generated evidence. This paper proposes the following capacity-building measures. The National Judicial Academy should offer specialised courses on the law of AI evidence to judges, at all levels, on the

[22] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated DecisionMaking Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76.

technical basics of machine learning, assessment of evidence of the reliability of an AI system, and application of our proposed legal framework.[23]

Further, courts should be given the power and incentives to appoint court-designated AI experts - similar to court-appointed experts in patent infringement or medical malpractice cases - in cases involving complex AI-generated evidence. These experts would help the court comprehend the technical aspects of disputed evidence, minimising the danger of courts being misled by expert evidence presented by parties.

VII. CONCLUSION

AI-generated evidence is one of the most important and pressing issues facing evidence law in 21stcentury India. The current evidentiary law, even as proposed by the Bharatiya Sakshya Adhiniyam, 2023, was not constructed to address evidence produced by non-human authors, whose decisionmaking processes are inscrutable, and whose veracity is dependent on factors - quality of the training data, validity of algorithms and potential demographic biases - that are beyond the traditional evidence-evaluation tools.

This paper has shown the presence of a structural and normative gap in Indian evidence law with regard to AI-generated evidence in several areas: authentication, chain of custody, hearsay, right to confrontation, and deepfakes and synthetic media. The comparative study of legal approaches in the US, the EU, the UK, and Singapore shows the problem is urgent, and the range of legislative and regulatory solutions available.

The roadmap for reform proposed in this paper - which includes targeted amendments to the BSA, the creation of a National AI Evidence Standards Authority and a network of accredited AI forensics labs, as well as a nationwide judicial capacity building program - offers one way for India to respond to the evidentiary vacuum. The need is pressing: AI systems are already in use in law enforcement and in the courts in India, and cases involving AI evidence are being litigated today, without an adequate normative framework for their adjudication.

Much is at stake. Justice's fair administration is premised on the reliability and integrity of evidence used to determine facts. At a time when predictive risk assessments, facial

[23] Gary Chan and Lee Pey Woan, *The Law of Torts in Singapore* (Academy Publishing 2016) (discussion on technology and liability).

recognition, and generative AI will increasingly be used to produce evidence in court, it is not a matter of technicality but of constitutional substance that the evidence produced by AI is reliable, transparent and fair. The promise of a fair trial - protected by Article 21 of the Constitution of India - cannot be fulfilled unless the evidence that informs criminal guilt and civil liability is assessed in a manner commensurate with the technological possibilities of our time.

Indian constitutional jurisprudence has been at the forefront of constitutional innovation. The adaptation of its evidentiary law to the challenges of AI-generated evidence is the next step in that tradition.

REFERENCES

Primary Sources

- Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
- Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.
- State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
- K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
- State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601.
- Daubert v. Merrell Dow Pharmaceuticals Inc., 509 US 579 (1993).
- Frye v. United States, 293 F 1013 (DC Cir 1923).
- State v. Loomis, 881 NW 2d 749 (Wis Sup Ct 2016).
- R v. Reed and Reed, [2009] EWCA Crim 2698.
- Indian Evidence Act, 1872, Sections 65A, 65B.
- Bharatiya Sakshya Adhiniyam, 2023.
- Information Technology Act, 2000.
- European Parliament and of the Council, Regulation (EU) 2024/1689 of 13 June 2024 on Artificial Intelligence (AI Act).

Secondary Sources

- Thaman, S.C. (ed.), Comparative Criminal Procedure (Edward Elgar Publishing, 2022).
- Casey, E., Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (Academic Press, 4th ed. 2020).
- Roth, A., 'Machine Testimony' (2017) 126 Yale Law Journal 1972.
- Wexler, R., 'Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System' (2018) 70 Stanford Law Review 1343.

- Nissenbaum, H., 'Accountability in a Computerized Society' (1996) 2 Science and Engineering Ethics 25.
- Goodman, B. and Flaxman, S., 'European Union Regulations on Algorithmic DecisionMaking and a Right to Explanation' (2017) 38 AI Magazine 50.
- Faigman, D.L., et al., Modern Scientific Evidence: The Law and Science of Expert Testimony (Thomson West, 2020).
- Bagaric, M. et al., 'Evidence Law and Artificial Intelligence' (2021) 44 UNSW Law Journal 1154.
- Bambauer, D. and Evans, B., 'Expert Court, Lay Jury: Artificial Intelligence and Evidence Law' (2022) 95 Southern California Law Review 585.
- Doshi-Velez, F. and Kim, B., 'Towards a Rigorous Science of Interpretable Machine Learning' (2017) arXiv:1702.08608.
- Buolamwini, J. and Gebru, T., 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 1.
- Law Commission of India, Report on Reforms in the Law of Evidence (Report No. 185, 2003).
- Ministry of Electronics and Information Technology, Report of the Committee on NonPersonal Data Governance Framework (Government of India, 2020).
- Singapore Academy of Law, Guidelines on the Use of Technology in Legal Practice (SAL, 2023).
- National Law University Delhi, AI and the Law in India: An Emerging Regulatory Agenda (NLU Delhi Working Paper, 2024).