# AI-GENERATED EVIDENCE IN INDIAN COURTS: ADMISSIBILITY, RELIABILITY AND THE CHAIN OF CUSTODY CHALLENGE

Deepanker Singhal, Advocate & Cyber Breach Review Attorney, GGIPU & Amity University

Pragya Narang, Senior Content Manager & Founder, ThinkPro (Research & Content Dev. Co.), Delhi University

## ABSTRACT

Artificial intelligence is not restricted to laboratories or commercial platforms anymore; rather it has shown its presence in the criminal justice system as well in multiple ways, like predictive policing, forensic image analysis, etc. The judicial system of India has struggled even with the admissibility of conventional electronic evidences which are given under the Indian Evidence Act, 1872, especially sections 65A and 65B. Landmark cases like *Anvar P.V. v. P.K. Basheer*[1] and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[2] demonstrate both judicial engagement and an on-going struggle. The challenge is more pressing as now we have AI-generated evidence such as deep fake videos, synthetic voices, machine translations, and algorithmic forensic reports, etc. Internationally-designed instruments such as the EU AI Act, 2024[3], the U.S. Federal Rules of Evidence[4] and the UK Criminal Justice Act, 2003[5] have started to address these questions, but India has no purposive framework at this time. This article argues the existing evidentiary law is inadequate, draws on the comparative features, and proposes statutory reform to ensure admissibility, reliability, and constitutionality of AI-generated evidence.

[1] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[2] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[3] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (EU AI Act).
[4] Federal Rules of Evidence, United States, Rules 702 & 901.
[5] Criminal Justice Act 2003 (UK), Part 11.

## Chapter 1: INTRODUCTION

### 1.1 Background

The evidentiary world in India has changed dramatically. While courts used to deal predominantly with oral testimony and documentary evidence, the advent of digital technology now makes electronic evidence the main focus of litigation. Mobile phone data, CCTV datasets, social media postings, and even e-signature contracts are commonly used as evidence in civil and criminal matters[6].

Indian courts started on a cautious note to begin with. State (NCT of Delhi) v. Navjot Sandhu (Parliament Attack Case)[7] in which the Supreme Court allowed the electronic records in the absence of the mandatory section 65B certificate, leaving the bar open to interpretation. This was rectified in *Anvar P.V. v. P.K. Basheer*[8] wherein the Court reiterated that section 65B compliance was not only mandatory, but was the only way to prove a secondary evidence of an electronic record. The view was reaffirmed by a 3 judge's bench in *Arjun Panditrao Khotkar*[9], where it was held that non-compliance of section 65B is fatal unless the device itself is produced in the court. This series of cases highlighted the judiciary's concern for authenticity.

However, AI-generated evidences pose unprecedented challenges. The deepfake technology[10] can generate extremely realistic but fake video. AI systems are able to create artificial recordings mimicking a person with uncanny precision[11]. Machine learning is used in handwriting recognition[12], facial recognition[13] and forensic image analysis[14]. Predictive algorithms are reportedly under consideration for police work in Indian states[15]. However, the evidentiary value of such AI outputs is not well-understood yet.

All over the world, scholars have shown concern for the "black box problem" in AI, where the

[6] Apar Gupta, "Electronic Evidence and Indian Courts" (2017) 10 NUJS L Rev 321.
[7] *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.
[8] Supra note 1.
[9] Supra note 2.
[10] Chesney & Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" (2019) 107 Cal L Rev 1753.
[11] K. Rini, "Deepfakes and the Epistemic Backstop" (2020) 33 Philos & Tech 461.
[12] R. Guest, "Automated Handwriting Comparison" (Forensic Science International, 2020).
[13] S. Garvie, "Facial Recognition and Law Enforcement" (Georgetown Law, 2019).
[14] Jain et al, "AI in Forensic Image Analysis" (2021) 61 Forensic Sci Int 101.
[15] Singh, "Predictive Policing in India: Prospects and Pitfalls" (2022) 44 J Indian L & Soc 67.

machine learning system's internal logic is opaque even to their own developers[16]. The debates have begun in the courts of the United States regarding admissibility of algorithmic evidence under Rule 702 (expert testimony) and Rule 901 (authentication) of the Federal Rules of Evidence[17]. Also, the EU AI Act classifies AI systems by risk level, subjecting high-risk forensic tools to strict compliance standards[18]. United Kingdom has formed a regulator's code of practice of forensic science that applies to digital and AI-based forensic techniques[19]. Singapore has brought amendments to its Evidence Act in 2012 in order to simplify electronic evidence rules, but AI-specific provisions still remain absent[20].

For India, there is more at stake, in the form of constitutional guarantees. The right of self-incrimination guaranteed under Article 20(3) had already driven the Supreme Court to outlaw compulsory narco analysis and brain mapping in the case of *Selvi v. State of Karnataka*[21]. The trials are required to be fair and evidence to be reliable as per the right to life and personal liberty under Article 21[22]. Due to absence of safeguards, the admissibility of AI-generated evidence can result into wrongful convictions and miscarriages of justice.

Therefore, this paper suggests for a model amendment to the Indian Evidence Act that includes an explicit definition of AI evidence, standards for admissibility and reliability, and mandates preservation of chain of custody. The paper also focuses on comparative study of global practices to demonstrate both pitfalls and possible solutions.

## 1.2 Current Legal Position in India

### 1.2.1 Electronic Evidence under the Evidence Act

The Evidence Act was enacted in 1872, when computers and electronic communication were not into existence[23]. The Act was amended by the Information Technology Act, 2000 to recognise electronic records as it inserted sections 65A and 65B[24]. Section 65A states that electronic records shall be proved in accordance with section 65B. Section 65B(4) talks about

[16] Burrell, "How the Machine 'Thinks': Understanding Opacity in Machine Learning" (2016) Big Data & Society 1.
[17] Cary Coglianese & David Lehr, "Regulating by Robot" (2017) 105 Geo LJ 1147.
[18] Supra note 3.
[19] Forensic Science Regulator, Code of Practice, UK (2021).
[20] Evidence (Amendment) Act 2012 (Singapore).
[21] *Selvi v. State of Karnataka*, (2010) 7 SCC 263.
[22] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
[23] Ratanlal & Dhirajlal, *The Law of Evidence* (LexisNexis, 2022).
[24] Information Technology Act, 2000, s. 92.

a certificate which identifies the device, describes the process of production, and attests to the integrity of the record.

In Anvar P.V. case[25], the Court held that the certificate to be mandatory. The case of *Arjun Panditrao Khotkar*[26] also reaffirmed the same by clarifying that this certificate will be issued only when the original device is itself produced. In the cases of *Shafhi Mohammad v. State of Himachal Pradesh*[27] and *Jagdeo Singh v. State (Govt of NCT of Delhi)*[28] High courts have also applied these provisions and guidelines.

But these sections cover only static electronic records. Whereas, AI-generated evidences are often dynamic, produced during the process of analysis, and they may not reside on a single device. When the algorithm is proprietary and controlled by private corporations, the certificate under section 65B becomes impractical[29].

### 1.2.2 AI in Criminal Investigations

Law enforcement bodies in India have already included AI tools in their practices. The Delhi Police has started using facial recognition technology to identify suspects during protests[30]. The National Crime Records Bureau has shown inclination towards predictive policing systems[31]. Forensic labs have used AI for handwriting and image analysis[32].

While these tools prove to be advantageous in investigations, but their admissibility still remains unsettled in court. Use of technology in limited context has been permitted by Indian courts, such as, video conferencing testimony in the case of *State of Maharashtra v. Dr. Praful Desai*[33]. Courts have admitted CCTV footage as evidence where proper certification exists[34]. But there is still no precedent directly addressing AI-generated evidence.

[25] Supra note 1.
[26] Supra note 2.
[27] *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.
[28] *Jagdeo Singh v. State (Govt of NCT of Delhi)*, (2015) SCC OnLine Del 13928.
[29] Edwards & Veale, "Slave to the Algorithm? Why a 'Right to Explanation' is Probably Not the Remedy You Are Looking For" (2017) 16 Duke L & Tech Rev 18.
[30] Scroll.in, "Delhi Police's Use of Facial Recognition Technology" (2019).
[31] NCRB Report on Crime Analytics, 2021.
[32] National Forensic Sciences University, Annual Report 2022.
[33] *State of Maharashtra v. Dr. Praful Desai*, (2003) 4 SCC 601.
[34] *Ram Singh v. Col Ram Singh*, 1985 Supp SCC 611.

### 1.2.3 Constitutional Concerns

Two safeguards have been provided in the Constitution. First, Article 20(3) gives protection against self-incrimination. In *Selvi v. State of Karnataka*[35], compulsory narco-analysis and brain mapping was prohibited, stressing dignity and autonomy. Similar issues may be raised due to AI-based lie detection or behavioural prediction. Second, Article 21 gives guarantee of right to fair trial. It has been repeatedly held by the Courts that unreliable evidences violate due process of law[36]. If AI evidence is admitted without proper scrutiny, it will result in undermining this guarantee.

Thus, the present framework is inadequate. The Evidence Act includes electronic records but does not cover AI related concerns. Law enforcement agencies are adopting AI tools without any statutory oversight. Constitutional rights require careful safeguards. Therefore, there is an urgent need of reform.

## Chapter 2: COMPARATIVE PERSPECTIVES

### Introduction

While India is struggling with the admissibility of electronic records issue, many other countries have begun addressing the application of AI in legal proceedings. The European Union has enacted a comprehensive regulation, i.e., the EU AI Act, 2024. The United States has continued to depend on their Federal Rules of Evidence, supported by relevant case law. The UK has also adopted regulatory laws which focus on standards of forensic science. Since Singapore was only nearer to Indian legal tradition, the evidentiary law with regard to electronic records has been simplified, but it has not instituted any provisions specific to AI. These advancements provide help and guide to shape India's legal response.

### 2.1 The European Union and the AI Act, 2024

A strong stance has been made by the European Union with The EU Artificial Intelligence Act (AI Act, 2024), which is the first holistic law about AI in the world. The Act is based on a risk-based framework which classifies AI systems as unacceptable risk, high risk, limited risk and

[35] Supra note 21.
[36] *Zahira Habibulla H. Sheikh v. State of Gujarat*, (2004) 4 SCC 158.

minimal risk[37]. Forensic AI tools, such as biometric identification and deep fake detection, fall in the high-risk class, where the need of compliance is rigorous and encompass data quality, transparency and human oversight.[38]

The AI Act does not directly amend evidential codes to address admissibility, but the repercussions are substantial. Courts in the EU must verify that evidence produced by AI systems falls within the certification parameters of the Act.[39] Scholars suggest this is a form of "pre-screening" gating unreliable AI evidence from getting into the proceedings.[40] Further, the Act imposes disclosure obligations to ensure litigants and courts have access to important information about the AI tool's operation, even if proprietary.[41]

The EU model exemplifies how to establish standards and certification for AI for India. Without standards and certification courts could admit AI generated evidence without an understanding of accuracy or bias.

### 2.2 The United States: Federal Rules of Evidence and Algorithmic Evidence

The United States is yet to adopt a comprehensive AI law but its evidentiary framework can provide some lessons. The Federal Rules of Evidence (FRE) contain two relevant provisions that courts have applied:

- Rule 702, which governs expert testimony and it stipulates the reliability of scientific, technical, or specialized knowledge and whether it can assist the trier of fact.[42]
- Rule 901 on authentication requires sufficient proof to support a finding that the said item is what the proponent claims.[43]

Courts have applied these provisions to algorithmic tools. In *State v. Loomis*, the Wisconsin Supreme Court upheld the use of COMPAS, a proprietary risk-assessment algorithm, while also acknowledging a due process violation because the defendant had no opportunity to

[37] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, 2024 O.J. (L 1689) 1.
[38] Id. arts. 6–9.
[39] Id. art. 43.
[40] See Andrea Bertolini, Artificial Intelligence and Legal Liability, 11 Eur. J. Risk Reg. 199, 214 (2020).
[41] EU AI Act, supra note 1, art. 52.
[42] Fed. R. Evid. 702.
[43] Fed. R. Evid. 901.

examine the internal workings of the algorithm.[44] Federal courts have also faced DNA analysis software which require disclosure of error rates and validation studies under *Daubert v. Merrell Dow Pharmaceuticals*.[45] Scholars contend the FRE framework and scrutiny from judicial scrutiny together provides courts with a flexible means of admitting or rejecting AI evidence.[46]

The U.S. experience has provided two lessons for India: first, judicial gatekeeping through standards of reliability matters; and second, the constitutional implications of using proprietary "black box" algorithms in criminal trials.

### 2.3 The United Kingdom: Forensic Science Regulator and Digital Evidence

The United Kingdom has taken a different approach in contrast to comprehensive AI legislation, via regulatory oversight of forensic practice. The Forensic Science Regulator Act, 2021 provides a regulatory body that can issue codes of practice that are binding for all forensic providers subject to the provisions, including those who use AI tools.[47]

When applying legislation to hearsay and expert evidence issues, UK courts rely on provisions in the Criminal Justice Act, 2003.[48] The admissibility test addresses reliability and will the evidence have the means to be challenged? In R v. Luttrell, the Court of Appeal pointed out that new scientific evidence must achieve standards of reliability. Furthermore, scientific evidence must be reliable, relevant, and capable of assisting the court.[49]

The Forensic Science Regulator's Code of Practice for Forensic Science Providers (2021) is systemic and specifically references digital forensics and emerging AI applications as technologies.[50] Before reliable AI-generated evidence could be relied on by a court, the Code requires validation, documentation, and quality assurance before the evidence could be relied on. Scholars argue that the Regulator's work seeks to overcome the tension between scientific innovation and the question of admissibility.[51]

---

[44] *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
[45] *Daubert v. Merrell Dow Pharms*., Inc., 509 U.S. 579, 592–93 (1993).
[46] Cary Coglianese & David Lehr, Regulating by Robot: Administrative Decision Making in the Machine-Learning Era, 105 Geo. L.J. 1147, 1170–71 (2017).
[47] Forensic Science Regulator Act 2021, c. 5 (U.K.).
[48] Criminal Justice Act 2003, c. 44, §§ 114–136 (U.K.).
[49] R v. Luttrell [2004] EWCA (Crim) 1344.
[50] Forensic Sci. Regulator, Code of Practice (2021) (U.K.).
[51] Carole McCartney, Forensic Science in England and Wales: A Legal Perspective, 54 Crim. L. Bull. 123, 130–31 (2018).

What the UK model would suggest for India is an independent oversight body that could set technical standards for the quality of AI-based evidence, would be able to determine and demonstrate reliability without an expectation that judges act as technologists.

### 2.4 Singapore: Simplified Evidence Rules without AI-Specific Provisions

Singapore provides an intriguing comparative example as a common law jurisdiction with advanced statutory regimes. The Evidence (Amendment) Act, 2012 modified previous statutory rules on electronic records to make them unambiguous and removed unnecessary technical requirements for the principles of certification.[52] Section 35 of the Singapore Evidence Act allows for admissibility of computer output where the system had operated properly and the record was not subject to interference.[53]

However, Singapore has no specific law dealing with AI. Courts in Singapore have traditionally relied on broad common law principles regarding authenticity and reliability. One commentator suggests that while flexibility in the law promotes efficiency and expediency, the risk of ambiguity arises as AI-generated evidence becomes commonplace.[54]

For India, the Singapore example suggests the value of developing a simplified process. The rigidity of certification rules, such as the provisions of section 65B and the pre-evidence deemed admissibility requirements of the Indian Evidence Act, can cause delays and result in obstructions to justice. At the same time, there are some potential disadvantages, as there is no fast-track for AI-generated evidence in the absence of safeguards to authenticity and reliability, similar to that which exists in section 65B of the Indian Evidence Act.

### 2.5 Key Takeaways for India

The materials from this comparative analysis suggest that India cannot ignore the relevance of admissible evidence generated through AI. Drawing from the experience of the EU as a model for regulatory standard setting, the U.S. example of the role of judicial gatekeeping, the use of forensic quality/auditing processes in the U.K., and the Singapore alternative of simplifying processes, India can find a comparative model that will assist. An Indian evidence standards

[52] Evidence (Amendment) Act 2012 (No. 4 of 2012) (Sing.).
[53] Evidence Act 1893, c. 97, § 35 (Sing.).
[54] Daniel Seng, Electronic Evidence in Singapore: Developments and Prospects, 14 Sing. Acad. L.J. 201, 222 (2019).

framework should consider all of these elements:

- Define AI-generated evidence in the Indian Evidence Act.
- Mandate certification and reliability standards (EU model).
- Empower judges to exclude unreliable evidence (U.S. model).
- Establish an independent forensic regulator for AI tools (UK model).
- Simplify procedures of certification (Singapore model).

This approach would help Indian legal system to prepare for the AI era, in accordance with constitutional protections under Articles 20(3) and 21.

## Chapter 3: CHALLENGES FOR INDIA

### Introduction

The Indian Evidence Act, 1872, drafted in an age of colonialism, was never meant to deal with Artificial Intelligence, machine learning, and blockchain based evidence. Even though section 65B was added in the year 2000 to deal with electronic records, but still there has been conflicting interpretations relating to it.[55] Since AI-based evidences are advancing in criminal trials, India will struggle with its admissibility, acceptability, reliability, authenticity, chain of custody, and constitutional safeguards. Each of these points needs further examination before we can begin to recommend changes.

### 3.1 Admissibility under Section 65B

The landmark decision in *Anvar P.V. v. P.K. Basheer* held that electronic records would be admissible only when they are accompanied by a certificate under section 65B(4).[56] Subsequent judgments like *Shafhi Mohammad v. State of Himachal Pradesh* reduced the requirement to accept secondary electronic evidence without a certificate under limiting circumstances.[57] But later the Supreme Court indicated that the certificate was mandatory in *Arjun Panditrao*

[55] Information Technology Act, No. 21 of 2000, § 92, Acts of Parliament, 2000 (India).
[56] Supra note 1.
[57] Supra note 27.

*Khotkar v. Kailash Kushanrao Gorantyal*.[58]

These earlier precedents demonstrate the inconsistencies in the judicial landscape and interpretations. The absolute requirement of the certificate has created a situation where critical evidence (for instance CCTV footage, or call records) does not get looked at because the certificate is not present.[59] AI-generated evidence makes this even more complicated. For example, how do they certify the algorithmic process that created the output? Should the certification cover just the device that stored the evidence or the AI system used to generate the evidence as well? The statute is silent.

### 3.2 Reliability and the "Black Box" Problem

Reliability is a core concept in evidentiary law. Section 45 of the Evidence Act establishes expert opinion, but presumes that a review of the basis of the expertise is available.[60] With AI, in particular proprietary algorithms, there may be little or no opportunity to review the reasoning process involved, referred to as the "black box problem".[61]

Indian courts have experienced types of difficulties related to forensic related challenges. In Selvi v. State of Karnataka, the Supreme Court found that narco-analysis and polygraph evidence were inadmissible in part due to reliability issues.[62] More recently, in critiquing facial recognition technology used in the Delhi riots trials, the courts referred to the lack of accuracy studies in the publicly available literature.[63] By not having transparency, accepting AI generated outputs into evidence is likely to breach an individual's due process rights.

Reliability is linked to bias; there is evidence suggesting facial recognition systems perform poorly for darker skin types, increasing the chances of producing wrongful convictions in India.[64] Unless error rates and validation studies are reported, reliance on AI generated

[58] Supra note 2.
[59] Rahul Sharma, Electronic Evidence and Section 65B: The Indian Experience, 12 Nat'l L. Sch. India Rev. 45, 49–50 (2021).
[60] Indian Evidence Act, 1872, § 45.
[61] Jenna Burrell, How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms, 3 Big Data & Soc'y 1, 3 (2016).
[62] Supra note 21.
[63] Apoorva Mandhani, Courts Flag Reliability of Facial Recognition in Delhi Riots Cases, Indian Express (Mar. 12, 2021).
[64] Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 Proc. Machine Learning Rsch. 1, 5 (2018).

evidence gives rise to a breach of the fair trials guarantee afforded under Article 21.[65]

### 3.3 The Chain of Custody and Authenticity

The chain of custody provides assurance that evidence is not altered or altered.[66] For traditional digital exhibits, courts require assurance that the data was produced by a specific evidence source and that data has not been altered.[67] For AI evidence, the situation is even more challenging: not only must the data be authenticated, but the actual algorithm must also be authenticated.

For instance, let's take deepfake videos. The prosecution may claim that it is a video produced by a suspect. The defense may claim it was artificially manipulated. Simply verifying it is a deepfake video requires the use of technical tools for deepfake detection, which may include their own AI.[68] This dependence on using AI to get information to authenticate other AI raises significant evidentiary challenges.

And there's more: Section 65B of the Evidence Act deals with the certification of a functioning "computer".[69] However, AI also often operates off a distributed cloud system; therefore, the accessing/processing platform may not be available to investigating agencies. Therefore, courts may be left to rely on third-party certifications from technology providers and thus rely on private companies.

### 3.4. Constitutional Concerns

The constitutional guarantees which accompany AI evidence cannot be ignored. Article 20(3) protects a person from self-incrimination.[70] If an accused is forced to give his or her biometric data which will be processed through an AI computer, has he or she been deprived of the right not to self-incriminate? The Supreme Court in Selvi, clearly stated that testimonial evidence is not compelled but physical evidence, in the form of fingerprints, is permissible.[71] Whether data processed by an AI computer can be classified as testimonial or physical remains unresolved.

[65] Usha Ramanathan, Due Process and Technology in India, 25 Nat'l L. Sch. India Rev. 87, 93 (2019).
[66] Paul Roberts & Adrian Zuckerman, Criminal Evidence 218 (3d ed. 2010).
[67] Supra note 7.
[68] Hany Farid, Photo Forensics, 98 Comm. ACM 56, 58 (2019).
[69] Indian Evidence Act, 1872, § 65B(4).
[70] India Const. art. 20(3).
[71] Selvi, supra note 21, at 310.

Article 21 of the Constitution guarantees a fair trial and is linked with due process. In Maneka Gandhi v. Union of India, the Court stated that due process was not only substantive law but included procedural fairness.[72] What happens if an accused cannot challenge how an algorithm works because of trade secrecy? Admitting evidence based on that process could be unfair and contrary to due process.[73]

Finally, Article 14 guarantees equal protection before the law. If a court admits evidence based on AI and the AI is flawed in terms of equality and produces biased results, then the court would be allowing systemic discrimination and prejudice to extend to marginalised peoples.[74]

### 3.5 Judicial Capacity and Technology Literacy

Even if the law is changed, the issue of judicial capacity will remain. Indian judges and lawyers are not uniformly trained to assess technical evidence.[75] Complex issues about the accuracy, bias, and error rates of algorithms may dissuade many trial courts from engaging. This exacerbates the problem of using AI too freely (e.g., taking it as gospel) and becoming too skeptical (e.g., rejecting it without proper analysis).[76]

Currently, judicial academies in India offer very limited training on digital evidence.[77] Without capabilities building, any reform will become merely aspirational.

## Conclusion

The challenges to admitting AI-generated evidence in India are diverse. Section 65B establishes procedural hurdles, while the issues of reliability, authenticity, and constitutional expectations express substantive concerns. Each of these concerns can only further complicate the uncertainty. If these challenges are not consider through legislative amendment, education of judiciary, and oversight responsibilities for AI, the court will still likely struggle to integrate technology with its concern with constitutional rights.

[72] Supra note 22.
[73] Nandan Kamath, Technology and Due Process: The Loomis Debate in India, 34 Nat'l L. Sch. India Rev. 101, 112 (2022).
[74] Nikita Sonavane, Algorithmic Discrimination and Indian Criminal Justice, 7 Indian J. L. & Tech. 155, 167 (2021).
[75] S.K. Verma, Judicial Training and Technology in India, 62 J. Indian L. Inst. 201, 209 (2020).
[76] Abhinav Chandrachud, AI Evidence and the Indian Judiciary, 45 Econ. & Pol. Wkly. 36, 37 (2021).
[77] National Judicial Academy, Annual Report 2021–22, at 72.

## Chapter 4: RETHINKING SECTION 65B – PROPOSED AMENDMENTS AND CASE STUDIES

### 4.1 The Inadequacy of Section 65B for AI Evidence

Section 65B of the Indian Evidence Act is concerned with the authenticity of electronic records, particularly emails and computer printouts, and documentation stored on DVDs, CDs, and similar electronic devices. The requirement of a certificate under Section 65B is indicative of a pre-AI world where human authorship was assumed.[78] The advent of AI-generated evidence, however, raises many issues that the drafters of Section 65B never contemplated. Unlike digital documents, outputs of AI may be probabilistic rather than definite, shaped by blurred and opaque training data, or there can be possibility of biasness.[79] This mismatch poses significant challenges for courts because they are relying on an outdated framework to address regionally novel challenges.

This tension is evident in Indian case law. For example, in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*,[80] the Supreme Court affirmed that Section 65B certificates are mandatory for the admissibility of electronic documents, but offered no guidance for when evidence does not have any human author. The reluctance of the Delhi High Court to admit CCTV footage in *State v. Navjot Sandhu*[81], could not be extrapolated to cover the type of analytics that had AI generated outputs, which include facial recognition technologies or predictive policing algorithms.

Comparative perspectives sharpen the critique. In the US, the Daubert standard requires scientific evidence to have been tested, peer-reviewed, and generally accepted, before admissibility.[82] The U.K. has created a relatively systemic approach by placing special emphasis regarding the responsibility of judges to screen expert evidence for reliability.[83] The European Union has proposed substantial transparency and accountability requirements for high-risk systems through its draft AI Act.[84]

[78] Indian Evidence Act, 1872, § 65B.
[79] Lawrence Lessig, *Code and Other Laws of Cyberspace* 56 (1999).
[80] Supra note 2.
[81] Supra note 7.
[82] Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579 (1993).
[83] *R v. Bonython*, (1984) 38 SASR 45 (Austl.).
[84] Proposal for a Regulation on Artificial Intelligence, COM (2021) 206 final (Eur. Comm'n).

These jurisdictions have room for improvement but at least they are iterating evidentiary rules in order to apply to the complexity of algorithms. Meanwhile, in India we have not yet moved the needle to recalibrate Section 65B.

### 4.2 Recommendations for a Proposed Section 65C

A practical solution would be to create a new section called Section 65C, relating specifically to AI-generated evidence. This new section could build on but also move beyond Section 65B by incorporating the following three conditions:

1. **Disclosure obligations:** If a party wants to rely on AI-generated evidence they would need to disclose the system's architecture, training data (to the extent feasible), error rates, and results of validation studies.[85]

2. **Judicial gatekeeping:** Judges would assess admissibility with a reliability assessment (aligned with a Daubert-style consideration) rather than solely be an assessment of certification.[86]

3. **Judicial bans and presumptions:** Some AI systems should be banned based on using "black box" systems such as predictive policing, while by contrast current validated forensic systems would be able to rely on a rebuttable presumption of reliability.[87]

Such framework prevents blind reliance on algorithmic outputs and gives courts structured tools to assess admissibility.

### 4.3 Draft Amendment Language

#### 4.3.1 Definitions (to be inserted in Section 3)

> **"Artificial Intelligence-generated evidence"** means any information, conclusion, or output produced wholly or partly by a system using machine learning, neural networks, or algorithmic decision-making.

[85] Cary Coglianese & David Lehr, Regulating by Robot: Administrative Decision Making in the Machine-Learning Era, 105 Geo. L.J. 1147, 1176 (2017).
[86] *United States v. Williams*, 506 F.3d 151 (2d Cir. 2007).
[87] Andrew Ferguson, *The Rise of Big Data Policing* 119 (2017).

**"Algorithmic system"** includes any automated system designed to process data and generate conclusions, predictions, or classifications without continuous human oversight.

### 4.3.2 Amendment to Section 45 (Expert Opinion)

After "science or art," insert:

*"or by an artificial intelligence system validated in accordance with prescribed standards."*

Insert a new Explanation:

*"For the purposes of this section, the court may admit outputs of algorithmic systems as expert opinion if accompanied by certification of reliability, validation studies, and error rates as prescribed."*

### 4.3.3 Amendment to Section 65B (Electronic Records)

Substitute sub-section (4):

*"An electronic record, including AI-generated evidence, shall be admissible if—*

(a) *it is accompanied by a certificate from the person responsible for the operation or maintenance of the device or system generating or storing such evidence, specifying the process by which it was produced;*

(b) *in the case of AI systems, the certificate shall also include—*

(i) *information on validation tests, accuracy rates, and known biases;*

(ii) *a statement on whether the system complies with technical standards notified by the Central Government; and*

(iii) *a declaration of human oversight in the generation of the evidence."*

### 4.3.4 New Section 65C (AI Evidence Oversight)

*"65C. (1) The Central Government may, by notification, designate a regulatory*

*authority to prescribe standards for the admissibility of AI-generated evidence.*

(2) *The authority shall publish guidelines on validation, certification, and disclosure of AI systems used in forensic or evidentiary contexts.*

(3) *Courts shall have discretion to exclude AI evidence where the system's reliability, transparency, or compliance with due process cannot be reasonably assured."*

### 4.4 Counterarguments

The argument has also been made regarding trial courts not being competent to assess AI systems.[88] Critics may be right, but objections similar to this one were raised at the time of the advent of DNA evidence in court cases. In the intervening period, training for judges and expert witnesses, and reliance on them has made assessed standards for DNA evidence. Judicial academies could provide a valuable or vital role in mentoring judges to interrogate AI evidence.[89]

Another counterargument might be that the disclosure duties might violate proprietary trade secrets. This is a valid argument, but not one that overrides fair trial rights. Courts may be able to craft orders of protection, similar to protective orders provided in U.S. federal courts allowing sensitive information to be made available natural before the public.[90]

### 4.5 Case Study Examples from India

The following examples indicate that the need for changes is urgent:

- **Delhi riots (2020):** The Delhi Police made use of facial recognition technology to identify suspects, with little disclosure as to accuracy or error rates.[91]
- **Deepfake evidence in Maharashtra (2021):** The courts were probing how to assess manipulated videos as evidence under Section 65B opening to doctrinal holes.[92]
- **Aadhaar authentication logs:** The logs were first introduced as evidence against main

[88] Richard Susskind, *Tomorrow's Lawyers* 144 (2019).
[89] S.C. Raina, Judicial Education and Training in India, 41 J. Indian L. Inst. 523 (1999).
[90] Fed. R. Civ. P. 26(c)(1)(G).
[91] Aparna Chandra, Facial Recognition and Indian Policing, 35 Nat'l L. Sch. India Rev. 77 (2022).
[92] Rahul Matthan, The Law and Deepfakes in India, 13 Indian J.L. & Tech. 65 (2021).

accused in criminal trials, notwithstanding significant concerns, related to the unreliability of biometric recognition systems as contained within Indian Supreme Court judgements.[93]

As evidenced by the cases, the courts were improvising with the straitjacket contained in the wording of Section 65B. A focused statutory amendment would delineate a much clearer, better principled regime.

### 4.5 Achieving Procedural Fairness

AI-based evidence adds exacerbation asymmetries between the prosecution and the defence. The state usually has the most access to specialist technicians and proprietary technology which can often render the defendant unable to adequately respond to algorithmically determined conclusions.[94] Legal reform should provide access to technical assistance (possibly through legal aid) for the defence.[95] Without this parity of arms, the reliance on AI based evidence would be contrary to due process.

### 4.6 A Balanced Reform

Section 65C should not pretend to be all-encompassing, but should provide a set of ideals for consideration, i.e., transparency, accountability, and fairness, and clarify that courts can contemplate the future in accommodating technologies.[96] This equilibrium could sustain the law without it being outdated in a few years.

## Chapter 5: CONCLUSION AND RECOMMENDATIONS

### 5.1 The Constitutional Stakes

Ultimately, the concern is not about technology but it is about rights. The Constitution guarantees equality, due process, and protection against arbitrary state actions.[97] Allowing AI evidences without any safeguards infringes these guarantees. The Supreme Court in the case of *Puttaswamy* emphasized informational privacy and accountability of the state in technology

[93] Usha Ramanathan, Aadhaar: A Biometric History of India's 12-Digit Identity, 55 Econ. & Pol. Wkly. 33 (2020).
[94] Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities, 81 Proc. Machine Learning Rsch. 1 (2018).
[95] Malavika Jayaram, The Constitutional Risks of Aadhaar-Based Evidence, 12 Indian J. Const. L. 89 (2019).
[96] Bharat Chugh, Artificial Intelligence and the Indian Evidence Act, 44 SCC Online J. 221 (2021).
[97] India Const. art. 14.

use.[98] Extending this principle to AI-generated evidence is not an extension but a practical necessity.

### 5.2 Key Recommendations

1. **Transparency as Baseline:** Courts must insist on disclosure of methodology, training data, and limitations.[99]

2. **Judicial Gatekeeping:** Following the spirit of *Arjun Panditrao*, courts should not admit AI evidence unless its reliability is demonstrated.[100]

3. **Defense Assistance:** Access to AI experts should be treated as integral to legal aid.[101]

4. **National Registry of Tools:** A statutory body could maintain a registry of validated AI forensic systems, with periodic audits.[102]

5. **Graduated Safeguards:** Different levels of scrutiny depending on risk—for example, higher scrutiny for predictive policing than for automated CCTV enhancement.[103]

### 5.3 The Role of Judicial Culture

Reform is not only statutory but cultural. Judges must approach AI evidence with humility and skepticism, resisting the allure of technological determinism.[104] Overconfidence in AI outputs—what some scholars call "automation bias"—can distort fact-finding.[105] Judicial education, cross-examination norms, and expert testimony must counter this bias.

### 5.4 Comparative Lessons

The experience of the United States shows the perils of building too much faith in proprietary risk assessment methods such as COMPAS which were criticized in State v. Loomis for which

[98] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).
[99] Daniel Schwarcz, Regulating Algorithmic Risk in Insurance, 89 U. Chi. L. Rev. 1405, 1420 (2022).
[100] Supra Note 1
[101] Marc Jonathan Blitz, The Right to an Explanation, 14 Ohio St. Tech. L.J. 43, 59 (2018).
[102] Proposal for a Regulation on Artificial Intelligence, supra note 84.
[103] Sandra Wachter et al., Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR, 7 Int'l Data Privacy L. 76, 82 (2017).
[104] Danielle Citron, Technological Due Process, 85 Wash. U. L. Rev. 1249 (2008).
[105] Cary Coglianese & David Lehr, Transparency and Algorithmic Governance, 71 Admin. L. Rev. 1, 19 (2019).

there was no transparency.[106] The United Kingdom demonstrates the need for checks on reliability prior to admission.[107] The EU's proposed AI Act shows how statutory frameworks can be used to create classifications of risk and impose duties.[108] India can learn from each model, but would need to make reforms applicable to its own constitutional context.

### 5.5. Final Thoughts

Evidence law is not just procedural; it shapes the lived experience of justice. An algorithm may seem neutral, but its mistakes fall squarely on real defendants. Unless the law reforms itself, Section 65B is bound to continue to stretch itself awkwardly over problems it was never meant to solve. A new Section 65C rooted in transparency and fairness will offer a way out.

Law need not inherently resist technology, but it must harness technology for justice. Courts, legislatures, and scholars must recognize AI in evidence not as a pernicious inevitability but as a function of human choice, conditioned and contingent on human values. Reform may not prevent all mistakes, but it would ensure that when mistakes are made that they are at least made through transparent and accountable processes and not blind faith in a machine.

[106] State v. Loomis, 881 N.W.2d 749 (Wis. 2016).
[107] *R v. Bonython*, supra note 83.
[108] Proposal for a Regulation on Artificial Intelligence, supra note 84.