
Driven Forensics and the Admissibility of Digital Evidence in Criminal Trial

Bhumika Batra
L.L.M Criminal Law
Amity University, Noida

ABSTRACT

This paper examines the admissibility of AI-generated forensic evidence in criminal trials. The growing adoption of AI presents promising results for investigative efficiency. Despite advancements, significant research gaps persist in practically understanding the legal limits of AI evidence in judicial processes. Existing literature lacks focused assessment of the evidentiary value of AI outputs. The objective of this study is to evaluate whether AI-generated evidence satisfies established legal standards of reliability. The methodology involves a comparative doctrinal legal analysis of evidentiary standards across common law jurisdictions. Preliminary results indicate that AI forensic tools can enhance scale of evidence analysis. However, challenges arise from reproducibility deficits. Courts exhibit variability in acceptance of AI evidence due to limited technical literacy and lack of standardized validation protocols. Liability implications reveal that developers and investigators may bear accountability for flawed outputs. This raises critical concerns related to wrongful conviction. The paper emphasizes the necessity of independent validation and, development of AI-specific admissibility criteria. Findings inform policy development for the responsible AI integration within criminal justice systems. The research advances the objectives of Sustainable Development Goal 16 by reinforcing equitable access to justice. Preliminary results contribute for a foundation for future empirical research in AI deployed criminal forensics.

Keywords: AI Forensic Evidence, Criminal Trial Admissibility, Algorithmic Bias, AI Evidence Reliability, Legal Liability of AI

INTRODUCTION

Artificial intelligence has rapidly permeated nearly every facet of modern criminal justice systems. It is particularly influencing forensic science. AI is transforming evidence collection and analysis in a variety of fields.¹ In digital forensics, algorithms retrieve and analyse data from electronic devices. AI is used in facial recognition systems. It aids in voice and handwriting pattern analysis. Predictive analytics are applied to reconstruct crime scenes.² This is possible due to AI's capacity to process enormous amounts of data and find hidden correlations. Police departments, prosecutors, and forensic specialists are using these technologies more and more to produce leads and even evidence in court.³ The main legal and scientific dilemma as law

¹ Esra Nur Bal & Aylin Yalcin Saribey, *Artificial Intelligence In Forensic Science: Applications, Legal Framework And Criminal Liability Regime*, In 2025 International Conference On Artificial Intelligence, Computer, Data Sciences And Applications (Acdsa) 1 (2025).

² RECOMMENDATION ON THE ETHICS OF ARTIFICIAL INTELLIGENCE (2021).

³ Ido Hefetz, *Integrating Ai Systems In Criminal Justice: The Forensic Expert As A Corridor Between Algorithms And Courtroom Evidence*, 5 *Forensic Sci.* 53 (2025).

enforcement implements these technologies is whether AI-generated forensic evidence can satisfy the accepted criteria of dependability and admissibility in criminal cases. Traditionally, courts have relied on human experts whose credentials, methods, and findings are subject to cross-examination. In contrast, jurors, judges, and attorneys find it challenging to understand how an algorithm arrived at a certain result because AI systems frequently function as “black boxes.”⁴ This paper explores the practical, ethical, and liability implications of relying on machine-generated outputs in criminal proceedings. The analysis is limited on admissibility and reliability rather than more comprehensive discussions of AI’s ethics or governance at the policy level. Adoption of AI without sufficient validation and legal control may jeopardise due process rights and erode public trust in justice, despite its vast potential to improve forensic efficiency and precision. UNESCO’s 2021 Recommendation establishes that explainability and accountability are essential for AI legitimacy. Therefore, this study is objected to find a path which strikes a compromise between technical innovation and long-term legal protections.

AI IN CRIMINAL FORENSICS

Overview of AI tools used in criminal investigations

Many AI-based tools are used in modern forensic practice to speed up and enhance investigation procedures. These algorithms use face recognition to identify criminals or missing people by comparing their recorded or real-time photos to an extensive database. The police departments in the United States and the United Kingdom have employed systems like Clearview AI, which illustrates the potential and controversy of the various automated identification techniques. AI algorithms help spot abnormalities and reconstruct human behaviour in digital forensics by helping investigators sort through terabytes of data, including emails, chat logs, social network posts, photos, and sensor data. Digital platforms use machine-learning algorithms that can easily identify the communication patterns, detect picture alteration, and cluster linked files. AI systems are used in predictive analytics and crime-scene reconstruction to simulate the events based on sensor inputs, ballistic trajectories, or digital traces. These systems often incorporate Bayesian networks or probabilistic reasoning to deduce expected outcomes. Furthermore, deep-learning architectures are used for the analysis of spectral and spatial information in voice and handwriting identification. In order to identify suspects in terrorist or ransom crimes, AI-driven speaker recognition has been investigated.⁵

i. Benefits of AI adoption

Using AI in forensic work has significant benefits. Machine-learning systems are notable for their speed. They can analyse large data sets in minutes. These can find connections that would take months for human analysts to find⁶. AI also promises consistency and objectivity. Once properly trained and validated, an algorithm applies uniform criteria to every case, potentially

⁴ Paul Grimm, Maura Grossman & Gordon Cormack, *Artificial Intelligence As Evidence*, 19 Northwest. J. Technol. Intellect. Prop. 9 (2021).

⁵ Stuart W. Hall, Amin Sakzad & Kim-Kwang Raymond Choo, *Explainable Artificial Intelligence For Digital Forensics*, 4 Wires Forensic Sci. E1434 (2022).

⁶ Roland Neil & Michael Zanger-Tishler, *Algorithmic Bias In Criminal Risk Assessment: The Consequences Of Racial Differences In Arrest As A Measure Of Crime*, 8 Annu. Rev. Criminol. 97 (2025).

reducing human bias and fatigue⁷. In digital forensics, AI classifiers can tag similar image clusters uniformly, improving reproducibility.

ii. Risks and limitations

Despite these advantages, bias, explainability, and data quality are major issues. Algorithmic prejudice is a persistent problem. According to a paper by Cuellar et al., when photos were degraded, top facial recognition algorithms misdiagnosed people from darker-skinned populations higher than those from lighter-skinned equivalents. These prejudices may directly result in erroneous detentions or misdirected investigations. Results are further compromised by errors resulting from data-quality issues, such as incomplete or incorrectly labelled training sets. The forecasts or correlations may not generalise when algorithms are programmed on datasets that are restricted by geography or demographic information. Buolamwini and Gebru's research revealed comparable differences in commercial face- analysis algorithms by gender and ethnicity.

The explainability problem exacerbates these dangers. Even their designers frequently struggle to completely understand deep learning systems, especially convolutional neural networks. This "black-box" aspect makes it highly challenging to examine in court, where opposing counsel must be able to question both the process and the outcome. According to a 2022 National Institute of Standards and Technology (NIST) special publication, AI-based forensic conclusions may lose their scientific legitimacy if they are not interpretable. Similar to this, the Artificial Intelligence Act 2024 of the European Commission classifies AI systems used for forensic and law enforcement applications as "high-risk". This classification requires human control. It also requires proper documentation. It further requires transparency. However, real-time biometric identification systems in public spaces are classified as "unacceptable risk". They are largely prohibited. But have limited exceptions for law enforcement. Collectively, these various risks underscore that AI in forensics is not inherently reliable. Rather its probative value depends entirely on robust transparent validation. It further depends on continuous human intervention.

OBJECTIVES OF THE STUDY

1. To examine the nature and scope of AI-driven forensic tools
2. To analyse existing legal frameworks governing digital evidence
3. To assess the reliability and scientific validity of AI-generated forensic evidence
4. To examine admissibility challenges posed by AI-based forensic evidence
5. To evaluate compliance of AI-driven forensic evidence with fair trial principles

OUTCOME OF THE WORK

o Reframing Admissibility Tests

Courts increasingly evaluate AI-generated digital evidence under traditional admissibility standards (relevance, authenticity, integrity, reliability), but with heightened scrutiny on:

⁷ Ibid

- Algorithmic transparency
- Error rates
- Validation and testing methods
- Human oversight

- **Chain of Custody Evolution**

The concept of chain of custody expands to include:

- Dataset provenance
- Model versioning
- Training history
- Audit logs of AI decision processes

- **Expert Testimony Requirements**

AI-driven forensic evidence typically requires expert witnesses who can explain:

- How the AI system functions
- Its limitations and biases
- The meaning of probabilistic outputs in legally comprehensible terms

LEGAL RELIABILITY STANDARDS

Trials must be based on techniques that have been scientifically established and outcomes that are resistant to criticism. The dependability of AI-generated outputs, such as image analysis, speech comparison, or predictive modelling, must be demonstrated to the same or even greater extent than that of conventional forensic methods when they are offered as evidence.

a) The Daubert Standard

The standard for the admissibility of scientific evidence was set in the 1993. This case was decided by the US Supreme Court. Trial judges act as gatekeepers under this standard. They evaluate the validity of the scientific process. They also assess the applicability of the process that supports expert testimony. The Daubert factors are as follows:

- (1) testability;
- (2) peer review and publication;
- (3) known or potential error rates;
- (4) the presence of standards governing the operation of the technology; and
- (5) widespread acceptability within the relevant scientific community.

All of these standards presents complex challenges when it comes to AI-based forensics. The quality and representativeness of the proprietary datasets used to “test” AI systems are frequently unknown to the court. Because commercial vendors protect algorithms as trade secrets, peer review may be restricted. Model drift, training data, and environmental factors can all affect error rates. As a result, without thorough independent validation, many AI tools can fall short of the Daubert criterion.⁸

⁸ Surya Gangadhar Patchipala, *Tackling Data And Model Drift In Ai: Strategies For Maintaining Accuracy During ML Model Inference*, 10 Int. J. Sci. Res. Arch. 1198 (2023).

Innovative scientific methods must first prove their acceptability and dependability. The idea is consistent with AI evidence that the court cannot assess the algorithm's dependability in a meaningful way until the algorithm's design, dataset, and validation procedure are revealed.⁹

b) The Frye Standard

The Frye test, which was derived from *Frye v. United States*¹⁰, was the governing standard in many jurisdictions prior to *Daubert*. It stipulates that the evidence must come from a scientific principle or finding that is "sufficiently established to have gained general acceptance in the particular field." Although the Frye test is still valid in some states and other common-law nations, it poses special difficulties for AI evidence because there isn't a single professional agreement in the "particular field" of forensic AI.¹¹

Artificial intelligence system is developing rapidly and frequently more quickly than professional associations are able to publish standards for accreditation. As a consequence, the popularity of a certain AI model does not necessarily translate into scientific acceptance. Therefore, in order to prevent popularity from being misinterpreted for dependability, courts must carefully balance innovation.¹²

c) International Approaches to Reliability

In the United Kingdom, the Forensic Science Regulator's statutory Code of Practice (2023) requires that all forensic methods must be demonstrably valid through method validation. The technical records must be maintained to ensure reproducibility by competent practitioners. Criminal Procedure Rules Part 19 requires expert evidence to be objective, unbiased, and sufficiently reliable for court admission. The U.S. Department of Justice's December 2024 report on AI in criminal justice emphasizes that AI-generated forensic evidence must meet established evidentiary standards for reliability, accuracy, and explainability. This particular to high-stakes applications. It is applicable in forensic analysis where errors can profoundly impact justice outcomes. These advancements reflect a global legal agreement that an AI system's dependability cannot be assumed only because it functions well in controlled settings; instead, it must be empirically and procedurally shown in a courtroom setting.

II. THE ADMISSIBILITY DILEMMA

The admissibility of AI-generated forensic evidence is closely linked to reliability but extends to procedural and constitutional dimensions. Apart from being reliable, evidence must also be pertinent, substantial, and acquired in accordance with due process. Courts must determine whether the admission of AI outputs that affect guilt determination violates the accused's right to a fair trial, which includes the rights to confront evidence and comprehend the foundation of conviction.

i. Authentication and Chain of Custody

The majority of evidentiary laws, such as the Federal Rules of Evidence (Rule 901) and the

⁹ Daniel Seng & Stephen Mason, *Artificial Intelligence And Evidence*, 33 *Singap. Acad. Law J.* 241 (2021).

¹⁰ *Frye V. United States*, 293 F. 1013 (D.C. Cir. 1923)

¹¹ FRAIGMAN KAYE, *SCIENCE LAW STANDARDS STATS: STANDARDS, STATISTICS AND RESEARCH ISSUES* (2002).

¹² Stanley Greenstein, *Preserving The Rule Of Law In The Era Of Artificial Intelligence (Ai)*, 30 *Artif. Intell. Law* 291 (2022).

Indian Evidence Act (Sections 65A–65B), require digital or electronic records to be authenticated in order to demonstrate that they are legitimate and unaltered. This entails confirming the data's provenance, the algorithm's integrity, and the analytical process's continuity in the case of AI evidence. The U.S. Department of Justice has advised that forensic algorithms be treated as instruments whose calibration, software version, and audit logs must be preserved and documented.

AI-based evidence have been instances of dismissed by courts because of inadequate documentation. The Wisconsin Supreme Court affirmed the use of the COMPAS risk-assessment algorithm for sentencing in *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016), although it also acknowledged transparency issues and cautioned that these systems cannot serve as the exclusive foundation for court decisions.

ii. Procedural and Constitutional Safeguards in Admitting AI Evidence

The admissibility of forensic evidence produced by AI presents foundational procedural issues. It also raises constitutional issues. These issues surpass basic scientific validity. Courts must protect the presumption of innocence. They must also protect due process. The defendant's right to a fair trial must be preserved. The right to a transparent trial must also be maintained. Automated decision-making technologies must not compromise these rights. The normative boundary that developing technologies must function within is formed by these protections.¹³

iii. Transparency and Explainability

According to the right to be heard principle of *audi alteram partem*, the accused must be given a meaningful chance to contest the evidence used against them. This right is weakened when AI systems function as “black boxes,” producing outcomes using opaque neural network topologies.¹⁴ It becomes arduous to challenge an AI's dependability if neither the defence nor the court can comprehend the logic underneath its output¹⁵ The court specifically acknowledged this issue in *State v. Loomis* (Wisconsin Supreme Court, 2016), cautioning that the defendant's capacity to contest the scientific validity of the COMPAS algorithm was restricted due to its proprietary nature. The ruling established a warning precedent for striking a balance between efficiency and transparency. Even, if the evidence was permitted.¹⁶

iv. Right to Confrontation and Cross-Examination

Every accused person has the right to confront witnesses. They also have the right to cross-examine witnesses. This right exists under the Sixth Amendment of the United States Constitution. It is also protected under Article 21 of the Indian Constitution. However, this right gets convoluted when AI systems function as algorithmic witnesses. A machine learning model

¹³ Brandon L Garrett & Cynthia Rudin, *The Right To A Glass Box: Rethinking The Use Of Artificial Intelligence In Criminal Justice*, 109 Cornell Law Rev. 561 (2024).

¹⁴ Chris Chambers Goodman, *Ai, Can You Hear Me? Promoting Procedural Due Process In Government Use Of Artificial Intelligence Technologies*, 28 Richmond J. Law Technol. 700 (2022).

¹⁵ Bryce Goodman & Seth Flaxman, *European Union Regulations On Algorithmic Decision Making And A “Right To Explanation,”* 38 Ai Mag. 50 (2017).

¹⁶ *State V. Loomis*, 881 N.W.2d 749 (Wis. 2016).

cannot be cross-examined by defendants. Also, the developers may decline to reveal proprietary source code due to intellectual property concerns.⁹⁸ In an effort to lessen this conflict, courts have required explainability reports or algorithmic audits prior to admitting evidence based on artificial intelligence. For example in the case of *Bridges v. South Wales Police* [2020] EWCA Civ 1058 the Court of Appeal determined that the use of facial recognition technology violated privacy rules. It also violated equality rules. This was due to inadequate transparency. It was also due to a lack of safeguards. The Metropolitan Police of the United Kingdom was put under judicial review.⁹⁹ These cases highlight the need for AI-generated forensic evidence to meet constitutional fairness requirements. They also show the need to meet scientific reliability requirements for the evidence to be admitted.

III. LIABILITY AND ETHICS

a) Attribution of Responsibility

When AI-generated evidence results in an erroneous conviction or acquittal of the accused persons, the dispersion of culpability among several players, including developers, law enforcement agencies, forensic specialists, and prosecutors, presents a unique challenge. Expert witnesses in traditional forensic science are accountable for the techniques they use.¹⁰⁰ In the United States, developers may be subject to product liability doctrine if an AI tool is determined to be unreasonably harmful in use or to have flawed design. However, if law enforcement organisations neglect to appropriately validate or interpret AI outputs, they may be considered responsible.

b) Ethical Dimensions

Admissibility is further complicated by ethical issues. The impartiality of criminal adjudication can be compromised by algorithmic bias, especially racial or gender bias. Commercial facial recognition algorithms misclassified darker-skinned women at rates of up to 34.7%, compared to 0.8% for lighter-skinned men. Article 14 of the Indian Constitution and the U.S. Fourteenth Amendment's protection of equality may be violated if biased algorithms generate evidence, such as voice matching or suspect identification. Evidence must be impartially produced in addition to being trustworthy in order to be considered due process. The idea of technical due process put out by academics is based on this moral precept.

IV. CONCLUSION AND RECOMMENDATIONS

In this contemporary era, artificial intelligence is rapidly transforming the criminal forensics technologies by offering significant unprecedented capabilities in data analysis, various pattern recognition, facial or voice identification, and crime-scene reconstruction. These advancements accelerate investigations while enhancing consistency. It potentially uncovers critical evidence that would otherwise remain hidden. However, there are many challenges with AI-generated evidence. Explainability is a major concern. Dependability is another concern. Legal professionals may find it challenging to fully comprehend the outcomes. Judges may also find it difficult. Jury members may struggle to scrutinise the outcomes. Algorithms have the potential to incorporate biases. They can reflect shortcomings in data quality. They may also function as opaque black boxes. A careful balance between technological innovation and fundamental legal

principles is required for the admissibility of AI-based forensic evidence. The liability considerations further complicate this landscape, as the responsibility for flawed AI outputs may be distributed across developers, forensic experts, and law enforcement agencies, which may result into raising both legal and ethical questions about accountability and impartiality of the flawed AI evidences. AI has the ability to improve the criminal justice system despite these obstacles if it is used carefully and with full accountability and transparency. The important things to be considered are the standardisation of evaluation frameworks, open procedures, ongoing human supervision, and interdisciplinary oversight combining legal, ethical, and technical knowledge, for integrating AI into forensic practice. Courts and investigative organisations can use AI to their advantage while upholding the integrity of these evidence. This will further lead to bolstering public trust in justice by including these protections. In the final analysis, it can be concluded that AI-generated forensic evidence is a promising field. But on the same part its full potential won't be realised until technological developments are accompanied by strict legal requirements, moral awareness, and careful application, guaranteeing that innovation advances justice rather than subverts it. To ensure effective integration of AI in criminal forensics, the following policies are proposed:

1. Establish clear liability attribution.
2. Product liability doctrines should apply to AI forensic vendors if systems are unreasonably dangerous or poorly designed.
3. Wrongful conviction remedies must address AI-generated errors with the same rigor as traditional forensic error.
4. Develop standardized AI validation protocols for forensic tools.