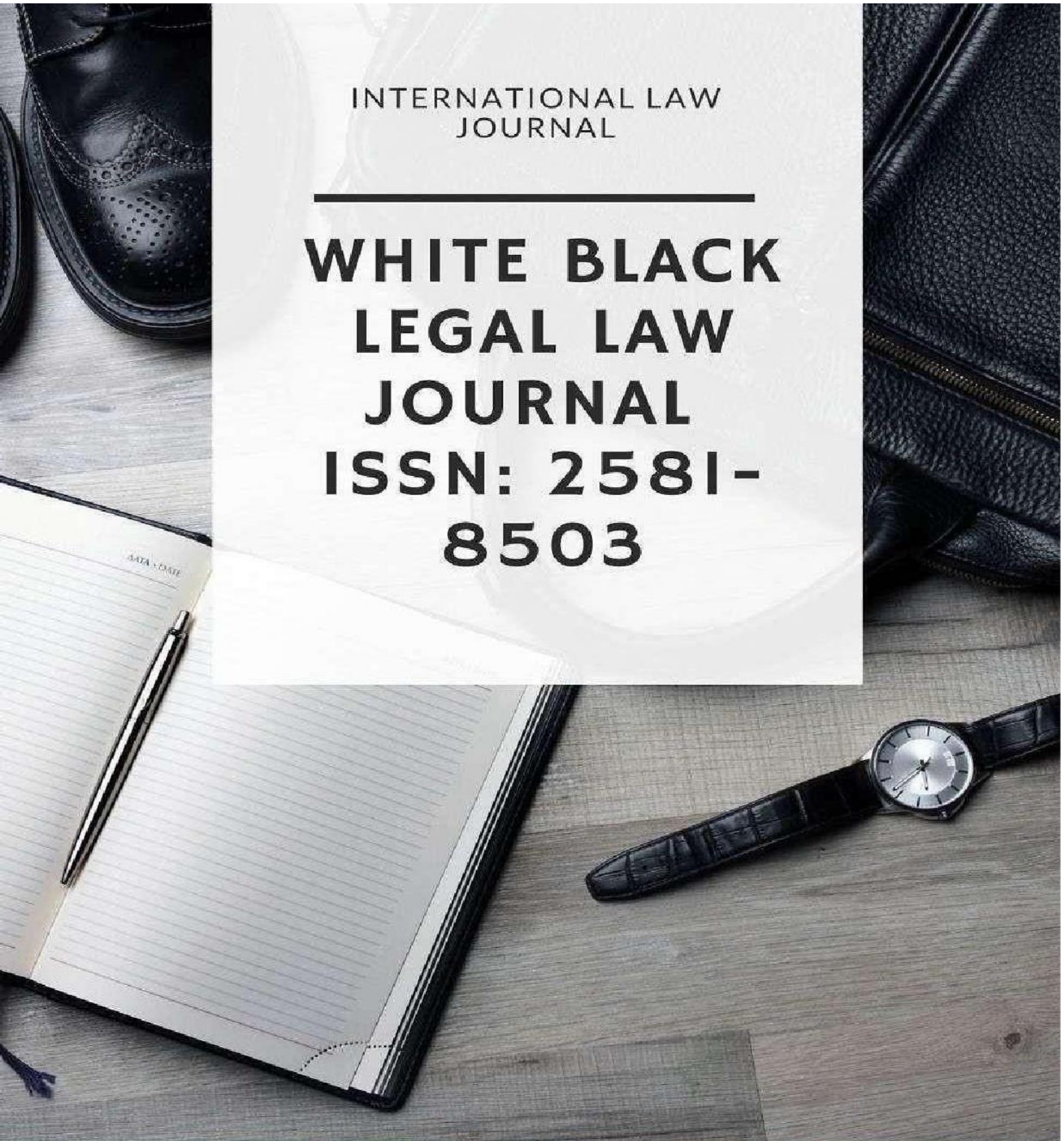




INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

ARTIFICIAL INTELLIGENCE AND DIGITAL EVIDENCE **IN CRIMINAL TRAILS: LEGAL CHALLENGES,** **ADMISSIBILITY AND FUTURE PROSPECTS IN INDIA**

AUTHORED BY - HARSHITA RAO¹

I. ABSTRACT

The rapid integration of Artificial Intelligence (AI) into criminal investigations and judicial processes has transformed the collection, analysis, and presentation of digital evidence. AI-powered technologies such as facial recognition systems, predictive analytics, automated surveillance, data mining, and digital forensic tool are increasingly being used by law enforcement agencies to detect crimes, identify suspects, and process vast amounts of electronic data. While these technologies enhance investigative efficiency and accuracy, they also raise significant legal, ethical, and procedural concerns regarding the admissibility, reliability, transparency, and authenticity of AI-generated evidence in criminal trails².

This research examines the evolving role of AI in the management of digital evidence within the Indian criminal justice system. It analyzes the legal framework governing electronic evidence, particularly under the Bharatiya Sakshya Adhiniyam, 2023³, and evaluates the challenges posed by algorithmic bias, lack of explainability, privacy violates, cybersecurity risks, and questions of accountability. The study further explores judicial approaches and relevant case laws concerning electronic and AI- assisted evidence, highlighting the need for safeguards to protect due process and the rights of the accused.

The paper argues that while AI has the potential to strengthen criminal investigations and improve evidentiary processes, its use must be accompanied by clear regulatory standards, transparent algorithms, independent audits, and robust procedural safeguards. By assessing contemporary legal development and future challenges, the study seeks to provide recommendations for balancing technological innovation with constitutional principles, fairness, and judicial integrity. Ultimately, the research contributes to the ongoing discourse on the admissibility and evidentiary value of AI genrated digital evidence and its implications for the future of criminal trails in India.

¹ LLB Student, Faculty of Law, MDUCPAS, Gurugram, Haryana, India

² Russell G. Smith et al., Artificial Intelligence and Criminal Justice (Springer 2020).

³ Bharatiya Sakshya Adhiniyam, 2023.

Keywords: Artificial Intelligence, Digital Evidence, Criminal Trials, Bharatiya Sakshya Adhiniyam, Electronic Records, Admissibility of Evidence, Digital Forensics, Criminal Justice System, India.

II. INTRODUCTION

The digital revolution of the late twentieth and early twenty-first centuries has fundamentally transformed the way individuals communicate, conduct business, store information, and interact with governmental institutions. In an increasingly interconnected world, a substantial portion of human activity now occurs through digital platforms, generating vast quantities of electronic data on a daily basis. Emails, digital signatures, CCTV recordings, call detail records, GPS logs, WhatsApp messages, social media posts, cloud-stored documents, and other forms of electronically generated information have become indispensable sources of evidence in contemporary legal proceedings. Consequently, courts are increasingly confronted with the complex task of determining the authenticity, reliability, evidentiary value, and admissibility of digital records.

The rapid expansion of information and communication technologies has also transformed the nature of criminal activity. Traditional crimes are now frequently facilitated through electronic devices, while entirely new forms of cybercrime have emerged. The widespread use of computers, smartphones, internet-based communication systems, and digital storage mechanisms has generated unprecedented challenges for legal systems across the world. As evidence increasingly exists in electronic form, conventional evidentiary principles designed for physical documents and oral testimony have often proven inadequate to address the unique characteristics of digital information, such as its susceptibility to alteration, duplication, and manipulation.

Recognising these challenges, the Indian legislature sought to modernise the law of evidence through the enactment of the Information Technology Act, 2000⁴, which introduced Sections 65A and 65B into the Indian Evidence Act, 1872⁵. These provisions established a special framework governing the admissibility of electronic records and represented a significant departure from traditional evidentiary rules. However, the practical application of these provisions generated considerable judicial controversy, particularly regarding the mandatory

⁴ Information technology act, 2000

⁵ Indian Evidence Act, 1872, ss 65A–65B.

certificate requirement under Section 65B(4)⁶. Divergent judicial interpretations led to uncertainty regarding the admissibility of electronic evidence and raised concerns about procedural complexity, evidentiary reliability, and access to justice.

In response to evolving technological realities and the need for comprehensive legal reform, Parliament enacted the Bharatiya Sakshya Adhiniyam, 2023 (BSA, 2023), as part of a broader restructuring of India's criminal justice framework⁷. Replacing the colonial-era Indian Evidence Act, 1872, the BSA seeks to modernise evidentiary rules and align them with the realities of a digital society. The legislation expressly recognises electronic and digital records within its definitional framework and attempts to streamline the legal regime governing their admissibility. Electronic records under the Act include data, records, images, sounds, information received or transmitted in electronic form, computer-generated documents, microfilms, and other forms of digitally stored information.

Despite these legislative developments, important legal questions remain unresolved. While the BSA, 2023, incorporates digital evidence into the evidentiary framework⁸, it remains uncertain whether the statute substantially reforms the law or merely reproduces the principles established under the previous regime. Questions concerning the authenticity, integrity, preservation, and evidentiary weight of electronic records continue to pose significant challenges for courts. Furthermore, the increasing use of emerging technologies such as artificial intelligence, automated surveillance systems, facial recognition software, predictive analytics, and digital forensic tools has introduced additional concerns regarding transparency, accountability, algorithmic bias, and procedural fairness.

The growing reliance on electronic and digital evidence has profound implications for criminal investigations, e-governance⁹, e-commerce, and judicial administration¹⁰. Government agencies, regulatory authorities, and law enforcement institutions increasingly depend upon digital records to establish facts, identify offenders, and support prosecutions. However, authenticating electronic evidence—including hard drives, mobile devices, social media communications, emails, instant messaging applications, websites, cloud-based data, and computer-generated outputs—remains a complex evidentiary challenge. The ease with which digital information can be modified, deleted, fabricated, or manipulated necessitates robust legal safeguards to ensure the credibility and integrity of such evidence.

⁶ Law Commission of India, 185th Report on Review of the Indian Evidence Act (2003).

⁷ Ministry of Home Affairs, Criminal Law Reforms Report (2023).

⁸ Bharatiya Sakshya Adhiniyam, 2023, ss 2(1)(e), 3.

⁹ Indian Journal of Law and Legal Research (IJLLR), Vol. VII, Issue VI (2025)

¹⁰ Journal of Informatics Education and Research (2026).

Against this backdrop, the present study critically examines the legal framework governing the admissibility of electronic evidence in India, with particular emphasis on the Bharatiya Sakshya Adhiniyam, 2023. It analyses the evolution of electronic evidence law, evaluates the effectiveness of the current statutory regime, and explores the practical and doctrinal challenges associated with the authentication and admissibility of digital records. The study further assesses whether the BSA, 2023, successfully addresses the shortcomings of the previous framework and is capable of responding to the demands of an increasingly technology-driven¹¹ justice system.

As society continues to migrate into the digital sphere, the future of criminal adjudication will increasingly depend upon the ability of legal institutions to adapt to technological innovation while preserving the fundamental principles of fairness, reliability, and due process. The admissibility of electronic evidence is therefore not merely a procedural issue but a critical determinant of the credibility and effectiveness of the modern criminal justice system.

III. ROLE OF AI IN DIGITAL EVIDENCE DURING CRIMINAL TRIALS

1. WHAT IS DIGITAL EVIDENCE:

Digital evidence refers to any information that is created, stored, transmitted, or processed through electronic devices and can be used to establish or disprove facts in a criminal investigation or trial. It includes electronic records such as emails, text messages, images, videos, audio recordings, internet browsing history, location data, social media communications, system files, and metadata. As a form of evidence, digital evidence plays a crucial role in modern criminal justice by helping investigators reconstruct events, identify suspects, and support legal proceedings.

The BSA significantly expands the scope of evidence by expressly recognizing electronic and digital records as "documents" under Section 3(d)¹², thereby granting them the same legal status, validity, and enforceability as traditional paper documents. The Act specifically includes emails, server logs, computer and smartphone records, electronic messages, websites, locational data, and voicemail messages within the ambit of documentary evidence. Furthermore, Section 2(e)¹³ broadens the definition of evidence by including statements given electronically as oral evidence, reflecting the realities of modern digital communication. Unlike

¹¹ Journal of Informatics Education and Research (2026).

¹² Bharatiya Sakshya Adhiniyam, 2023, s 3(d).

¹³ Bharatiya sakshya adhiniyam ,2023, s 2(e)

the Indian Evidence Act, 1872, which primarily contemplated physical documents and in-person witness statements, the BSA acknowledges the increasing importance of digital information in legal proceedings and provides a comprehensive framework for the admissibility and evidentiary value of electronic records.

2. UNDERSTANDING AI EVIDENCE:

Artificial Intelligence (AI) evidence refers to information or outputs generated by AI systems that are presented before courts or other legal authorities to establish or challenge facts relevant to a case. Unlike traditional forms of evidence, which are often based on direct human observation, testimony, or interpretation, AI evidence¹⁴ is produced through complex computational processes that analyze large volumes of data and generate conclusions, predictions, identifications, or assessments during bail hearings to forensic analysis generated by machine learning models.

The types of AI evidence commonly encountered in criminal trials include facial recognition outputs, predictive policing data, digital forensics from automated tools, and biometric identification systems. For instance, facial recognition software may identify a suspect from CCTV footage, while a predictive policing algorithm might generate data suggesting a higher probability of crime occurrence in certain areas, influencing investigative decisions. Additionally, AI-driven tools are increasingly used to analyze voice samples, fingerprints, and DNA evidence, with claims of higher accuracy and efficiency compared to traditional methods¹⁵.

Its distinguishing feature is that it originates from algorithmic decision-making rather than human judgment, making it a novel form of evidence that raises important questions regarding reliability, transparency, explainability, and fairness within the criminal justice system¹⁶.

IV. APPLICATION OF AI IN DIGITAL EVIDENCE

The implementation of artificial intelligence (AI)-based technologies in digital evidence analysis offers a diverse range of practical applications, which significantly contribute to the efficiency and accuracy of criminal investigations. These applications not only optimize traditional processes of identifying and classifying evidence, but also enable innovative approaches that would previously have been impossible to achieve in a reasonable time frame.

¹⁴ Brennan-Marquez, 'Artificial Intelligence as Evidence' (2021) *Yale Journal of Law & Technology*.

¹⁵ William & Mary Law School, filede@wm.edu

¹⁶ UNODC Practical Guide for Digital Evidence (2022).

or with limited human resources.

1. Facial Recognition Technology

Facial recognition technology has emerged as a powerful AI tool in criminal investigations, enabling law enforcement agencies to identify suspects by matching facial images captured through surveillance cameras with existing biometric databases. In India, initiatives such as the National Automated Facial Recognition¹⁷ System (AFRS)¹⁸ demonstrate the government's efforts to integrate this technology into policing and public security. The technology is particularly valuable in cases involving terrorism, missing persons, and wanted criminals, as it significantly accelerates the identification process and enhances investigative efficiency. The availability of large biometric databases, including Aadhaar records, further strengthens its utility.

2. Cybercrime and Digital Forensics

The passage discusses AI's crucial role in combating the growing challenge of cybercrime in India. With increasing internet penetration and digital transactions, crimes such as hacking, identity theft, online fraud, and ransomware attacks¹⁹ have become more prevalent. AI-powered digital forensic tools assist investigators by recovering deleted data, decrypting information, tracing online activities, and analyzing large volumes of digital evidence. Machine learning algorithms can also identify suspicious transaction patterns, detect fraud²⁰ in real time, and predict potential cyber threats before they occur. These capabilities significantly improve the speed and accuracy of cybercrime investigations and help law enforcement agencies respond more effectively to emerging threats.

3. Natural Language Processing (NLP) and Sentiment

Natural Language Processing (NLP)²¹ and sentiment analysis enable AI systems to examine large volumes of textual data, including emails, social media posts, and text messages, for investigative purposes. The passage highlights how these technologies help law enforcement

¹⁷ National Institute of Standards and Technology (NIST), *Face Recognition Vendor Test Reports*.

¹⁸ National Automated Facial Recognition System (AFRS), Ministry of Home Affairs, Government of India.

¹⁹ Navin Kumar, 'The Role of Artificial Intelligence in Criminal Investigations in India' (2025) 35(49) *Journal of Legal Studies* 98.

²⁰ Aishwarya Sharma and others, 'Artificial Intelligence in the Indian Criminal Justice System: Advancements, Challenges, and Ethical Implications' (2025) 5(1) *Journal of Lifestyle and SDGs Review*.

²¹ Gargi Singh and Utkarsh Verma, 'Justice in the Age of Algorithms: Artificial Intelligence, Data Privacy, Surveillance, and Digital Evidence in Criminal Adjudication' (2026) 2(5) *Naveen International Journal of Multidisciplinary Sciences* 31

agencies extract relevant information, identify communication patterns, classify documents, and detect potential criminal intent. Sentiment analysis further enhances this capability by assessing the emotional tone of written content, helps to identify signs of aggression, hostility, anxiety, or other emotions that may indicate criminal behavior or threats. These tools are particularly useful in addressing cyberbullying, hate speech, online radicalization, and terrorism-related activities, where language plays a central role in spreading harmful content. By enabling early detection of dangerous communications, NLP can contribute to crime prevention and public safety.

4. Metadata Extraction and Timeline Reconstruction

Metadata extraction²² and timeline reconstruction represent one of the most valuable applications of AI in digital forensics. Metadata, which includes information such as the creation date of a file, its location, the author, and the device used, can provide critical insights into the circumstances surrounding a criminal act. The passage explains that AI algorithms can automatically collect, organize, and analyze this metadata from large volumes of digital evidence. By integrating these data points into a chronological sequence, AI helps investigators reconstruct the timeline of events with greater accuracy and efficiency. This capability is particularly important for establishing when specific actions occurred, identifying the individuals involved, and tracing the progression of criminal activities.

5. Digital File Classification

Digital file classification refers to the use of AI systems to automatically categorize and organize electronic files according to their type and relevance to an investigation. As highlighted in the passage, intelligent algorithms can analyze the contents of files and determine whether they contain text, images, videos, audio recordings, or other forms of data. Beyond simple categorization²³, AI can also assess the potential evidentiary value of each file in relation to the investigative hypothesis. This capability is particularly useful in modern criminal investigations, where authorities often encounter enormous volumes of digital data²⁴. By prioritizing files that are most relevant, AI reduces the time and resources required for manual examination and enables investigators to focus on critical evidence more efficiently.

²² Justice Reimagined: The Role of AI in Modern Criminal Justice by Lisa Stolzenberg (Author), Stewart D'Alessio (Author)

²³ Giovanni Sartor and Karl Branting, 'Judicial Applications of Artificial Intelligence' (2020) 28 *Artificial Intelligence and Law* 1–17.

²⁴ Kevin Ashley, 'Artificial Intelligence and Legal Analytics' (2017) 25 *Artificial Intelligence and Law* 1–8.

Consequently, digital file classification enhances investigative productivity and accuracy.

6. Detection of Altered Documents

The detection of altered documents is a crucial forensic application of AI aimed at preserving the authenticity and integrity²⁵ of digital evidence. The passage explains that cybercriminals frequently manipulate electronic documents through editing, forgery, overwriting, or other unauthorized modifications to conceal their activities or mislead investigators. AI-powered technologies²⁶, particularly computer vision systems and digital signature analysis tools, can identify such alterations by detecting inconsistencies in document structure, formatting, embedded data, or security features. These systems can uncover signs of tampering that may not be easily visible to human investigators, thereby increasing the reliability of forensic examinations. The ability to verify whether a document has been modified is essential for ensuring that evidence presented in court is genuine and trustworthy.

7. Predictive Policing

Predictive policing²⁷ refers to the use of AI algorithms to analyze historical crime data and forecast where and when crimes are likely to occur. The passage highlights its growing adoption in Indian cities such as Delhi, Mumbai, and Bangalore to improve the allocation of police resources and enable proactive crime prevention. By examining factors such as past crime records, geographic patterns, time, and socioeconomic conditions, AI systems can identify crime hotspots and assist law enforcement in deploying personnel more effectively. The primary advantage of predictive policing is its potential to reduce crime rates and improve response times through data-driven decision-making.

V. ADMISSIBILITY OF AI EVIDENCE IN INDIA

1. LEGAL FRAMEWORK IN INDIA

A. LEGAL RECOGNITION OF ELECTRONIC EVIDENCE UNDER THE INFORMATION TECHNOLOGY ACT, 2000

Section 2(t)²⁸ of IT Act, 2000 defines “*electronic record*” as any record or generated data,

²⁵ OECD Artificial Intelligence in Society (2019).

²⁶ Aparna Chandra, ‘Artificial Intelligence and Constitutional Rights in India’ (2021) 17 *Indian Journal of Law and Technology*.

²⁷ Gargi Singh and Utkarsh Verma, ‘Justice in the Age of Algorithms: Artificial Intelligence, Data Privacy, Surveillance, and Digital Evidence in Criminal Adjudication’ (2026) 2(5) *Naveen International Journal of Multidisciplinary Sciences* 31

²⁸ Information technology act 2000, s2(t)

image or its stored, received or transmitted in electronic or microfilm format or computer generated microfilm.

Legal recognition of Electronic Record under *Section 4*²⁹ of the IT Act: Are displayed or available in an electronic form Accessible for use by another reference *Section 79A*³⁰ of IT Act, 2000 further mandates the Central Government to appoint an examiner of electronic evidence to provide an expert opinion before such document is presented before the court.

B. UNDER BSA

The admissibility of electronic evidence is dealt under *Section 61, 62 & 63* of the Bharatiya Sakshya Adhiniyam.

Section 61 – electronic and digital records

Section 61³¹ establishes the fundamental principle that electronic or digital records cannot be denied admissibility merely because they exist in electronic form. This provision places digital evidence on the same footing as traditional documentary evidence and reflects the realities of a technology-driven society. The section marks a significant shift from the traditional preference for physical documents by recognizing that modern transactions and communications largely occur through electronic means. However, the section does not grant automatic admissibility to all electronic records. Their legal validity and evidentiary value remain subject to compliance with the requirements prescribed under Section 63. Thus, Section 61 serves as the statutory foundation for the acceptance of electronic evidence in Indian courts.

Section 62 – Proof of Contents of Electronic Records

Section 62 acts as a procedural provision by specifying that the **contents of electronic records can be proved only in the manner prescribed under Section 63**³². The purpose of this section is to ensure uniformity and reliability in proving electronic evidence. Since digital records can be easily altered, copied, or manipulated, the legislature requires parties to follow the safeguards laid down in Section 63 before such evidence can be relied upon. Therefore, Section 62 functions as a link between the recognition of electronic evidence and the conditions necessary for its admissibility.

Section 63 – Conditions for Admissibility of Electronic Records³³

Section 63(1): Recognition and Admissibility of Electronic Records

²⁹ Information technology act 2000, s(4)

³⁰ Information technology act 2000, s(79)(A)

³¹ Bharatiya Sakshya Adhiniyam, 2023, ss 61 electronic and digital records

³² Bharatiya Sakshya Adhiniyam, 2023, ss 62 proof of content of electronic records

³³ Bharatiya Sakshya Adhiniyam, 2023, ss 63 conditions for admissibility of electronic records

This subsection provides the legal foundation for the admissibility of electronic evidence. It declares that information stored, recorded, copied, or printed from a computer, communication device, or other electronic medium shall be treated as a **document** and may be admitted as evidence without producing the original record, provided the statutory conditions are fulfilled. It is an exception to the traditional requirement of producing original evidence and facilitates the use of digital records in court proceedings.

Section 63(2): Conditions for Admissibility

This subsection lays down the safeguards necessary to ensure the reliability and authenticity of electronic records. The party relying on the evidence must show that:

- The device was regularly used for storing or processing information.
- The information was entered in the ordinary course of activities.
- The device was functioning properly during the relevant period.
- The electronic output accurately reproduces the original information.

These conditions help prevent the admission of manipulated or unreliable electronic records.

Section 63(3): Multiple Devices Treated as One System

This provision recognizes modern technological environments where information may be processed through multiple computers, networks, servers, cloud systems, or intermediaries. It treats all such interconnected devices as a **single computer system** for evidentiary purposes. This ensures that electronic evidence is not excluded merely because data has passed through several devices or networks before being produced.

Section 63(4): Certificate Requirement

This subsection mandates the submission of a **certificate** along with the electronic record. The certificate must identify the electronic record, explain how it was produced, provide details of the device used, and confirm compliance with the conditions under Section 63(2). It must be signed by a responsible person in charge of the system and may be supported by an expert. The certificate serves as proof of authenticity and reliability, making it a crucial requirement for the admissibility of electronic evidence.

C. UNDER BNSS

The BNSS recognizes the increasing role of technology in criminal investigations and incorporates several provisions facilitating the use of electronic evidence.

Section 176 BNSS³⁴, which mandates the recording of search and seizure proceedings through

³⁴ Bharatiya Nagarik Suraksha Sanhita, 2023, s 176.

audio-video electronic means wherever practicable. This enhances transparency and strengthens the evidentiary value of materials collected during investigations. Similarly, provisions relating to searches, seizures, and investigations allow law enforcement agencies to collect electronic devices such as computers, mobile phones, hard drives, servers, CCTV recordings, and other digital records that may contain relevant evidence.

The BNSS also encourages the use of **forensic investigation and scientific methods**³⁵, particularly in serious offences. Digital evidence recovered from electronic devices may be sent for forensic examination to establish authenticity, recover deleted data, analyze communications, and trace criminal activities. Proper preservation of the chain of custody under the BNSS is crucial because the admissibility of electronic evidence under the BSA depends upon proving that the evidence has not been tampered with.

Further, the BNSS permits the use of **electronic communication technologies**³⁶ during criminal proceedings, including electronic transmission of documents, electronic records of statements, and audio-video recording of investigative processes. These provisions reflect the legislature's intention to modernize criminal procedure and improve the reliability of digital evidence.

2. Conditions for Admissibility of AI Evidence

1. Relevance of the Evidence

AI evidence must be directly related to the facts in issue in a case. Evidence that has no connection with the dispute cannot be admitted merely because it was generated by an AI system.

Example:

In a robbery case, a facial recognition system identifies a suspect from CCTV footage near the crime scene. The AI output is relevant because it helps establish the identity of the accused. However, the suspect's unrelated social media activity would not be relevant unless it has some connection to the crime.

2. Authenticity and Integrity

The party producing the AI evidence must demonstrate that the record has not been altered, manipulated³⁷, or tampered with after its creation.

Example:

³⁵ M. Monir, Law of Evidence (latest Indian edn, Universal/LexisNexis)

³⁶ Justice Yatindra Singh, Cyber Laws (Universal/LexisNexis, latest edn)

³⁷ Justice Yatindra Singh, Cyber Laws (Universal/LexisNexis, latest edn)

Suppose an AI tool analyzes a suspect's phone and generates a report showing communication with a criminal organization. The prosecution must establish that the phone data remained unchanged from the time it was seized until it was analyzed. If there is evidence of tampering, the reliability of the AI report may be questioned.

3. Reliability of the AI System

The court must be satisfied that the AI technology³⁸ used is sufficiently accurate and dependable.

Example:

A fingerprint-matching AI system compares latent fingerprints from a crime scene with a national database and identifies the accused. Evidence showing that the system has been scientifically tested and has a high accuracy rate strengthens its reliability.

4. Transparency and Explainability (The Black Box Problem)

AI evidence must also satisfy the condition of transparency, meaning courts should understand how the AI arrived at its conclusion. Many AI systems function as “black boxes”³⁹, where even developers cannot fully explain the internal reasoning process. This creates legal difficulties because judges generally prefer evidence that can be logically examined and challenged.

Example:

Suppose an AI system predicts that a person is likely involved in organised crime based on behavioural data. If the court asks: “How did the AI reach this conclusion?” and investigators simply reply, “The software detected suspicious patterns but we cannot explain the reasoning,” the court may question admissibility. Judges cannot blindly trust technology without understanding the basis of its conclusions.

5. Compliance with Legal Requirements under the Bharatiya Sakshya Adhiniyam, 2023

Since AI evidence is usually stored electronically, it must comply with statutory requirements governing electronic⁴⁰ evidence. Courts may require: proof of source, proper storage, lawful collection, certification where necessary.

Example:

Suppose WhatsApp chats recovered from an accused’s mobile phone are analysed through AI software to detect conspiracy patterns in a fraud case. If investigators fail to produce proper records showing: where chats were recovered, how data was extracted, whether it remained

³⁸ Avtar Singh, Law of Evidence (Central Law Publications, latest ed.)

³⁹ Pavan Duggal, Guide to Cyber Laws, Information Technology Act and E-Commerce (latest edn)

⁴⁰ Aishwarya Sharma and others, ‘Artificial Intelligence in the Indian Criminal Justice System: Advancements, Challenges, and Ethical Implications’ (2025) 5(1) Journal of Lifestyle and SDGs Review

unaltered, the defence can challenge admissibility. However, when investigators maintain proper records and statutory compliance, courts are more likely to admit the evidence. Thus, procedural compliance protects reliability.

6. Chain of Custody

Another important condition is chain of custody, meaning there must be a proper record showing how evidence moved from collection to courtroom presentation.

Courts need assurance that evidence was not tampered with at any stage.

Example:

Suppose police seize a laptop in a cyber fraud case. The laptop data is: Collected by investigators, Sent to forensic experts, Analysed using AI software, Produced before court. If investigators fail to maintain records showing who accessed the laptop and when, the defence may argue that files were altered. However, if authorities maintain a documented chain proving the evidence remained secure, courts are more likely to accept it.

7. Expert Verification and Opinion

Since AI technology is highly technical, courts often depend on expert testimony⁴¹. Experts explain: how the AI system works, accuracy of results, possibility of manipulation, limitations of technology.

Example:

Suppose an accused denies involvement in an extortion call. Police use AI-based voice recognition software claiming the voice belongs to the accused. The defence disputes accuracy. In such a case, forensic voice experts may testify regarding: matching process, probability levels, reliability of results. Their testimony helps judges understand technical evidence.

8. Absence of Bias and Fairness

Courts also examine whether AI systems⁴² are fair and unbiased. Some AI systems may unintentionally discriminate due to flawed training data.

Example:

In some countries, facial recognition software incorrectly identified innocent persons because it worked poorly with certain facial features. Suppose an AI tool repeatedly misidentifies individuals from a specific demographic group. Such evidence may violate fairness and equality principles and courts may refuse to rely upon it.

⁴¹ Kritika Goyal and Shreya, 'The Future of Justice: Navigating AI's Ethical and Legal Maze in India's Criminal Justice System' (2026) Journal of Informatics Education and Research.

⁴² Kritika Goyal and Shreya, 'The Future of Justice: Navigating AI's Ethical and Legal Maze in India's Criminal Justice System' (2026) Journal of Informatics Education and Research.

VI. CONSTITUTIONAL ANALYSIS OF AI-GENERATED EVIDENCE

The use of **AI-generated evidence** in criminal proceedings raises significant constitutional concerns under **Articles 14, 20, and 21 of the Constitution of India**. While AI can improve efficiency and accuracy in investigations, its use must conform to the constitutional principles of fairness, equality, and due process that form the foundation of the Indian criminal justice system.

CHALLENGES AND VIOLATION UNDER COI

1. Violation of the Right to Privacy (Article 21)⁴³

The right to privacy was recognized as a fundamental right by the Supreme Court in Justice K.S. Puttaswamy v. Union of India⁴⁴. AI systems often rely on the collection and analysis of vast amounts of personal data, including facial images, biometric information, location records, social media activity, and communication data. Technologies such as facial recognition, predictive policing, and mass surveillance can monitor individuals without their knowledge or consent. Excessive or indiscriminate use of such technologies may amount to an unreasonable intrusion into personal privacy and autonomy, thereby violating Article 21⁴⁵.

Example:

If law enforcement agencies continuously monitor citizens through AI-powered facial recognition cameras in public spaces without adequate legal safeguards, it could lead to mass surveillance and infringe the constitutional right to privacy.

2. Violation of the Right to a Fair Trial (Article 21)

A fair trial requires that evidence used against an accused be transparent, reliable, and open to challenge. Many AI systems operate as "black boxes," meaning that even experts may not fully understand how a particular conclusion was reached. When an accused person cannot effectively challenge the methodology or reasoning behind AI-generated evidence, the fairness of the trial may be compromised.

The Supreme Court in Maneka Gandhi v. Union of India⁴⁶ held that any procedure affecting personal liberty must be just, fair, and reasonable. If courts rely heavily on opaque AI-generated evidence without allowing meaningful scrutiny, the constitutional guarantee of due process

⁴³ Constitution of India, art 21.

⁴⁴ Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

⁴⁵ Constitution of India, art 21.

⁴⁶ Maneka Gandhi v. Union of India (1978) 1 SCC 248.

may be undermined.

Example:

If an AI-based risk assessment tool labels an accused as "high risk" and influences bail decisions without explaining the basis of that conclusion, the accused may be deprived of a fair opportunity to contest the evidence.

3. Violation of Equality Before Law (Article 14)

AI systems learn from historical data. If that data contains social, economic, racial, caste-based, or policing biases, the AI may reproduce and amplify those biases. This can result in discriminatory treatment and arbitrary decision-making, contrary to Article 14⁴⁷.

Example:

A predictive policing system trained on historical crime data may repeatedly identify certain neighborhoods as high-crime areas because they were historically overpoliced. This could lead to disproportionate surveillance of residents in those areas, creating unequal treatment before the law.

4. Concerns Regarding Presumption of Innocence

The criminal justice system is based on the principle that every accused person is presumed innocent until proven guilty. AI systems that generate risk scores, predictive assessments, or behavioral predictions may indirectly influence investigators, prosecutors, or judges, potentially creating a presumption of guilt before evidence is fully examined.

Example:

If an AI tool predicts that a person is likely to commit future crimes, decision-makers may unconsciously treat that individual with greater suspicion, even when concrete evidence is lacking.

Therefore, from a constitutional perspective, the admissibility of AI-generated evidence cannot depend solely on compliance with statutory provisions such as the BSA. Courts must also ensure that the use of AI respects **due process, transparency, accountability, equality, and the right to a fair trial**⁴⁸. Judicial scrutiny of AI evidence is essential to prevent wrongful convictions, discriminatory outcomes, and violations of fundamental rights. In this way, constitutional safeguards act as an important check on the growing use of artificial intelligence in criminal justice.

⁴⁷ Constitution of India, arts 14.

⁴⁸ United Nations Office on Drugs and Crime (UNODC), *Practical Guide for Digital Evidence* (2022)

VII. JUDICIAL INTERPRETATIONS

Judicial Interpretation of the Admissibility of Electronic Evidence in India

The admissibility of electronic evidence in India has evolved significantly through judicial interpretation, particularly concerning the requirement of certification under Section 65B⁴⁹ of the Indian Evidence Act, 1872 (now reflected in Section 63⁵⁰ of the Bharatiya Sakshya Adhiniyam, 2023). The Supreme Court has progressively clarified the conditions under which electronic records may be admitted, balancing technological realities with evidentiary safeguards.

1. State (NCT of Delhi) v. Navjot Sandhu (2005)

In **State (NCT of Delhi) v. Navjot Sandhu**⁵¹, commonly known as the Parliament Attack Case, the Supreme Court adopted a liberal approach towards electronic evidence. The Court held that the absence of a certificate under Section 65B did not necessarily render electronic evidence inadmissible. It observed that electronic records could still be admitted through the provisions governing secondary evidence under Sections 63 and 65 of the Indian Evidence Act. The Court reasoned that electronic data is often stored on large servers and computer systems that cannot practically be produced before the court. Therefore, copies of such records could be admitted as secondary evidence. This judgment facilitated the admission of electronic evidence by emphasizing substance over procedural formalities.

2. Anvar P.V. v. P.K. Basheer (2014)

The legal position underwent a major transformation in **Anvar P.V. v. P.K. Basheer**⁵², where a three-judge bench overruled the approach adopted in *Navjot Sandhu*. The Court held that electronic records constitute a special category of evidence and must be proved strictly in accordance with Section 65B. It clarified that any electronic record sought to be introduced as evidence through a copy or computer output must be accompanied by the certificate prescribed under Section 65B(4). The judgment emphasized that compliance with the statutory requirements was mandatory and that electronic evidence could not be admitted through the general provisions relating to secondary evidence. This decision strengthened the authenticity and reliability requirements governing digital evidence.

⁴⁹ Indian evidence act ,1872, ss 65B

⁵⁰ Bharatiya Sakshya Adhiniyam, 2023 SS 63

⁵¹ State (NCT of Delhi) v. Navjot Sandhu (2005) 11 SCC 600.

⁵² Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473.

3. **Vikram Singh v. State of Punjab**

In **Vikram Singh v. State of Punjab**⁵³, the Supreme Court reaffirmed the principle laid down in *Anvar P.V.* and reiterated that electronic evidence is admissible only when accompanied by the requisite Section 65B certificate. The Court emphasized that procedural safeguards are essential to ensure the credibility and integrity of electronic records. By insisting upon compliance with Section 65B, the Court sought to prevent manipulation and fabrication of digital evidence.

4. **Shafhi Mohammad v. State of Himachal Pradesh (2018)**

A different perspective emerged in **Shafhi Mohammad v. State of Himachal Pradesh**⁵⁴, where a Division Bench adopted a more flexible approach. The Court held that the requirement of a certificate under Section 65B(4) is procedural in nature and may be relaxed where the party seeking to rely on the electronic record does not possess or control the device from which the evidence was obtained. The judgment recognized that strict insistence on certification could sometimes obstruct justice, particularly where obtaining the certificate was impossible. Consequently, the Court prioritized substantive justice over rigid procedural compliance.

5. **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)**

The conflicting views expressed in *Anvar P.V.* and *Shafhi Mohammad* were finally resolved in **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal**⁵⁵. A threejudge bench, speaking through Justice R.F. Nariman, reaffirmed the correctness of *Anvar P.V.* and overruled *Shafhi Mohammad*. The Court held that the certificate requirement under Section 65B(4) is mandatory whenever secondary electronic evidence is sought to be produced. The judgment distinguished between **original electronic records** and **secondary electronic copies**. Where the original electronic device itself is produced before the court, a certificate may not be necessary. However, where copies, printouts, or electronic reproductions are tendered, compliance with Section 65B(4) is essential. The Court thus restored certainty and uniformity in the law governing electronic evidence.

6. **Pegasus Surveillance Case (2021)**

is a landmark judgment that strengthened constitutional protections against excessive digital

⁵³ *Vikram Singh v. State of Punjab* (2017) 8 SCC 518.

⁵⁴ *Shafhi Mohammad v. State of Himachal Pradesh* (2018) 2 SCC 801.

⁵⁵ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.

surveillance. The Supreme Court held that the State cannot justify intrusion into citizens' privacy merely by invoking national security without adequate proof and judicial scrutiny. Relying on the principles established in *Puttaswamy (2017)*⁵⁶, the Court reaffirmed that the **right to privacy under Article 21**⁵⁷ is a fundamental right and that any restriction must satisfy the tests of legality, necessity, and proportionality.

The judgment is particularly significant in the context of **AI and digital evidence** because it recognizes the dangers posed by advanced surveillance technologies that collect and process vast amounts of personal data. The Court also highlighted the "chilling effect" of surveillance⁵⁸ on freedom of speech and expression under **Article 19(1)(a)**, observing that constant monitoring may discourage individuals from exercising their democratic rights.

From the perspective of AI-generated evidence, the case establishes that evidence obtained through intrusive technological surveillance must be examined not only for statutory admissibility but also for compliance with constitutional safeguards. Thus, the judgment reinforces the principles of **privacy, transparency, accountability, and fair procedure**, ensuring that technological advancements do not undermine fundamental rights.

VIII. CHALLENGES AND SUGGESTIONS

CHALLENGES AND SUGGESTIONS REGARDING AI AND DIGITAL EVIDENCE IN CRIMINAL TRIALS

Challenges

1. Authenticity and Reliability of Evidence

The increasing sophistication technologies⁵⁹ makes electronic. Evidence susceptible to alteration, fabrication, and manipulation. Consequently, establishing the authenticity and integrity of digital evidence remains a significant evidentiary challenge.

2. Emergence of Deepfakes

AI-generated deepfakes⁶⁰ have blurred the distinction between have blurred the distinction between genuine and fabricated evidence. Their potential misuse threatens the credibility of digital evidence and increase the risk of wrongful convictions.

⁵⁶ Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

⁵⁷ Constitution of India, art 21.

⁵⁸ Kanika Rathore, 'Artificial Intelligence and Criminal Justice' (2025) 7(6) *Indian Journal of Law and Legal Research*.

⁵⁹ Danielle Keats Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 *Washington Law Review* 1.

⁶⁰ Navin Kumar, 'The Role of Artificial Intelligence in Criminal Investigations in India' (2025) 35(49) *Journal of Legal Studies*.

3. Inadequate Legal Framework

Existing evidentiary laws were not designated to address the complexities of A-generated content and advanced digital technologies. This regulatory gap creates uncertainty regarding admissibility and evidentiary standards.

4. Algorithmic Bias

AI systems may reproduce biases embedded within training datasets, leading to discriminatory outcomes. Such biases can undermine the principles of fairness, equality, and due process in criminal proceedings.

5. Lack of Transparency

Many AI models function as opaque "black-box" systems⁶¹, making their making their decision making processes difficult to scrutinize. This lack of explainability raises concerns regarding accountability and procedural fairness.

6. Privacy and Surveillance Concerns

The extensive use of AI-powered surveillance technologies poses serious threats to individual privacy rights. Excessive data collection may result in disproportionate state intrusion and constitutional violations.

7. Chain of Custody Issues

The ease with which digital information can be copied or modified complicates the maintenance of a secure chain of custody. Any procedural lapse may compromise evidentiary reliability.

8. Technical Knowledge Deficit

The limited technological expertise of judges, lawyers, and investigators often hinders the effective assessment⁶² of AI-based and digital evidence, affecting the quality of judicial decision making.

Suggestions

1. Comprehensive Legal Reforms

Legislatures should formulate dedicated legal frameworks governing the collection, authentication, preservation, and admissibility of AI-generated⁶³ and digital evidence.

2. Adoption of Advanced Verification Tools

⁶¹ Navin Kumar, 'The Role of Artificial Intelligence in Criminal Investigations in India' (2025) 35(49) *Journal of Legal Studies*.

⁶² Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences' (2019) 35 *Computer Law & Security Review* 105121.

⁶³ OECD, *Artificial Intelligence in Society* (2019).

Law enforcement agencies should employ sophisticated forensic technologies capable of detecting manipulated or synthetic digital content, including deepfakes.

3. Promotion of Explainable AI

AI systems used within the criminal justice system should adhere to principles of transparency and explainability, enabling meaningful judicial scrutiny.

4. Capacity Building and Training

Regular training programmes⁶⁴ should be conducted for judges, prosecutors, investigators, and defence counsel to enhance technological competence and digital literacy.

5. Strengthening Digital Forensic Infrastructure

Investment in modern forensic laboratories and cybersecurity mechanisms is essential to ensure the integrity and security of digital evidence.

6. Standardisation of Procedures

Uniform protocols for the collection, preservation, and presentation, of digital evidence should be established to minimise inconsistencies and procedural errors.

7. Independent Auditing of AI Systems

Periodic audits by independent experts⁶⁵ can improve accountability, detect algorithmic bias, and enhance public confidence in AI-assisted criminal justice process.

8. Balancing Innovation with Rights Protection

The deployment of AI technologies must be accompanied by robust⁶⁶ safeguards that protect privacy, due process, and other fundamental rights while maintaining investigative efficiency.

IX. CONCLUSION

The growing integration of Artificial Intelligence and digital evidence into the criminal justice system has fundamentally transformed the investigation, prosecution, and adjudication of crimes. AI-driven technologies such as facial recognition systems, predictive analytics, automated surveillance, digital forensics, and data - processing tools have significantly enhanced the efficiency, speed, and accuracy of criminal investigations. At the same time, the increasing reliance on algorithm systems and electronically generated evidence has raised complex legal, ethical, and procedural concerns regarding admissibility, authenticity, reliability, privacy, and the protection of fundamental rights.

⁶⁴ OECD, Artificial Intelligence in Society (2019).

⁶⁵ NITI Aayog, National Strategy for Artificial Intelligence (#AIForAll) (Government of India, 2018).

⁶⁶ Cary Coglianese and David Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105 *Georgetown Law Journal* 1147.

This study demonstrates that while the Indian legal framework, particularly the provisions of the **Bharatiya Sakshya Adhiniyam, 2023**, has strengthened the recognition and admissibility of electronic evidence, substantial challenges remain. Issues such as algorithmic bias, lack of transparency and explainability, risk of manipulation, cybersecurity vulnerabilities, and the absence of uniform standards for AI-generated evidence may undermine the fairness of criminal trials if left unaddressed. Judicial scrutiny and procedural safeguards therefore become essential to ensure that technological innovation does not compromise the principle of due process and natural justice.

The analysis of relevant legal developments and judicial approach further highlights that AI should function as a tool to assist investigators and courts rather than replace human judgment. Human oversight, accountability mechanisms, independent audits of AI systems, robust data protection measures, and clear evidentiary standards are indispensable for maintaining public trust in the criminal justice process.

Ultimately, the future of AI and digital evidence in criminal trials lies in achieving a careful balance between technological advancement and constitutional safeguards. With comprehensive regulation, ethical governance, judicial awareness, and continuous technological oversight, AI can serve as a powerful instrument for enhancing the administration of justice while preserving fairness, transparency, and the rule of law. The effective integration of AI into criminal proceedings must therefore be guided not only by efficiency but also by the enduring principles of justice, accountability, and human rights.

WHITE BLACK
LEGAL