Page: 1758-1780 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 2

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.220

DIGITAL EVIDENCE, AI, AND CRIMINAL TRIALS IN INDIA: A CRITICAL ANALYSIS

Puneet Kumar Rastogi[1]

I. ABSTRACT

The operational framework of criminal investigations and trials in India is undergoing a structural transformation due to rapid advances in consumer electronics, cloud storage, encrypted communications, algorithmic databases, and artificial intelligence. Investigating agencies increasingly rely on data drawn from remote servers, mobile devices, transient messaging platforms, automated forensic systems, and synthetic-media environments to reconstruct criminal conduct. This paper undertakes a doctrinal and constitutional critique of the statutory framework governing electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023 (BSA), particularly the admissibility regime created by Section 63 and the certificate mechanism under Section 63(4). It argues that the BSA modernizes Indian evidence law by placing electronic records within the mainstream of documentary proof and by introducing clearer distinctions between primary and secondary electronic evidence. However, the paper also finds that the dual-certification model, while improving reliability through custodian and expert validation, may create practical burdens for police agencies and forensic laboratories unless supported by adequate infrastructure and standardized procedures. The analysis further examines the evidentiary risks posed by artificial intelligence, deepfakes, opaque forensic software, and machine-generated outputs. It contends that metadata verification and hash-value integrity, though essential, are insufficient where synthetic media is created as an original digital file. In such cases, courts must demand deeper forensic scrutiny, source-code accountability, error-rate disclosure, and algorithmic transparency. The paper concludes that Article 21's guarantee of fair trial and due process requires a right to meaningful challenge against automated or AI-assisted evidence, ensuring that technological efficiency does not override constitutional safeguards in Indian criminal trials.

[1] B.A.LL.B.(H), 9th Semester, Student at Faculty of Law, University of Allahabad (India). Email: rastogipuneet00@gmail.com

II. KEYWORDS

Bharatiya Sakshya Adhiniyam, Digital Evidence, Artificial Intelligence, Section 63(4), Deepfakes.

III. INTRODUCTION & RESEARCH METHODOLOGY

A. Structural Introduction & Contextual Background

The integrity of any criminal justice system is structurally dependent on the reliability of the tools it uses to reconstruct past events. For more than a century, Indian trial courts evaluated reality through the lens of the Indian Evidence Act, 1872 (IEA). This code was built entirely around an analog worldview where statements were spoken, agreements were stamped on paper, and evidence consisted of physical, tangible objects. The subsequent digital revolution completely upended this stable legal framework, moving human communications, financial exchanges, social interactions, and criminal operations into volatile, boundaryless networks of binary code. Today, the details of a crime are rarely found exclusively on a paper ledger or spoken from a witness stand; instead, they are recorded within cloud sync containers, mobile device logs, encrypted application storage, and network transport metadata files.

B. Statement Of Problem & Conceptual Framework

The core issue analyzed in this project is the deep structural disconnect between the rapid advancement of modern data storage systems or artificial intelligence models and the rigid, procedural laws used to govern their admission in criminal trials. While the BSA is progressive in its text, bringing digital logs directly into the definition of documentary evidence, its practical application creates severe procedural bottlenecks. Section 63 of the Act aims to establish clear rules for primary and secondary data classifications. However, the newly engineered Section 63(4) certificate introduces a mandatory dual-signature rule, requiring validation from both the active device user/ custodian and a certified forensic examiner. This creates a massive compliance burden for local police stations and state Forensic Science Laboratories, which are already understaffed and dealing with multi-year backlogs of electronic devices.

C. Significance Of Study & Legal Imperatives

This dissertation holds immediate practical and academic relevance as India's criminal justice system adapts to the structural overhauls mandated by the BSA, BNSS, and BNS. Judges, prosecutors, and defense counsel are currently operating within a blank slate, navigating a brand-new statutory landscape without a deep well of high court or apex court precedents to guide them. By providing a comprehensive, critical review of Section 63 of the BSA and its interaction with technical data capture methods, this study offers a clear framework for understanding the criteria for digital admissibility. It acts as a helpful analysis for legal professionals looking to ensure that critical electronic evidence is preserved and presented without risking sudden exclusion due to a technical misstep. Furthermore, by confronting the legal implications of artificial intelligence within criminal trials, this research addresses a major gap in modern Indian legal scholarship. While international legal bodies are actively creating standards to govern algorithmic proof, predictive policing outputs, and automated facial recognition systems, Indian legal literature remains largely caught up in older debates surrounding Section 65B of the IEA. This dissertation bridges that gap by connecting statutory language with technical concepts, ensuring that constitutional protections, particularly the right to a fair trial and algorithmic accountability under Article 21 are actively defended against the risks of hidden machine processes and AI fabrications.

D. Research Methodology & Doctrinal Boundaries

The methodology applied throughout this project is strictly doctrinal, analytical, and qualitative. It relies on a close statutory examination of Indian legislation, including the Bharatiya Sakshya Adhiniyam, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, and the historical Indian Evidence Act, 1872. The study tracks statutory changes by comparing old legislative provisions with their newly enacted equivalents to determine legislative intent and evaluate the real-world impact of these shifting rules on trial procedure. The research features a detailed review of

judicial precedents from the Supreme Court of India and state High Courts to understand the development of judicial attitudes toward electronic data verification and certificate compliance. To analyze the technical nature of artificial intelligence models, deepfakes, and cryptographic file security, the study integrates secondary technical sources. These include data standards from the National Institute of Standards and Technology (NIST), cyber-forensic manuals from the Centre for Development of Advanced Computing (CDAC), and peer-reviewed technical journals. This combined approach ensures that the legal arguments presented are grounded in technical reality.

IV. ELECTRONIC EVIDENCE: TECHNICAL ARCHITECTURE & VULNERABILITIES

A. Foundational Hardware Architecture

To properly track how electronic evidence works within a criminal trial, we must first look at its underlying technical characteristics. Unlike standard physical evidence such as a signed paper contract, an items log, or a tool used in a crime digital data is entirely intangible. It has no permanent physical form; instead, it consists of transient collections of binary digits, or bits (0s and 1s), stored on magnetic, optical, or semiconductor hardware. When a judge reviews an email or views a video file in court, they are not looking at the raw evidence itself. They are looking at the final visual output of an application processing background file sector. This fundamental distinction means that electronic proof is highly vulnerable to being modified, corrupted, or deleted, often without leaving any surface indicator on the main file.

B. The Architectural Value of Metadata Tiers

A critical part of any piece of digital proof is its metadata, frequently defined as "data about data." Whenever an action takes place on an electronic device whether a folder is created, an encrypted chat is sent, or a cell tower ping is logged the operating system automatically records background information about that transaction. This metadata includes parameters like user accounts, file size, device models, and exact

timestamps recording when the file was created, modified, or accessed. In criminal trials, this automated background metadata can be far more valuable than the content of the file itself.

C. The Volatility Hierarchy Protocol

The volatile nature of digital data presents significant challenges for police collection and evidence storage. Volatility refers to how easily data can be altered or lost when a device changes power states or is shut down. Computer memory operates on a strict hierarchy of volatility. Data held within Random Access Memory (RAM) and central processing unit (CPU) registers is highly volatile and disappear completely the moment the machine loses power. This volatile memory space often contains the most critical evidence, such as active encryption keys, running network connections, unbacked messaging logs, and executing malware strains. If an investigating officer uses older, physical preservation protocols and immediately pulls the power cord on a running computer, they risk permanently wiping this vital information, leaving behind only the static data stored on the main drive.

D. Non-Volatile Hardware Maintaining Routines

Conversely, data stored on traditional hard drives, solid-state drives (SSDs), and mobile flash memory are non-volatile, meaning it remains intact after the device is powered down. However, even non-volatile storage media is subject to automated internal alterations. Modern solid-state storage uses automated background system maintenance routines, such as "garbage collection" processes and TRIM commands, which permanently wipe deleted data sectors to maintain drive performance. To protect digital proof from these hidden internal changes, forensic examiners rely on cryptographic hashing algorithms. A hash function, such as SHA-256, acts as a permanent digital fingerprint for a specific file or an entire storage drive. The algorithm takes an input stream of data of any size and processes it into a fixed-length string of alphanumeric characters. This process is governed by two strict rules: it is deterministic, meaning the exact same dataset will always produce the identical alphanumeric hash value, and it possesses an "avalanche effect," meaning that altering even a single bit of data within a massive multi-gigabyte folder will result in

an entirely different hash output. In criminal investigations, calculating this cryptographic hash value at the immediate point of seizure establishes a reliable baseline integrity score. If an investigator images a smartphone's internal storage and generates a specific SHA-256 hash value, any subsequent forensic expert, defense counsel, or court official can run the same algorithm on that data image. If the final hash output matches the initial value exactly, it provides mathematical proof that the evidence has remained completely untampered with throughout transport, storage, and analysis.

V. HISTORY OF DIGITAL PROOF UNDER THE INDIAN EVIDENCE ACT, 1872

A. The Analog Evidence Era and Early Technical Adaptation

To trace how the newly enacted Bharatiya Sakshya Adhiniyam, 2023 arrived at its current form, we must first look at the historical developments and sharp judicial conflicts that emerged under the old Indian Evidence Act, 1872. Prior to the year 2000, the IEA contained no specific provisions designed to handle electronic data. When litigants attempted to introduce early computer printouts, tape recordings, or automated telephone logs, courts had to force these new formats into standard analog categories, treating them as oral statements or secondary paper documents. The first major statutory correction came with the Information Technology Act, 2000, which formally recognized electronic data by altering Section 3 of the IEA to include digital entries within the definition of "evidence." To control how this new type of evidence could be introduced at trial, the legislature created Sections 65A and 65B of the IEA. Section 65A served as a statutory guide, stating that the contents of electronic records must be verified using the rules laid down in Section 65B. Section 65B set up a strict gatekeeping mechanism, dictating that any data contained in an electronic record that was printed on paper or copied onto magnetic or optical media would be deemed a "document" and allowed into evidence, provided it satisfied a set of operational conditions.

B. The Era of Judicial Flexibility and Administrative Lapses

Despite the detailed rules written into Section 65B, Indian courts spent the next twenty years deeply divided over whether this electronic certificate was an absolute requirement. The first major interpretation came from a three-judge bench of the Supreme Court in State (NCT of Delhi) v. Navjot Sandhu (2005), commonly known as the Parliament Attack case. In this decision, the apex court took a relaxed view of the rules, holding that even if a party failed to produce a valid Section 65B certificate, electronic evidence could still be admitted under the general provisions of Sections 63 and 65 of the IEA, which controlled traditional secondary paper documents. The core conflict under the old IEA framework emerged from judicial attempts to treat volatile electronic data with the same procedural flexibility applied to physical documentation, completely overlooking the technical reality of digital replication and storage. This relaxed approach meant that secondary digital evidence, such as mobile detail records (CDRs) printed out by cellular operators, could be let into the record solely based on the oral testimony of a police officer or company clerk who claimed the printout was accurate. While this flexible approach made the prosecution's job easier in complex conspiracy cases, it overlooked the technical reality of digital data. By treating volatile digital outputs exactly like stable paper documents, the court removed the key procedural checks designed to catch tampering or errors, creating a dangerous loophole where unverified or altered data could be used in major criminal trials.

C. The Restoration of Strict Statutory Gatekeeping

Recognizing these serious procedural risks, a three-judge bench of the Supreme Court explicitly overturned the Navjot Sandhu approach in the landmark case of Anvar P.V. v. P.K. Basheer (2014). In this ruling, the apex court restored the strict separation of electronic evidence rules, declaring that Sections 65A and 65B operated as a complete, self-contained code that entirely shut out the general secondary evidence rules for digital data. The court held that if a party sought to introduce secondary electronic data, producing a Section 65B (4) compliance certificate was a mandatory requirement that could not be waived through ordinary secondary-evidence principles. The reasoning behind the Anvar P.V. ruling was tied directly to how easily digital files can be manipulated. The court noted that

electronic records are highly vulnerable to background alterations, meaning that allowing them into a trial without strict validation certificates would undermine the integrity of the judicial system. This ruling caused a major shift in everyday trial practice: any electronic printout or data copy introduced without a signed compliance certificate became vulnerable to exclusion, forcing police units and private litigants to meet a much higher standard of technical compliance.

The temporary relaxation introduced in Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801, created a significant doctrinal interruption in this strict framework. In Shafhi Mohammad, the Supreme Court permitted an exception where a party was not in possession or control of the device from which the electronic record was produced, thereby reducing the practical rigidity of the Section 65B certificate requirement. However, this permissive position was later expressly disapproved by the three-judge bench in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1. The Court reaffirmed Anvar P.V., held that the certificate under Section 65B (4) is a condition precedent for admitting secondary electronic evidence, and declared the contrary clarification in Shafhi Mohammad to be incorrect law. This clarification completed the jurisprudential movement from the flexible Navjot Sandhu model to the strict statutory gatekeeping model, forming the doctrinal foundation for the heightened compliance logic now reflected in Section 63(4) of the BSA.

VI. STATUTORY OVERHAUL: DEFINING PRIMARY AND SECONDARY EVIDENCE UNDER BSA

A. The Architectural Dismantling of Colonial Hierarchies

The implementation of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) represents a major shift designed to bring India's law of evidence into alignment with the modern digital ecosystem. Instead of merely pasting new tech-focused clauses onto an outdated colonial framework, the BSA completely updates how electronic records are classified and processed within criminal trials. The old Indian Evidence Act, 1872 treated physical objects and paper sheets as the standard form of documentary proof, treating digital entries as a secondary category that always

required special verification under Section 65B. The BSA dismantles this old hierarchy, elevating electronic records to ensure they stand on equal footing with traditional physical documentation. This major re-engineering begins in Section 2(1)(d) of the BSA, which completely redefines the term "document." Under this updated definition, a document explicitly includes any electronic or digital record that is printed, stored, or copied onto any media format. By moving electronic records directly into the foundational definition of documentary evidence, the legislature has removed the historical distinction that treated digital files as inherently inferior or separate. This integration signals a clear legislative intent: in modern Indian criminal trials, a digital data file is legally equivalent to a signed paper document, provided its core authenticity can be reliably established.

B. Technical Realignment of Primary Evidence Frameworks

To understand how this new classification functions in practice, we must examine the updated distinction between primary and secondary electronic evidence established under Section 57 and Section 61 of the BSA. Under the old IEA framework, a digital file was almost always categorized as secondary evidence because it had to be transferred from its original device onto an external medium, such as a CD-ROM or printed paper, to be presented in court. This process triggered an automatic requirement for a compliance certificate. The BSA updates this model by expanding the definition of primary evidence to include original digital sources. Under the new provisions, if an electronic record is created or stored simultaneously across multiple devices, or if it exists within a system that automatically replicates data across local and cloud environments, each output qualifies as primary evidence. For instance, if a financial ledger is automatically mirrored across an office laptop, an enterprise server, and a cloud backup database, the files on each of these endpoints are considered primary originals. This update eliminates the need to track down a single “original” hard drive-in complex network environment, allowing investigators to introduce a direct forensic clone from any of the synchronized endpoints as primary proof.

Furthermore, the BSA introduces explicit statutory recognition for data stored

within semiconductor memory architectures, such as smartphones, solid-state drives (SSDs), and tablet devices. The old IEA text referred primarily to traditional "magnetic or optical media," which reflected the floppy disks and CD-ROMs of the late twentieth century. By updating the language to cover modern storage hardware, the BSA ensures that logs, encrypted chat data, and location history extracted directly from a smartphone's flash memory can be treated as primary documentary evidence. This expanded definition means that if an investigating officer seizes an original smartphone used in the commission of an offense, the data contained within that device's local memory chips can be presented directly as primary evidence. This change reduces the systemic reliance on the secondary certificate process in cases where the original hardware itself is secured and brought before the court, streamlining the introduction of digital evidence while maintaining a focus on sourcing proof from the original device.

C. Tabular Dissection of Statutory Variations

EVIDENTIARY METRIC	OLD INDIAN EVIDENCE ACT, 1872 FRAMEWORK	NEW BHARATIYA SAKSHYA ADHINIYAM, 2023 FRAMEWORK
Definition of "Document"	Restricted primarily to physical paper, inscriptions, or stone carvings.	Includes electronic and digital records directly under Section 2(1)(d).
Primary vs. Secondary	Digital files were almost always secondary, requiring strict proof of the origin medium.	Expands primary options under Section 57 to include live synchronized cloud and local copies.
Certificate Scope	Single signature required under Section 65B (4) from system custodians.	Dual signature is mandatory under Section 63(4) (splitting into Part A & Part B checks).

Hardware Scope	Limited to outdated definitions of "magnetic or optical media."	Modernized to explicitly include smartphone semiconductor flash storage arrays.

To systematically unpack the operational evolution between the colonial evidence regime and the modern, technological architecture of the BSA, the following comparative matrix presents a detailed textual dissection:

VII. THE SECTION 63(4) CERTIFICATE REGIME: PART A & PART B MECHANICS

A. Constitutional Mandates: Articles 20(3) And 21 of the Indian Constitution

The application of procedural rules to digital evidence cannot occur in isolation from the foundational constitutional protections guaranteed under Part III of the Constitution of India. When an investigating agency seizes a suspect's smartphone, laptop, or private cloud account, it directly engages two core constitutional rights: the protection against self-incrimination under Article 20(3), and the right to privacy and a fair trial under Article 21. The intersection of technology and constitutional criminal procedure requires a careful balance between the state's interest in securing evidence and the individual's right to be protected from unlawful intrusion.

The scope of Article 20(3), which provides that no person accused of an offence shall be compelled to be a witness against himself, was evaluated by the eleven-judge bench of the Supreme Court in State of Bombay v. Kathi Kalu Oghad. The Court distinguished between the compulsory production of physical or identifying material and compelled testimonial communication drawn from the accused's personal knowledge. In the digital context, however, the application of this distinction to smartphone passwords, passcodes, and biometric unlocking remains unsettled. One view, consistent with the reasoning in Selvi v. State of Karnataka, treats compelled disclosure of an alphanumeric passcode as testimonial because it requires the accused to communicate the contents of the mind. A contrary view was adopted by the Karnataka High Court in Virendra Khanna v. State of Karnataka, where the Court, relying on Kathi Kalu Oghad, treated compelled assistance in

unlocking digital devices as non-testimonial and therefore outside the direct protection of Article 20(3). The Delhi High Court in Sanket Bhadresh Modi v. CBI later adopted a more rights-protective approach, observing that an accused cannot be coerced during trial to reveal passwords or similar details in view of Article 20(3). Therefore, no definitive Supreme Court ruling has yet conclusively resolved whether passcode compulsion in the digital-device context is testimonial or physical in character. This unresolved conflict represents a serious constitutional gap in India's digital-evidence framework.

Simultaneously, the right to privacy, recognized as an integral part of the right to life and personal liberty under Article 21 by the nine-judge bench in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), places strict limits on digital search and seizure. A modern smartphone contains an individual's entire personal history, including financial transactions, private conversations, medical data, and location logs. Allowing law enforcement agencies to perform broad, unrestricted extractions of a device's storage without targeted warrants violates the principle of proportionality established in the Puttaswamy ruling. A fair trial under Article 21 also requires that the methods used to collect and analyze digital evidence are fully transparent. If an investigating agency uses proprietary software to extract data or relies on automated algorithms to link a suspect to a crime, the defense must have a meaningful opportunity to examine and challenge those tools. If the mechanisms used to validate electronic evidence are kept hidden behind corporate secrets, the trial loses the transparency required by due process, converting the constitutional right to a fair trial into an empty promise.

B. Overlapping Statutory Spheres: The Information Technology Act, 2000

The procedural processing of electronic proof under the BSA must be read alongside the regulatory frameworks established by the Information Technology Act, 2000 (IT Act). The IT Act functions as the core regulatory text for the digital ecosystem in India, defining cyber infractions, electronic signatures, and the duties of data intermediaries. Crucially, Section 79A of the IT Act empowers the Central Government to designate specialized agencies and institutions like Central

Examiners of Electronic Evidence. These accredited laboratories provide expert opinions on digital data integrity, hash values, and file authentication within judicial proceedings. This technical certification system creates a direct link between IT Act standards and BSA admissibility rules. When a cyber forensic expert signs a compliance certificate under the new BSA rules, their formal authority and the validation of their testing methods are grounded in the standards maintained under the IT Act. Furthermore, Section 79 of the IT Act governs the data retention obligations of intermediaries like internet service providers and messaging platforms. If an investigating officer fails to follow the correct statutory timelines for serving data preservation notices under Section 94 of the BNSS, the intermediary may routinely delete the background server logs, permanently destroying the metadata required to validate the evidence.

C. Primary Vs. Secondary Electronic Evidence Under the BSA, 2023

As analyzed in Chapter 4, the BSA fundamentally re-engineers how electronic evidence is categorized. However, the practical application of this framework requires a precise evaluation of when an electronic record qualifies as primary evidence under Section 57, versus when it is relegated to secondary evidence under Section 63. This boundary determines whether a party can introduce data directly, or whether they must first produce a compliance certificate to clear the admissibility hurdle. An electronic record qualifies as primary evidence when it represents the original output generated by a system or is stored directly within the source device's internal memory chips. For example, if a company uses an automated network security tool that automatically records system intrusions across a distributed ledger or a synchronized multi-server database, each synchronized instance functions as an original primary record. This recognition accounts for the architecture of modern enterprise systems, where data does not live on a single hard drive but is spread across automated network environments. In this scenario, producing a verified data clone from any of the synchronized endpoints satisfies the primary evidence standard, allowing the data to be evaluated without an immediate certificate requirement.

Conversely, an electronic record falls into the secondary evidence category under Section 63 when it is exported, printed, or copied from the original storage system onto an external medium for use in court. This scenario applies to the vast majority of digital evidence used in standard criminal trials, such as mobile call history printouts, WhatsApp chat backups exported to a flash drive, or security video copied onto a DVD-ROM. The moment data undergoes this transfer process; it is exposed to potential modification or loss of structural metadata. The law therefore applies a strict filtering mechanism: secondary electronic data cannot be considered by the court unless it is accompanied by a valid compliance certificate.

D. The Joint Signature Mandate: Part A And Part B Certification Under Section 63(4)

The most significant operational change introduced by the BSA is found within the text of Section 63(4), which establishes a revised certificate regime that completely replaces the old Section 65B(4) framework of the IEA. Under the previous law, a compliance certificate required only a single signature from the person in lawful charge of the device or computer system, which frequently led to disputes regarding the signer's technical competence. To address this, Section 63(4) introduces a dual-signature mandate, requiring the certificate to be explicitly split into two functional technical components to verify execution: Part A (User / Device Custodian Certification) and Part B (Independent Forensic Expert Validation).

Part A must be executed by the person in lawful charge of the management, daily operation, or direct custody of the device, computer system, or network synchronization environment from which the electronic record was drawn. Part B must be executed by a certified cyber forensic expert or an accredited Examiner of Electronic Evidence under Section 79A of the IT Act. They must independently verify the cryptographic hash extraction. This dual-signature requirement is designed to significantly improve the reliability of digital evidence introduced in criminal trials. By requiring an independent expert to validate the data capture, the law aims to eliminate the historical problem where police officers or corporate officials with limited technical training signed off on complex data transfers that accidentally

altered or corrupted underlying metadata fields. However, this updated requirement introduces immediate structural and logistical challenges within India's criminal justice system. For standard local police stations handling hundreds of routine cases, securing an independent, certified cyber forensic expert to attend every local device seizure or validate every exported data file creates an immediate bottleneck. India's state Forensic Science Laboratories (FSLs) are already facing extensive backlogs, with devices often waiting months or years for formal forensic imaging. If trial courts enforce the dual-signature requirement strictly from the early stages of a case, a failure to secure the co-signature of a certified expert at the time of data collection could result in critical digital proof being ruled completely inadmissible.

E. Cryptographic Integrity: Metadata, Cryptographic Hash Values, And Chain Of Custody Secure Mechanics

To satisfy the demanding standards of Section 63, an investigating agency must maintain a complete, forensically sound record of data integrity, a process governed by the mechanics of the digital chain of custody. This process requires documenting every handoff, access attempt, and transfer of a digital device or file from the exact moment of seizure to its final presentation in the courtroom. Under the procedural provisions of Section 105 and Section 176 of the BNSS, 2023, this chain of custody is reinforced by mandatory requirements for videographing search and seizure operations and utilizing forensic teams for serious offenses. The baseline technical tool used to verify this chain of custody is the continuous logging of cryptographic hash values. Once isolated, the device's storage must be imaged using an accredited forensic tool that creates an exact bit-stream clone of the drive while utilizing a physical or software-based write-blocker to prevent any data modification.

The forensic imaging tool automatically processes the captured bit-stream to generate a unique cryptographic hash value, such as a SHA-256 output. This hash score must be recorded directly onto the seizure memo and included within Part B of the Section 63 compliance certificate. When the data image arrives at the state Forensic Science Laboratory, the examiner must recalculate the hash value before beginning their analysis. If the initial hash matches the secondary hash exactly, it

provides mathematical proof that the contents of the drive remained completely unaltered during transport. If the hash values do not match, it indicates that a bit-level modification has occurred, breaking the chain of custody and compromising the reliability of the evidence. By embedding these cryptographic requirements directly into the statutory certificate templates, the new framework ensures that mathematical validation serves as the primary standard for verifying the integrity of digital proof within Indian courts.

VIII. THE AI CONUNDRUM: DEEPFAKES, OPAQUE CODE & FAIRNESS STANDARDS

A. Algorithmic Transparency & The "Black Box" Admissibility Problem

As the legal system adapts to the digital tracking models of the BSA, it faces a more complex technological challenge: the integration of Artificial Intelligence (AI) models within the criminal justice ecosystem. This challenge manifests in two distinct ways: the introduction of machine-generated output as evidence within trials, and the use of algorithmic tools by law enforcement to identify suspects and predict behavior. At the core of this integration lies the "Black Box" problem, a structural characteristic of advanced deep learning networks where the system's internal decision-making path is too complex to be interpreted or explained by human observers. The legal dangers of algorithmic opacity within forensic science are clearly detailed in a joint report by INTERPOL and the United Nations Interregional Crime and Justice Research Institute (UNICRI) titled "Towards Responsible AI Innovation" The report warns that integrating artificial intelligence into law enforcement including automated data sorting, predictive policing, and facial recognition functions as a double-edged sword that can infringe on fundamental human rights if left unchecked.

Specifically, the report emphasizes that using "Black Box" machine-learning models to analyze forensic evidence can directly undermine core legal principles, including the presumption of innocence, the privilege against self-incrimination, and the standard of proof beyond a reasonable doubt. Traditional expert evidence under Section 45 of the IEA (and its modern equivalent in Section 45 of the BSA) relies on the expert's ability to clearly explain the underlying logic and testing methods that

led to their conclusions, allowing the court to evaluate the reliability of the output. Advanced machine learning models operate through complex layer topologies that adjust weights across billions of separate parameters. When these networks flag a specific suspect or analyze biometric data, they do not provide a transparent step-by-step reasoning path. This lack of transparency directly conflicts with the fundamental right to a fair trial under Article 21, as an accused person cannot meaningfully cross-examine an opaque machine algorithm, creating a dangerous gap in procedural accountability.

B. Detection, Authentication, and Verification of Deepfakes and Synthetic Media Under Section 63 BSA

The emergence of advanced generative AI models presents an immediate threat to the integrity of digital evidence by allowing for the creation of highly realistic "deepfakes." These synthetic audio files, manipulated videos, and fabricated images are generated by pitting two neural networks against each other, a generator that creates fake data and a discriminator that tests it against real-world parameters until the output is indistinguishable from reality. This technology undermines the historical assumption that video recordings or audio tracks provide a reliable, objective record of real-world events. This development complicates the application of Section 63 of the BSA. Traditional electronic authentication relies on metadata verification and hash-value tracking to prove that a file has not been altered since it was recorded. However, when an individual uses a generative AI model to synthesize a completely fabricated video of a suspect committing a crime, the resulting file is an original creation of that software. Its metadata and cryptographic hash values are perfectly intact and show no signs of alteration. To detect these sophisticated fabrications, forensic laboratories must move beyond traditional hash tracking and utilize specialized deep learning detection tools.

C. Automated Forensic Systems & The Fundamental Right to Code Explainability

To preserve the truth-seeking mandate of criminal courts in an environment increasingly altered by AI, the legal framework must establish a clear Right to Code

Explainability. This principle dictates that whenever an automated software tool or AI system is used to generate forensic proof or assist in a criminal conviction, the underlying source code, training datasets, and error margins must be made accessible to the defense and the court for independent review. This requirement directly counters the risk of automation biases the natural human tendency to accept computer-generated outputs as inherently accurate and objective without questioning their operational limits. If an automated forensic tool is used to analyze blood spatter patterns, match ballistic data, or interpret voice recordings, its internal models may be affected by biases or gaps within its training datasets. For instance, if a facial recognition algorithm is trained primarily on data from a single demographic group, its error rates will rise significantly when applied to individuals outside that group, leading to a higher risk of false identifications. A commitment to due process under Article 21 requires that these algorithmic tools are not insulated from judicial review behind claims of corporate trade secrecy, ensuring that all automated proofs remain subject to the same strict standards of verification applied to traditional forensic science.

IX. JUDICIAL RESPONSES AND POST-BSA JURISPRUDENCE

A. Transitional Interpretations Across State Judiciaries

As the Indian criminal justice system begins to apply the provisions of the Bharatiya Sakshya Adhiniyam, 2023, the judiciary faces the challenging task of interpreting these new statutory rules without a deep reservoir of established precedent. Trial courts and regional High Courts are encountering cases where digital extractions, cloud sync captures, and smartphone logs are introduced under the new definitions of Section 57 and Section 63. In interpreting these provisions, judges are drawing on the foundational principles developed during the historical disputes under the old Indian Evidence Act, ensuring that the transition to the new framework maintains a strong commitment to data integrity. The practical challenges Indian judges face when evaluating Section 63 certificates are mirrored in international courts. Research conducted under the European Research Council's TRUE Project (Trust in User-generated Evidence) examined how judges handle digital proof in the age of artificial

intelligence. The interviews revealed that judges frequently struggle with the technical burden of ensuring data reliability and managing the risk of sophisticated deepfakes.

B. Global Comparative Frameworks and Admissibility Screens

To address this issue without slowing the trial process to a crawl, international bodies have proposed frameworks similar to the upcoming US Proposed Rule of Evidence 707, which subjects machine-generated evidence to the same strict reliability standards applied to expert testimony. This comparative trendline indicates that Indian high courts, when interpreting the expert validation requirements of Part B under Section 63(4), should look to these international models to establish practical guidelines for verifying digital proof without overwhelming the trial courts. Early judicial feedback highlights a strict approach toward the new certificate requirements under Section 63(4). While some initial interpretations suggested that the expansion of primary evidence definitions under Section 57 would allow investigators to bypass the certificate requirement entirely by simply producing the physical device in court, High Courts have quickly clarified that this path is limited. In cases involving highly volatile data transfers, such as cloud data extractions or mobile app data dumps, courts continue to demand strict compliance with certificate rules. Judges emphasize that because digital data is easily altered during extraction, the dual-signature requirement must be treated as a mandatory safeguard.

C. Judicial Fact-Finding Shielding Tasks

Furthermore, the judiciary is encountering a growing number of cases involving sophisticated digital manipulations, including deep-fake recordings and synthesized audio tracks, which challenge traditional methods of authentication. In recent procedural reviews, trial judges have noted that simply producing a signed certificate indicating that a file was copied correctly from a hard drive does not prove that the underlying content represents a real-world occurrence. When the defence raises credible doubts regarding generative AI manipulation, courts may rely on Section 79A of the Information Technology Act, 2000, read with Section 39 of the

Bharatiya Sakshya Adhiniyam, 2023, to seek expert opinion from notified Examiners of Electronic Evidence or accredited cyber forensic laboratories for deep structural analysis of the disputed electronic files. This evolving judicial approach reflects a growing recognition that in the modern technical environment, formal compliance with paperwork is not enough to ensure reliability. Courts are shifting from a purely bureaucratic review of certificates to a deeper, forensic evaluation of data integrity, ensuring that the introduction of advanced technology does not compromise the core standards of a fair trial.

X. CONCLUSION & FORWARD-LOOKING LEGAL SUGGESTIONS

A. Synthesis Of Inquiries and Core Findings

The structural transition from the colonial Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023 marks a significant and necessary evolution in India's legal infrastructure. By formally integrating electronic records into the foundational definition of documentary evidence and modernizing statutory language to cover smartphones, cloud architectures, and semiconductor memory systems, the BSA creates a legal framework designed for the digital age. However, as this dissertation has analyzed, the practical success of this statutory overhaul depends heavily on how well its procedural safeguards are executed, and how effectively the legal system responds to the unique challenges presented by generative artificial intelligence and deep-fake technology.

While the updated certificate rules under Section 63(4) provide clear benefits by introducing a dual- signature mandate to ensure technical verification, they also impose significant administrative burdens on under- resourced law enforcement agencies and backlogged Forensic Science Laboratories. Furthermore, the ease with which generative AI can fabricate realistic, synthetic media without altering metadata exposes vulnerabilities within traditional forensic validation models.

B. Targeted Legislative and Structural Remodeling Recommendations

To address these challenges and ensure a reliable, forensically sound ecosystem for digital proof, this study offers the following forward-looking legal and structural

recommendations:

1. **Expansion of Regional Forensic Infrastructure:** The Central Government and state administrations must urgently fund and establish certified cyber forensic extraction units at the district level. Equipping local stations with standardized write-blockers and accredited imaging software will allow investigators to secure valid cryptographic hash values at the immediate point of seizure, reducing backlogs at central FSLs and ensuring compliance with Section 63(4) rules.
2. **Statutory Framework for AI and Deepfake Detection:** The legislature should introduce specialized forensic protocols under the IT Act and BSA rules to govern the evaluation of synthetic media. This framework should mandate the use of advanced deep learning detection systems at accredited laboratories and establish clear legal standards for admitting machine-generated outputs.
3. **Enforcement of Code Explainability:** Trial courts must strictly uphold the principle of algorithmic transparency under Article 21. Whenever law enforcement relies on automated facial recognition or predictive software to secure a conviction, the underlying source code, validation metrics, and error rates must be made available for independent review to eliminate automation bias.
4. **Comprehensive Training Programs:** The judiciary, in coordination with National Law Universities and police academies, must implement continuous technical training programs for magistrates, prosecutors, and defense counsel. This training should focus on the mechanics of the digital chain of custody, hash tracking, and metadata evaluation, ensuring that all legal actors can properly evaluate digital evidence.

XI. REFERENCES

A. Primary Legislative Sources

1. The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023).

2. The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023).
3. The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023).
4. The Indian Evidence Act, 1872 (Act No. 1 of 1872) [Repealed].
5. The Information Technology Act, 2000 (Act No. 21 of 2000).
6. The Constitution of India, 1950.
7. Law Commission of India, 185th Report on Review of the Indian Evidence Act, 1872 (2003).

B. Standard Legal Treatises

1. Sarkar, S. (2020). *Law of Evidence* (20th ed.). LexisNexis.
2. Woodroffe, J., & Amir Ali, S. (2022).
3. *Commentary on the Law of Evidence* (5th ed.).
4. Verdis. Gauba, K. N. (2018).
5. *The Law of Electronic Evidence*. Universal Law Publishing.

C. Technical & Forensic Guidelines

1. National Institute of Standards and Technology (NIST). (2022).
2. *Guide to Digital Forensics Examination* (Special Publication 800-86).
3. U.S. Department of Commerce.
4. Centre for Development of Advanced Computing (CDAC) (2024).
5. *Advanced Manual on Cyber Crime Investigation and Digital Evidence Preservation*.
6. Ministry of Electronics and Information Technology, Government of India.

D. International Reports & Global Surveys

1. INTERPOL and UNICRI, *Towards Responsible AI Innovation: Artificial Intelligence for Law Enforcement* (INTERPOL Innovation Centre 2020).
2. National Center for State Courts (NCSC), & CivAI. (2024). *AI-Generated*

Evidence: A Guide for Leaders and Judges. National Center for State Courts.

3. TRUE Project. (2024). *Trust in User-generated Evidence: Analysing the Impact of Deepfakes on Accountability Processes for Human Rights Violations*. European Research Council.
4. United Nations Office on Drugs and Crime (UNODC). (2023). *What to Know About Cybercrime and Cross-Border Electronic Evidence Protocols*. United Nations Office on Drugs and Crime.