

Electronic Evidence and Criminal Justice in India: An Empirical Study of Judicial and Investigative Challenges under the Bharatiya Sakshya Adhiniyam, 2023

Chanchal Meena¹, Dr. Pooja Jain²

¹Research Scholar, School of Law, Mody University of Science and Technology, Lakshmangarh (Raj.)
332311

²Assistant Professor, School of Law, Mody University of Science and Technology, Lakshmangarh (Raj.)
332311

Abstract

Electronic records including emails, messages, social media postings, papers, CCTV video, and gadget data are used in criminal proceedings. Rapid digital technological development has revolutionised evidence presentation. As digital evidence becomes more important in trials, the Indian government approved the Bharatiya Sakshya Adhiniyam, 2023 (BSA), which replaced the Indian Evidence Act, 1872. Under Section 61, digital and electronic recordings are main evidence, replacing Section 65B, which was often condemned for its uneven judicial interpretation and technical conservatism. This mixed method research examines how the Bharatiya Sakshya Adhiniyam, 2023 has changed criminal digital evidence processing and admissibility. For example, Section 63 requires electronic records to be accompanied by an authenticity certificate signed by both the device's owner and an expert to ensure chain of custody. The doctrinal part also covers digital signatures, secondary evidence, evidentiary presumptions, and electronic records. In using the new legal framework, advocates, court officials, police detectives, forensic professionals, and law professors provide feedback. The study examines procedural compliance, legal issues in gathering and storing digital evidence, law enforcement's technological capabilities, and the Act's ambiguity on expert qualifications for evidence authenticity, chain of custody, cyber manipulation, and certification. Despite BSA's significant legal enhancement to electronic evidence, digital forensics infrastructure, training, data quality, procedural uniformity, and court capacity still limit its application. Research concluded that the new framework can only be implemented effectively if the criminal justice system as a whole undergoes legislative reform, institutional preparation, technological development, and continual capacity building.

Keywords: Bhartiya Sakshya Adhiniyam 2023, Electronic Evidence, digital forensics, admissibility, judiciary Judicial Interpretation, Legal Reform.

1. INTRODUCTION

The digital era has changed every element of human civilization, but the criminal justice system has been most affected. Crime has swiftly moved online due to digital communication, cloud computing, and

automated record-keeping, making a strong legal framework for electronic evidence essential. This critical investigative and judicial necessity prompted India's Bharatiya Sakshya Adhiniyam (BSA), 2023, a major law that substantially transforms digital evidence in criminal prosecutions. The Indian Evidence Act of 1872, despite patchwork modifications, failed to keep up with fast technology improvements and complex cybercrimes. The BSA, 2023 is a long-overdue reform. This new law recognizes the crucial, sometimes essential role electronic recordings play in contemporary criminal procedures and seeks to standardize their admission, verification, and treatment from the crime scene to the courtroom.¹

Digital evidence is crucial to contemporary criminal justice. Electronic data, from encrypted emails and instant chats to real-time geolocation data, social media activities, and digital financial footprints, is used to prove guilt or innocence in white-collar and violent crimes. The unique, volatile nature of digital evidence—its susceptibility to seamless manipulation, challenges in establishing pristine authenticity, and the advanced technical expertise required for its forensic interpretation—presents unprecedented challenges for investigating officers and trial judges. This essay will critically analyse the BSA, 2023's core sections, its direct influence on criminal investigations and judicial procedures, and its systemic problems and procedural protections. This empirical research examines how the BSA, 2023 is changing India's criminal justice environment by linking legislative intent and ground-level enforcement in the digital era.

2. DECONSTRUCTING THE DIGITAL FRAMEWORK UNDER BSA 2023

2.1 Definition and Classification of Digital Evidence

The BSA's definition of "document" in Section 2(d)² states that it "means any matter expressed or described or otherwise recorded upon any substance by means of letters, figures or marks or any other means or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter and includes electronic and digital records." This expanded definition of "document" to explicitly cover electronic and digital records is a key change from the previous Indian Evidence Act, 1872. The BSA aims to treat electronic evidence on par with traditional documentary evidence, subject to certain safeguards.

The Bharatiya Sakshya Adhiniyam, 2023 provides a comprehensive definition of digital evidence, expanding upon previous legislative efforts to encompass the wide array of electronic records that are now commonplace in legal proceedings. Under the BSA, digital evidence is broadly defined as any information of probative value that is stored or transmitted in digital form.³ This includes, but is not limited to:

1. Emails and instant messaging communications
2. Social media posts and interactions
3. Digital documents and spreadsheets
4. Database records
5. Digital images and videos
6. Website content and metadata
7. Log files from computers and networks

¹ Kanishka & Nikita Sharma, *Electronic Evidence Under Bharatiya Sakshya Adhiniyam: A Critical Analysis*, 7 Indian J.L. & Legal R. 5404 (2024).

² Bharatiya Sakshya Adhiniyam, 2023, § 2(1)(d), No. 47, Acts of Parliament, 2023 (India).

³ John Varghese, *Electronic and Digital Records Under Bharatiya Sakshya Adhiniyam, 2023: Part II – Electronic Form Evidence and Treatment of Digital Records Under Bharatiya Sakshya Adhiniyam, 2023*, Kerala Jud. Acad. 1, 1–28 (2024).

8. Data from mobile devices and apps

The Act further classifies digital evidence into two main categories:

- **Native Digital Evidence**

Information that is "born digital,"⁴ i.e., created, stored, and transmitted in digital form from its inception. Examples include emails, digital photographs, and computer-generated reports.

- **Digitized Evidence**

Physical evidence that has been converted into digital form, such as scanned documents or digitized audio recordings. This classification is significant as it recognizes the diverse origins of digital evidence and potentially impacts the methods used to authenticate and present such evidence in court.

2.2 Relevance of Section 57 Primary Evidence with new explanations under the Bharatiya Sakshya Adhiniyam (BSA) 2023

Section 57 of the Bharatiya Sakshya Adhiniyam (BSA) 2023⁵ has added four new explanations to define what constitutes primary evidence:

1. Electronic or digital records, when recorded or stored, are each considered primary evidence.
2. An electronic or digital record produced from proper custody is primary evidence unless contested.
3. Each stored video recording in electronic form or during transmission is primary evidence.
4. When an electronic record is stored in multiple spaces within a computer resource, each automated storage, including temporary files, is considered primary evidence.

2.3 Admissibility Criteria for Electronic Records

One of the most significant aspects of the BSA 2023 is its establishment of clear criteria for the admissibility of electronic records in legal proceedings. The Act stipulates that electronic records are admissible as evidence if they meet the following conditions:

1. **Authenticity:** The electronic record must be demonstrably authentic, meaning it can be shown to be what it purports to be. The Act provides guidelines for establishing authenticity, including the use of digital signatures, hash values, and metadata analysis.
2. **Integrity:** The record must be shown to have maintained its integrity from the time of its creation to its presentation in court. This means demonstrating that the record has not been altered or tampered with in any unauthorized manner.
3. **Reliability:** The system or process used to produce the electronic record must be shown to be reliable. This includes considerations of the security measures in place, the expertise of the personnel involved, and the consistency of the output.
4. **Best Evidence Rule:** The BSA 2023 modifies the traditional "best evidence" rule to accommodate electronic records. It stipulates that an electronic record can be considered the best evidence if it is the original or a duplicate that accurately reproduces the original.
5. **Hearsay Rule:** The Act addresses the application of the hearsay rule to electronic records, providing exceptions for business records and public records that are kept in electronic form.
6. **Chain of Custody:** For electronic records to be admissible, a clear chain of custody must be established, detailing how the evidence was collected, stored, and handled from its creation or discovery to its presentation in court.

⁵ Bharatiya Sakshya Adhiniyam (BSA), 2023, § 57 (India).

7. **Expert Testimony:** In cases where the interpretation of electronic evidence requires specialized knowledge, the Act provides for the admissibility of expert testimony to explain technical aspects of the evidence. These admissibility criteria are designed to ensure that electronic records are treated with the same rigor as traditional forms of evidence while acknowledging their unique characteristics. The Act also empowers judges to consider the reliability and accuracy of the methods used to generate, store, and retrieve electronic records when determining their admissibility. Furthermore, the BSA 2023 introduces a presumption of validity for certain types of electronic records, such as those produced by government agencies or regulated financial institutions, provided they meet specific criteria outlined in the Act. This presumption shifts the burden of proof to the party challenging the authenticity or reliability of such records. By establishing these clear and comprehensive admissibility criteria, the BSA 2023 aims to provide a robust framework for the handling of digital evidence in Indian courts, balancing the need for technological adaptation with the fundamental principles of evidence law.

3. INVESTIGATIVE CHALLENGES FOR LAW ENFORCEMENT

3.1 Unique Inherent Challenges of Digital Evidence

Despite its growing importance, the use of digital evidence presents unique challenges compared to traditional physical evidence, particularly concerning its admissibility in court. The vast amount of data and its rapid creation and transmission make digital evidence susceptible to manipulation, alteration, or degradation. Several cases have highlighted the difficulties in maintaining the integrity and authenticity of digital evidence, leading to its exclusion from court proceedings. Digital evidence, like physical evidence (e.g., documents, weapons, fingerprints), provides critical information linking individuals and events to criminal activities. However, key differences distinguish digital evidence from traditional forms of physical evidence:

- **Broader Information Range:** Digital evidence can encompass a vast array of data.
- **Sensitivity:** It involves handling data that may be both personally and physically sensitive.
- **Complex Interactions:** Digital evidence often intersects with broader criminal justice issues beyond traditional evidence collection roles.

Despite its advantages in providing extensive information for convictions, digital evidence poses unique challenges. Its large volume, rapid creation, and potential for manipulation make authentication complex. Digital evidence is also vulnerable to various external influences and human factors that can threaten its integrity. Unlike physical evidence, which is straightforward to document, digital evidence requires more complex procedures. The ease of remote access, file copying, and user mobility complicates the documentation and preservation of digital evidence. The volatile nature of digital evidence necessitates meticulous documentation throughout the investigation. Only the evidence that remains unaltered and reliable meets the admissibility standards in court.

The collection, examination, and analysis phases are particularly vulnerable to tampering or manipulation, given the involvement of multiple stakeholders. Addressing these challenges is crucial for ensuring trustworthy and secure forensic investigations, especially as the ecosystem evolves with emerging intelligent systems and technologies. A break in the CoC signifies a period during which control of the

evidence becomes uncertain, and actions conducted on the evidence remain unaccounted for. These breaks create potential vulnerabilities for malicious activities that could jeopardize the integrity of the evidence.⁶ In digital forensics, the principle “if you didn’t write it down, it didn’t happen” reflects the vital need for thorough documentation, given the volatile nature of digital evidence. Proper documentation is essential to verify that the evidence presented in court is genuine and untampered.

4. COURTROOM REALITIES: JUDICIAL FRICTION POINTS

4.1 The "Trial by Certificate" and Legal Invisible Truth

This legislative intent, while noble, has drawn sharp criticism for creating a "procedural rigidity" that may prioritize form over substance. Legal scholars argue that this strict adherence risks creating a "Trial by Certificate" In this scenario, substantive justice is held hostage to the technical availability of a certification document. If a prosecutor possesses a video clearly depicting a homicide, but lacks the Section 63(4)⁷ certificate due to a bureaucratic delay, the evidence is inadmissible. This creates a paradox where the "truth" is visible to the court but legally invisible to the judgment.⁸

4.2 The Expert Bottleneck and Remote Certification Dilemma

The second signatory creates the bottleneck. The BSA mandates that the certificate must also be signed by an expert, specifically one notified under Section 79A of the Information Technology Act, 2000.⁹ This provision has disastrous logistical implications. As noted in recent judicial trends, specifically, there is a chronic and severe deficit of notified forensic experts across India.¹⁰ This shortage creates an "Administrative Bottleneck" where the legal process is effectively paused, waiting for an expert signature. Investigating officers are finding themselves in a queue, sometimes lasting months, to get a Section 63(4) countersignature from a Central Forensic Science Laboratory (CFSL) or State Forensic Science Laboratory (SFSL)

Furthermore, this regime introduces a profound legal liability paradox. The expert is required to sign a certificate vouching for the integrity of data on a device they did not personally seize or maintain in the chain of custody. They are essentially certifying a "black box" based on a hash value generated at the lab. If it is later revealed that the device was tampered with during transit between the police station and the lab, the expert who signed the certificate faces potential cross-examination and liability for certifying a compromised device. This "remote certification" dilemma makes experts hesitant to sign, further exacerbating the bottleneck.¹¹

Consequently, the dual-signature requirement, intended to be a shield against tampering, has become a sword that cuts into the efficiency of the trial process. It forces the defense to attack the absence of the second signature rather than the content of the evidence, leading to acquittals based on technical non-compliance rather than innocence.

⁶ Souradip Nath, Keb Summers, Jaeyong Baek, & Gail-Joon Ahn, *Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics*, Proceedings of the 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA) 11 (2024).

⁷ Bharatiya Sakshya Adhiniyam, 2023, § 63(4), No. 47, Acts of Parliament, 2023 (India).

⁸ Mridul Bhatt, *Admissibility of Electronic Record and the Dual-Certification Regime Under BSA, 2023*, 8 Indian J.L. & Legal Res. 374, 374–80 (2026).

⁹ Information Technology Act, 2000, § 79A, No. 21, Acts of Parliament, 2000 (India).

¹⁰ Rohit, *Digital Evidence and Its Admissibility in Criminal Trials: A Study Under the Indian Evidence Regime (BSA, 2023)*, 3 Int’l J. Legal Res. & Analysis 803 (2026).

¹¹ *Supra* note 8.

4.3 Friction in Filing Timelines: Charge Sheet vs. Trial

Given the "Administrative Bottleneck" caused by the shortage of experts, investigating agencies frequently struggle to procure the expert signature by the time the statutory period for filing the charge sheet (60 or 90 days) expires. Consequently, courts are frequently petitioned to condone delays.

This creates a friction between the accused's right to a speedy trial and the prosecution's need for procedural compliance. The judiciary is forced to balance the strict mandate against the pragmatic necessity of justice. Emerging jurisprudence suggests that while the certificate must exist to make the evidence admissible, its production can be delayed if the prosecution can demonstrate "sufficient cause." Courts are distinguishing between a "fatal defect" (non-existence of the certificate) and a "curable defect" (delayed production). Yet, this flexibility is a double-edged sword; it allows the prosecution to patch up investigations retrospectively, potentially undermining the rigorous standards the BSA sought to impose.

4.4 Underlying Technological and Digital Infrastructure Deficiencies

A secure system is the backbone of a company's cybersecurity policy. A secure system is made up of three moving parts—hardware, software, and humans—that work together to keep company data safe from cyberattacks and data breaches. When a system is secure, the business becomes stronger and more resilient as a result. Let's review the three elements of a secure system:

Many courts suffer from unreliable internet connectivity, outdated hardware, and insufficient technical support. These challenges are more acute in rural and semi-urban regions, where digital infrastructure mirrors broader socio-economic disparities. As a result, technological reforms have benefitted certain courts while leaving others functionally excluded. Digital literacy among litigants, lawyers, and court staff also varies significantly. Without adequate training and support, technological systems often create new barriers rather than removing existing ones.¹²

Human infrastructure remains one of the most critical constraints on judicial functioning in India. Chronic vacancies in judicial positions have placed excessive workloads on serving judges, limiting their ability to devote adequate time to hearings, evidence evaluation, and judgment writing. Court staff shortages further exacerbate inefficiencies. Clerks, stenographers, and administrative personnel are often overburdened with multiple responsibilities, including record management, scheduling, and compliance monitoring.

A key limitation of judicial infrastructure reform lies in fragmented governance and weak institutional coordination. Responsibility for judicial infrastructure is shared between multiple actors, including the Union government, state governments, and the judiciary itself. This diffusion of responsibility often leads to delays, accountability gaps, and inconsistent planning. Digital reforms have often been implemented without corresponding investment in physical infrastructure, training, and technical support.¹³

Excessive caseloads and time constraints limit opportunities for detailed hearings, careful evaluation of evidence, and reasoned judgment writing. Judges operating under infrastructural pressure may be compelled to prioritize disposal over deliberation, raising concerns regarding procedural fairness. Limited access to research tools, inadequate courtroom acoustics, and technological failures during hearings further compromise the adjudicatory process.

¹² Gaurav & Diptimoni Boruah, *Infrastructure Deficiency in Indian Courts: A Stakeholder-Based Analysis and Policy Recommendations for Strengthening Justice Delivery*, 6 Int'l J.L. Just. & Juris. 7, 7–15 (2026).

¹³ Chandan Kumar Singh, Sunidhi Singh & Mohd Tauheed Khan, *Criminal Justice System and Governance in India: An Analysis Under the New Criminal Laws and Current Conditions*, 12 Int'l J.L. 185, 185–89 (2026).

5. CONCLUSION

The Bharatiya Sakshya Adhiniyam, 2023 is a turning point in India's judicial system, notably with digital evidence. The BSA 2023 tackles many digital evidence concerns, but it also underlines the difficulties of fast-growing technology like deep fakes and enhanced data manipulation. Dual-certification may boost digital evidence credibility, but excessively mechanical implementation may shift litigation from record truth to certificate sufficiency. The best judicial method is severe about authenticity but restrained about speed and curability, satisfying the statutory protection without detriment to the accused or opposing party. Indian courts' infrastructure shortages significantly affect adjudicatory efficiency, procedural fairness, and public faith in the rule of law. The results show that poor infrastructure causes case pending, procedural delays, and plaintiff dignity loss. Overcrowded courtrooms, judge vacancies, and unequal technology integration delay justice and penalize economically and socially disadvantaged litigants. Shifting to infrastructure-driven methodologies has made the CoC process more complicated than before. India must define "secure system," and create rigorous frameworks for processing, authenticating, and presenting digital documents to maximize this reform's potential. Legal professionals require ongoing education and training to appropriately evaluate electronic evidence. Digital forensic specialists in difficult cases and court infrastructure modernization will improve law enforcement. Infrastructure reform must align with constitutional principles and stakeholder realities to make India's judicial system efficient, inclusive, and accessible.

6. REFERENCES

1. Government of India. (2023). The Bharatiya Sakshya Adhiniyam, 2023. Ministry of Law and Justice.
2. Law Commission of India. (2022). Report on the Reform of Evidence Law for the Digital Age. Government of India.
3. OECD. (2024). Digital Evidence in Legal Proceedings: A Comparative Study of OECD Countries. OECD Digital Economy Papers, No. 324.
4. Bhatia, K. (2023). The Role of Expert Witnesses in Digital Evidence Cases: New Paradigms Under the BSA 2023. Expert Evidence Report, 21(1), 15-32.
5. Goel, M. (2023). Cloud Computing and Digital Evidence: Jurisdictional Challenges Under the BSA 2023. Computer Law & Security Review, 39(4), 105706
6. Al-Khateeb, H., Epiphaniou, G., & Daly, H. (2019). Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger. Blockchain and Clinical Trial: Securing Patient Data, pp. 149-168.
7. Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital evidence and the US criminal justice system: Identifying technology and other needs to more effectively acquire and utilize digital evidence.
8. Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with POC in hyperledger composer. Digital Investigation, vol. 28, pp. 44-55.
9. Prayudi, Y., & Sn, A. (2015). Digital chain of custody: State of the art. International Journal of Computer Applications, vol. 114, no. 5.
10. Aithala, V., Sachan, A., Sen, S., Payal, H., & Bhattacharya, C. (2024). Decision time: Illuminating performance in India's district courts. Data Policy, 6, e24.
11. opal, G. M. (2024). Evaluating the impact of judicial reforms on access to justice in India. Indian Journal of Law, 2(5), 32-48.

12. Gupta, M., & Bolia, N. B. (2023). Factors affecting efficient discharge of judicial functions: Insights from Indian courts. *Socio-Economic Planning Sciences*, 91, 101755
13. Mishra, S. (2022). Cyclic syndrome of arrears and efficiency of the Indian judiciary. *SN Business & Economics*, 3(1), 6.