DIGITAL FORENSICS AND ELECTRONIC EVIDENCE IN INDIA: ADMISSIBILITY, INTEGRITY AND DUE PROCESS UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

Pooja Singh, BA LLB, Amity University Gwalior

ABSTRACT

The rapid digitization of society has transformed the nature of crime and criminal investigation in India. Electronic evidence such as mobile phone records, CCTV footage, emails, cloud data, and social media communications now plays a decisive role in criminal trials. The enactment of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) marks a significant shift from the colonial-era Indian Evidence Act, 1872 in regulating the admissibility of electronic evidence. This paper critically examines the legal framework governing digital forensics and electronic evidence under the BSA, with particular focus on admissibility standards, integrity of evidence, chain of custody, and due process safeguards. It analyses key judicial precedents such as *Anvar P.V. v. P.K. Basheer* and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* to highlight challenges in authentication and certification of electronic records. The paper further evaluates practical difficulties faced by investigating agencies and courts in handling digital evidence and proposes reforms including uniform Standard Operating Procedures (SOPs), judicial training in cyber forensics, and independent forensic oversight mechanisms. The study concludes that while the BSA, 2023 is a progressive reform, effective implementation is essential to prevent misuse and miscarriage of justice.

Keywords: Digital Forensics; Electronic Evidence; Bharatiya Sakshya Adhiniyam, 2023; Admissibility; Chain of Custody; Due Process.

Introduction

The digital transformation of society has altered not only modes of communication and commerce but also the nature of criminal activity and law enforcement. Contemporary crimes increasingly leave digital footprints in the form of mobile phone logs, GPS location data, CCTV recordings, emails, online transactions, and social media interactions. Consequently, electronic evidence has emerged as a decisive factor in modern criminal trials. In India, courts now routinely rely on digital records to establish timelines, identify accused persons, corroborate witness testimony, and reconstruct crime scenes.

However, unlike traditional physical evidence, digital evidence is inherently fragile and susceptible to manipulation. A single alteration of metadata, unauthorized access to storage devices, or improper forensic imaging can compromise the authenticity of electronic records. This fragility raises serious concerns regarding reliability, admissibility, and the protection of due process rights. Historically, the Indian Evidence Act, 1872 was ill-equipped to address these challenges, leading to piecemeal judicial interpretations after the Information Technology Act, 2000 introduced Sections 65A and 65B.

The Bharatiya Sakshya Adhiniyam, 2023 represents a legislative attempt to modernize evidentiary rules to align with technological realities. By recognizing electronic records more comprehensively and redefining admissibility standards, the BSA seeks to streamline evidentiary processes. Nonetheless, the transition from the old regime to the new framework raises critical questions: Do the new provisions sufficiently safeguard the integrity of electronic evidence? Are due process guarantees adequately protected in the digital age? This paper seeks to address these questions through doctrinal analysis, judicial interpretation, and comparative insights.

Evolution of Legal Framework on Electronic Evidence in India

The recognition of electronic evidence in Indian law commenced with the enactment of the Information Technology Act, 2000, which amended the Indian Evidence Act, 1872 by introducing Sections 65A and 65B. These provisions laid down specific conditions for the admissibility of electronic records, including the requirement of a certificate certifying the manner of production and integrity of the device used. The Supreme Court in *Anvar P.V. v. P.K. Basheer* clarified that compliance with Section 65B is mandatory, thereby overruling

earlier decisions that permitted relaxed standards. This strict approach was reaffirmed in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, emphasizing the importance of certification to prevent fabrication and misuse of electronic evidence.

While these judicial pronouncements strengthened evidentiary reliability, they also exposed practical challenges. Litigants often struggled to obtain certificates from service providers or access original devices, resulting in the exclusion of potentially crucial evidence. The Bharatiya Sakshya Adhiniyam, 2023 attempts to address these challenges by recognizing electronic records as primary evidence under specified circumstances and simplifying procedural requirements. However, the absence of detailed statutory protocols on forensic acquisition, storage, and verification continues to pose risks of inconsistent application.

Admissibility of Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023 (Expanded Analysis)

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) signifies a notable conceptual shift in India's evidentiary framework by seeking to integrate electronic records more seamlessly into the mainstream law of evidence. Unlike the earlier regime under Sections 65A and 65B of the Indian Evidence Act, 1872—where electronic records were treated as a special category of secondary evidence requiring strict procedural compliance—the BSA attempts to normalize digital evidence within the broader evidentiary structure. By recognizing electronic records as primary evidence in specified circumstances, the legislature aims to reduce procedural bottlenecks that previously led to the exclusion of otherwise reliable digital material on technical grounds. This reform reflects an acknowledgment of the pervasive role of digital technology in contemporary criminal investigations and the need for evidentiary rules to adapt accordingly.

However, while the BSA simplifies the formal classification of electronic evidence, it does not fully resolve the underlying concerns relating to authentication and reliability. The core challenge lies in ensuring that electronic records produced before courts are genuine, untampered, and accurately reflect the original data. Unlike physical documents, digital records are inherently mutable and can be altered without leaving visible traces. The BSA does not lay down detailed statutory criteria or standardized formats for authentication, leaving courts to rely on general evidentiary principles and judicial discretion. This absence of precise statutory guidance risks perpetuating inconsistent judicial approaches, where similar forms of electronic

evidence may be admitted in one jurisdiction and rejected in another based on differing thresholds of judicial satisfaction.

Further, the lack of uniform forensic guidelines for the collection, preservation, and presentation of electronic evidence exacerbates these inconsistencies. In practice, investigating agencies employ varied methods for seizing digital devices, extracting data, and presenting electronic records before courts. Without standardized procedures for forensic imaging, hash verification, and documentation of chain of custody, the probative value of electronic evidence remains vulnerable to challenge. Defence counsel often contest the authenticity of digital records by pointing to procedural lapses in seizure or preservation, leading to prolonged evidentiary disputes and delays in trials. The BSA's silence on these operational aspects limits its capacity to ensure uniformity and reliability in the admission of electronic evidence.

Judicial training in digital forensics emerges as a critical factor in the effective application of the BSA. Courts are increasingly required to assess technical concepts such as metadata, hash values, server logs, geolocation data, and forensic imaging techniques. Without a foundational understanding of these concepts, judges may either adopt an overly cautious approach, excluding relevant electronic evidence due to minor procedural irregularities, or an overly permissive approach, admitting unreliable material that may prejudice the accused. Both extremes undermine the fairness and accuracy of the adjudicatory process. Structured training programs and judicial handbooks on digital evidence can bridge this knowledge gap and promote informed adjudication.

Another significant concern relates to the involvement of third-party service providers, such as telecom companies, cloud service providers, and social media platforms, in the authentication process. In many cases, crucial electronic evidence is stored on servers controlled by private entities, often located outside India's jurisdiction. The BSA does not provide a clear mechanism to compel cooperation from such entities or to standardize the format in which digital records are certified and produced. This lacuna may impede effective prosecution in cases involving transnational digital evidence and raises questions regarding the enforceability of evidentiary standards in cross-border investigations.

The success of the BSA's reformist intent ultimately depends on the development of consistent interpretative standards by higher judiciary and the institutionalization of technical competence within the criminal justice system. Judicial precedents interpreting the BSA will play a crucial

role in shaping admissibility thresholds and authentication requirements. In the absence of detailed statutory guidance, coherent jurisprudence from appellate courts can provide much-needed clarity and uniformity. Additionally, the formulation of statutory Standard Operating Procedures (SOPs) for digital evidence handling, coupled with judicial and police training, can operationalize the BSA's objectives and ensure that the admissibility of electronic evidence advances both efficiency and due process.

Integrity, Chain of Custody and Due Process Concerns

The integrity of electronic evidence hinges on proper chain of custody procedures. Digital devices must be seized lawfully, preserved securely, and subjected to forensic imaging using standardized protocols. Any break in the chain of custody raises doubts about authenticity. In India, the lack of uniform SOPs for handling electronic devices leads to ad hoc practices by investigating agencies, increasing the risk of evidentiary contamination.

Due process concerns also arise from intrusive digital searches and surveillance practices. Unregulated access to personal devices infringes upon privacy rights and may violate Article 21 of the Constitution. The balance between effective investigation and protection of fundamental rights is delicate and demands clear statutory safeguards. Without such safeguards, the increasing reliance on digital evidence may lead to arbitrary state action and erosion of civil liberties.

Institutional and Practical Challenges in Digital Forensics

India's forensic infrastructure faces significant capacity constraints. Many state forensic laboratories lack advanced tools and trained cyber forensic experts. Delays in forensic examination and reporting often prolong criminal trials, undermining the right to speedy justice. Moreover, investigating officers frequently lack technical training, resulting in improper handling of digital devices and loss of evidentiary value.

The judiciary also grapples with technical complexities. Limited familiarity with forensic methodologies hampers effective evaluation of electronic evidence. These institutional challenges underscore the need for comprehensive reforms to strengthen digital forensic capabilities and ensure credible evidentiary practices.

Comparative Perspective: UK and US Practices

The United Kingdom and the United States have developed structured protocols for handling digital evidence, emphasizing forensic imaging, hash verification, and independent expert audits. These practices ensure evidentiary integrity and protect due process rights. India's fragmented approach contrasts sharply with these jurisdictions. Adopting international best practices through statutory SOPs and independent forensic oversight can enhance the reliability of digital evidence in Indian courts.

Findings and Recommendations

This study finds that the BSA, 2023 represents a progressive legislative reform but requires robust implementation mechanisms. The following recommendations are proposed:

1. Enact uniform statutory SOPs for seizure, preservation, and forensic analysis of electronic evidence.

2. Establish an independent forensic oversight authority to ensure accountability and quality control.

3. Mandate judicial and police training in cyber forensics and digital evidence evaluation.

4. Strengthen privacy and due process safeguards during digital searches and surveillance operations.

Conclusion

The growing reliance on electronic evidence necessitates a comprehensive legal and institutional framework to ensure admissibility, integrity, and due process. While the Bharatiya Sakshya Adhiniyam, 2023 modernizes evidentiary law, its effectiveness hinges on standardized procedures, capacity building, and judicial clarity. Without these supporting mechanisms, digital evidence risks becoming a source of miscarriage of justice rather than a facilitator of truth. Implementing the recommended reforms will strengthen the credibility of digital forensics and uphold the rule of law in the digital age.

REFERENCES

1. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
2. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
3. Information Technology Act, 2000.
4. Bharatiya Sakshya Adhiniyam, 2023.
5. Interpol, Digital Forensics Guidelines.