DIGITAL EVIDENCE IN INDIAN CRIMINAL LAW: ADMISSIBILITY AND AUTHENTICITY UNDER THE BSA, 2023

Shashank Mohan Gupta[1] & Dr. Astitwa Bhargava[2]

ABSTRACT

India's evidentiary framework has undergone a paradigm shift as digital life dominates social, financial, and criminal spheres. The Bharatiya Sakshya Adhiniyam (BSA), 2023, replaces the 150-year-old Indian Evidence Act (IEA), 1872[3], to reflect this transformation. Electronic records, once treated as secondary evidence, now lie at the core of justice delivery. This paper focuses on the pivotal reform in proving digital authenticity under the BSA, tracing the evolution from the rigid certification regime of Section 65B of the IEA to the simplified approach under Section 63(4) of the BSA. The new provision recognizes electronic records as primary evidence-a landmark departure that resolves long-standing judicial ambiguities. Landmark Supreme Court rulings, including Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, shaped this debate, and the BSA now attempts to settle it decisively. Yet, challenges persist in ensuring forensic reliability, authentication consistency, and uniform procedural application across courts. Achieving a robust digital justice framework demands standardized forensic protocols, judicial capacity building, and seamless integration between the BSA, the Bharatiya Nagarik Suraksha Sanhita (BNSS), and the Information Technology Act, 2000-ensuring that law and technology evolve in tandem toward a transparent, fair, and future-ready justice system.

Keywords: Digital Evidence – Admissibility – Authentication – Bharatiya Sakshya Adhiniyam 2023 – Cyber Crime – Forensic Protocols

[1] PhD Scholar, National Law Institute University, Bhopal, Advocate, Delhi High Court
[2] Assistant Professor, National Law Institute University, Bhopal
[3] Indian Evidence Act, 1872, No. 1, Acts of Parliament, 1872.

Introduction

The digital revolution of the twenty-first century has fundamentally changed how crimes are detected, investigated, and prosecuted. Evidence increasingly takes the form of emails, CCTV recordings, transaction logs, and data stored on cloud servers. These digital traces have become central to modern criminal trials. Yet, the Indian Evidence Act (IEA) of 1872-drafted in an era of paper documents and oral testimony-was ill-equipped to handle the complexities of today's technologically driven investigations.

To modernize India's evidentiary framework, Parliament enacted the Bharatiya Sakshya Adhiniyam (BSA), 2023, which came into force on 1 July 2024. Part of a broader criminal law reform initiative alongside the Bharatiya Nyaya Sanhita (BNS) and the Bharatiya Nagarik Suraksha Sanhita (BNSS), the BSA replaces archaic language, streamline evidentiary procedures, and, crucially, recognizes electronic records as equivalent to traditional documentary evidence. This represents a decisive shift, acknowledging the centrality of digital information to the delivery of justice.

The key challenge lies in verifying the authenticity and reliability of digital evidence. In an era where data can be easily altered or fabricated, questions of integrity, authorship, and chain of custody become critical. Section 63(4) of the BSA moves beyond the rigid certification requirements of Section 65B of the IEA[4], aiming for a more practical and technologically aware approach. The success of this reform depends on establishing consistent procedures for authentication, secure handling, and expert verification of digital records.

By giving electronic records, the status of primary evidence while retaining mechanisms for certification and integrity checks, the BSA seeks to balance technological realities with evidentiary safeguards.[5] Its provisions are designed to provide courts with clear standards for admitting and evaluating digital evidence, ensuring reliability without unnecessary procedural hurdles, and aligning India's legal framework with the demands of a digitally integrated criminal justice system.

[4] https://www.drishtijudiciary.com/bharatiya-sakshya-adhiniyam-&-indian-evidence-act/electronic-evidence-under-bhartiya-sakshya-adhiniyam-2023
[5] https://www.livelaw.in/top-stories/bharatiya-sakshya-adhiniyam-changes-electronic-evidence-admissibility-explainer-245852

Historical Evolution

The Indian Evidence Act (IEA), 1872, drafted by Sir James Stephen, marked a transformative milestone in India's legal evolution. As one of the earliest codifications of evidentiary law, it introduced clarity, uniformity, and predictability to the administration of justice in colonial India. Grounded in the English common law tradition, the Act successfully standardized evidentiary principles across a vast and diverse jurisdiction. However, with the advent of the digital era, its emphasis on physical documents and oral testimony rendered it increasingly inadequate to address the complexities of modern, technology-driven communication and data exchange.

The dawn of the new millennium brought India's first statutory recognition of electronic evidence through the Information Technology Act, 2000, which inserted Sections 65A and 65B into the IEA. These provisions established a legal framework for the admissibility of electronic records, with Section 65B (4) mandating a certificate to verify the authenticity and integrity of digital content. Yet, this certification requirement soon became a source of judicial contention. In State v. Navjot Sandhu (2005), the Supreme Court adopted a flexible approach, allowing electronic records without strict compliance, provided their authenticity was established. This leniency shifted dramatically in Anvar P.V. v. P.K. Basheer (2014), where the Court held that certification under Section 65B was a mandatory prerequisite for admissibility.

The pendulum swung once again in Shafi Mohammad v. State of Himachal Pradesh (2018), where the Court recognized that rigid compliance could cause injustice when the party presenting the evidence lacked control over the device generating it-such as surveillance or third-party server data. However, this relaxation was short-lived. In Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), the Supreme Court reaffirmed Anvar, emphasizing that certification was essential except in cases where obtaining it was genuinely impossible.

This judicial oscillation underscored the courts' struggle to balance procedural rigor with technological practicality-striving to uphold evidentiary authenticity without compromising the pursuit of justice. Recognizing this need for coherence, Parliament enacted the Bharatiya Sakshya Adhiniyam (BSA), 2023, as part of a broader criminal law reform alongside the Bharatiya Nyaya Sanhita (BNS) and Bharatiya Nagarik Suraksha Sanhita (BNSS), effective from 1 July 2024.

The BSA modernizes evidentiary law by expanding the definitions of "document" and "evidence" to expressly include digital records, replacing Section 65B with Section 63(4), which simplifies certification while maintaining integrity. Section 57 further broadens "primary evidence," ensuring electronic records-original or faithfully reproduced-are admissible. Thus, the BSA bridges the gap between traditional evidence law and the digital age, ensuring authenticity, adaptability, and fairness in India's evolving justice system.

The Concept of Digital Evidence under the BSA

The Bharatiya Sakshya Adhiniyam (BSA), 2023 represents a transformative shift in India's evidentiary regime, explicitly recognizing digital data as an integral and legitimate form of documentary evidence. Section 2(1)(d) of the Act expands the definition of "document" to encompass a wide spectrum of digital and electronic formats, including emails, server logs, website content, computer and mobile data, and even voice messages. By incorporating these diverse forms of electronic communication, the law acknowledges the centrality of digital interactions in contemporary personal and professional life, and the consequential role such data plays in the administration of justice.

Section 57 of the BSA further strengthens this modernization by establishing that electronic records-whether stored across multiple devices or retrieved from lawful custody-constitute primary evidence. This marks a significant departure from the Indian Evidence Act, 1872, under which electronic data was generally treated as secondary evidence, admissible only after strict procedural compliance. The BSA recognizes that digital records naturally exist in multiple identical copies, each carrying equivalent evidentiary weight. Explanations 4 to 7 of Section 57 clarify that electronic records[6] stored simultaneously or sequentially across files, devices, or servers are to be treated as primary evidence unless their authenticity is specifically contested.

Section 63(4)[7] reintroduces the certification mechanism that previously existed under Section 65B of the Indian Evidence Act, but with refinements tailored to modern technological realities. Certification provides assurance of reliability by requiring a formal statement that identifies the device or system used, describes the process by which the electronic data was generated,

[6] Anand & Anand, The Bharatiya Sakshya Adhiniyam, 2023: Key Highlights, Mondaq (Jan. 12, 2024)
[7] India Corporate Law, Bharatiya Sakshya Adhiniyam, 2023: Admissibility of Electronic Records, Cyril Amarchand Mangaldas (Jan. 16, 2024)

and confirms proper system operation throughout. Notably, the BSA broadens the category of authorized certifiers to include technical experts in addition to the person responsible for the device or data, aligning the law with practical requirements in complex digital environments.

Collectively, these provisions strike a deliberate balance between accessibility and authenticity. By granting electronic records the status of primary evidence, the BSA reduces procedural obstacles that previously hindered the judicial acceptance of digital data. At the same time, the certification requirement ensures the integrity and reliability of such evidence, maintaining high evidentiary standards. This dual approach fosters transparency and consistency in judicial evaluation, signaling a legal framework that evolves in tandem with technological progress while safeguarding the credibility of digital evidence in India's courts.

Admissibility and Interpretation

Section 57 of the Bharatiya Sakshya Adhiniyam (BSA), 2023, introduces a landmark shift in the treatment of digital material within Indian evidentiary law. By recognizing electronic records as primary evidence, the legislature departs from the long-standing assumption that digital files are inherently secondary. Courts are now empowered to rely directly on digital sources such as emails, CCTV footage, databases, or mobile communications without necessitating printed reproductions or additional formalities, provided the material originates from a credible and lawful source. This legislative stance acknowledges the digital ecosystem as an authentic reflection of contemporary life, where communication, transactions, and record-keeping are largely conducted electronically.

Nonetheless, this recognition interacts complexly with Section 63(4) of the Adhiniyam, which continues to mandate a certification process for electronic evidence. Certification under Section 63(4) requires verification of the device used, the method of data generation, and the integrity of the system. The coexistence of these provisions raises interpretative questions: if an electronic record is already recognized as primary evidence under Section 57[8], is certification under Section 63(4) still obligatory? Legal commentary suggests that certification may not be necessary in all circumstances. Digital records originating from undisputed or officially maintained systems-such as government databases, institutional repositories, or telecom service logs-may be presumed authentic, reducing the need for formal certification.

[8] Vivek Sood, Electronic Evidence in the Indian Legal System: Bharatiya Sakshya Adhiniyam, 2023, Bar & Bench (Feb. 10, 2024)

Conversely, in criminal or contested proceedings where the reliability of the source is uncertain or the potential for tampering exists, certification remains crucial. It safeguards the evidentiary process and ensures that electronic material is not manipulated or misrepresented.

Judicial interpretation will be key in resolving this apparent overlap. Courts are likely to adopt a balanced approach, treating the presumption of primary evidence under Section 57 as rebuttable. When a party challenges the genuineness or integrity of a digital record, the court may require certification under Section 63(4) to corroborate authenticity. Certification, therefore, functions not as a rigid procedural barrier but as a reinforcing mechanism to confirm reliability when necessary. This approach harmonizes efficiency with evidentiary discipline, allowing the expedited admission of uncontested electronic records while preserving rigorous scrutiny in disputed cases. Such a calibrated framework ensures that the modernized evidentiary system remains technologically relevant, legally sound, and capable of accommodating the complexities of the digital age.

Ensuring Authenticity and Reliability

Digital evidence, by its very nature, is fragile and highly susceptible to manipulation. Even minor alterations to a file's metadata or a single change in a data string can compromise its integrity and render it unreliable in court. The Supreme Court's caution in Anvar P.V. v. P.K. Basheer[9] remains as relevant today as it was at the time of the judgment: uncertified or mishandled electronic records can threaten the fairness of a trial. A weak or broken chain of custody may invalidate otherwise compelling evidence, undermining the credibility of the judicial process.

Recognizing these risks, the Standing Committee on Home Affairs (2023) emphasized the necessity of a clearly documented and verifiable chain of custody for all forms of digital material. Such a system ensures that every transfer or access point-from seizure to final court presentation-is recorded, authenticated, and traceable. This approach not only protects against tampering but also enhances the evidentiary value of digital records in judicial proceedings.

The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, complements this vision by introducing procedural innovations that integrate technology into criminal justice operations. Provisions including Sections 105, 173(1)(ii), 176(3)(b), and 185(2) allow for electronic First

[9] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473

Information Reports (FIRs), video recording during searches and seizures, and mandatory forensic documentation for offences punishable by seven years or more. These measures modernize investigative procedures while creating a seamless link between evidence generation and admissibility under the Bharatiya Sakshya Adhiniyam (BSA), 2023. Together, the reforms aim to ensure that digital evidence is verified, tamper-proof, and accountable throughout its lifecycle.

The Information Technology Act, 2000 further strengthens this framework. Sections 4 and 5 confer statutory recognition to electronic records and digital signatures, establishing their legal equivalence with traditional documents. Section 79A authorizes the appointment of certified "Examiners of Electronic Evidence" to provide expert authentication and analysis of digital materials. Such expertise is critical for the effective application of BSA provisions, particularly in confirming the authenticity and integrity of electronic records before courts.

However, implementation remains uneven across India. Investigative agencies often lack standardized digital forensic protocols, with variations in imaging and data extraction tools and limited expertise in hash verification-a fundamental process to ensure data integrity. The Karnataka High Court's 2021 guidelines offer a valuable model, mandating Faraday bags to prevent remote tampering, the presence of forensic examiners during seizures, and prohibiting the use of devices prior to forensic imaging.

For India to fully realize the potential of the BSA and BNSS, national standardization is essential. This includes uniform forensic procedures, ongoing training for law enforcement and judiciary, and secure, tamper-proof evidence storage. Only through such coordinated efforts can technology reliably serve justice, not as a source of doubt, but as a foundation of truth.

Comparative Analysis

Across the globe, the admissibility of digital evidence is anchored in the principles of authenticity, integrity, and reliability, each reinforced by technology-driven verification mechanisms. Leading jurisdictions, such as the United States and the United Kingdom, have institutionalized technical safeguards to prevent manipulation and enhance the trustworthiness of electronic records. In the United States, the Federal Rules of Evidence, particularly Rule 902(14), permit electronic data to self-authenticate if its integrity is demonstrably established through a digital hash-an alphanumeric fingerprint unique to each file. This allows courts to

verify that the evidence has not been altered from its original state. Similarly, the UK's Police and Criminal Evidence Act (PACE) 1984 mandates strict forensic imaging protocols to preserve the original condition of electronic material, ensuring that every modification can be traced in a transparent, verifiable manner and providing investigators and courts with a reliable audit trail.

India's Bharatiya Sakshya Adhiniyam (BSA), 2023, conceptually aligns with these global standards by emphasizing certification and the authentication of electronic records. Section 63(4) retains a formal certification requirement, ensuring that the device used, the method of data generation, and the integrity of the system are verified. However, the Indian framework still predominantly relies on human verification through formal certificates rather than automated or cryptographic validation. While this approach accommodates practical limitations within India's judicial and investigative infrastructure, it lacks the technological precision offered by systems using digital hash values, blockchain-based ledgers, or automated metadata tracking to guarantee integrity and detect tampering objectively.

To strengthen India's digital evidence ecosystem, a hybrid approach could be adopted, combining the procedural safeguards of the BSA with advanced technological tools. Embedding digital signatures in the chain of custody could ensure accountability for each individual who handles a record. Blockchain-based audit trails could provide immutable verification for seized devices and forensic images, preventing tampering. Automated metadata tracking integrated into chain-of-custody documentation would enhance transparency by recording every interaction with the evidence in real time.

Implementing such measures would not only bring India's evidentiary system closer to international best practices but also bolster judicial confidence in electronic materials. In an era when commerce, communication, and criminal activity are increasingly digital, the credibility of justice depends on the integrity of the technology underpinning it. By embedding objective, verifiable methods within the legal framework, India can transform the BSA from a procedural reform into a global benchmark for digital integrity and evidentiary trust.

Continuity of Judicial Philosophy

Even though the Indian Evidence Act (IEA) has been repealed, the judicial principles developed under it still hold significant interpretative value for the Bharatiya Sakshya

Adhiniyam (BSA). Landmark rulings such as *Anvar P.V. v. P.K. Basheer*, *Shafi Mohammad v. State of Himachal Pradesh*, and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* continue to shape the understanding of how electronic evidence should be treated. This is because Section 63(4) of the BSA essentially carries forward the logic and spirit of Section 65B of the old Act. Until new judgments emerge that reinterpret these ideas in light of the present law, these earlier precedents will continue to serve as persuasive authority and a guiding foundation for courts assessing the admissibility of digital evidence.

Challenges in Criminal Adjudication

Investigating agencies and trial courts continue to face substantial challenges in implementing the Bharatiya Sakshya Adhiniyam (BSA), 2023 effectively. Digital evidence is inherently fragile and susceptible to remote alteration, while forensic capabilities remain uneven across states. Many courts lack the infrastructure to securely store electronic records or to present them during proceedings. Moreover, the global nature of digital data complicates collection and verification, particularly when relevant servers are located outside India. In the absence of harmonized Mutual Legal Assistance Treaties (MLATs) and adequate technological support, criminal trials risk delays and uncertainty regarding the reliability of evidence.

Digital records differ fundamentally from traditional paper documents: they are intangible, highly replicable, and prone to tampering. Establishing authenticity requires specialized technical skills, including metadata analysis, hash-value verification, and forensic imaging. Courts often struggle to distinguish between deliberate manipulation and benign alterations caused by system processes or updates. The widespread use of cloud storage further exacerbates these challenges, as retrieving data from foreign servers necessitates formal cross-border cooperation under MLATs, often causing delays in time-sensitive cases. Additionally, the BSA's provisions must be harmonized with the Digital Personal Data Protection Act, 2023, to ensure that evidence collection does not violate privacy rights.

While the BSA introduces a dual-signature requirement-verification by both the custodian and a technical expert-proceedings can slow when qualified experts are unavailable. Establishing a central registry of certified electronic-evidence examiners under Section 79A of the Information Technology Act, 2000, could mitigate this gap. Many courts also lack secure servers or digital presentation systems, making investments in e-court facilities and dedicated repositories critical to translating statutory reforms into practical outcomes.

The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 complements the BSA through procedural innovations such as electronic summons, digital FIRs, and video-recorded searches. When produced from legitimate custody, Section 57 of the BSA recognizes these materials as primary evidence, with Section 63(4) providing verification mechanisms. In an era dominated by automation, authenticity increasingly derives from technology rather than human validation. Subordinate legislation incorporating cryptographic hashing, blockchain-based evidence logs, and detailed metadata audit trails could strengthen digital chains of custody, reducing reliance on manual certification.

Finally, expanding digital evidence must not compromise privacy under Article 21 of the Constitution. Landmark rulings, such as K.S. Putt swamy v. Union of India (2017), emphasize that any intrusion into personal data must be lawful, necessary, and proportionate. Incorporating exclusionary principles for unlawfully obtained electronic evidence would harmonies the BSA's reforms with constitutional safeguards, ensuring justice while protecting individual liberties.

Policy Recommendations and Conclusion

The full potential of the Bharatiya Sakshya Adhiniyam (BSA), 2023 can only be realized through systematic and structured implementation. There is an urgent need for codified Digital Evidence Handling Rules that standardize the collection, preservation, and presentation of electronic records nationwide. Equally critical is the establishment of comprehensive forensic training programmes for police officers and judiciary members, ensuring that all stakeholders can competently manage complex digital material. A tamper-proof National Forensic Data Repository, accessible to courts at all levels, would further secure evidence while streamlining judicial processes. To address the global nature of digital information, India must strengthen mutual legal frameworks for cross-border evidence sharing. Introducing a statutory requirement to periodically revise technical standards every three years would ensure that the legal system keeps pace with rapidly evolving technology.

The enactment of the BSA represents a transformative moment in Indian evidence law. By recognizing electronic records as primary evidence and refining certification requirements, it addresses the procedural rigidity of colonial-era legislation and aligns domestic law more closely with international practices. Yet, the value of these reforms ultimately depends on the authenticity and integrity of the evidence. Certification, rigorous chain-of-custody protocols,

expert verification, and privacy-conscious procedures are essential to ensure that digital records are not merely admissible but also reliable.

Looking forward, the effectiveness of the BSA will depend on harmonizing legislative ambition with practical implementation. Investments in forensic infrastructure, judicial awareness, and technological safeguards will determine whether the law truly transforms evidentiary justice or simply digitizes existing uncertainties. The enduring challenge is to create a system where technology reinforces the pursuit of truth, ensuring that the byte strengthens justice rather than undermines it.