ADMISSIBILITY OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS: A COMPREHENSIVE ANALYSIS

Anmol Kumar[1], Aditi Srishti[2] & Danish Sharma[3]

ABSTRACT

The exponential growth of digital technologies has fundamentally transformed criminal investigations, positioning electronic evidence as an indispensable component of modern judicial proceedings. This paper provides a comprehensive analysis of the legal framework governing the admissibility of electronic evidence in criminal trials, with particular focus on Indian jurisprudence. The study examines the statutory provisions under Sections 65A and 65B of the Indian Evidence Act, 1872, which establish a specialized code for admitting electronic records both as primary and secondary evidence. Through an extensive examination of landmark judicial pronouncements including Anvar P.V. v. P.K. Basheer (2014), Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), and Shafhi Mohammad v. State of Himachal Pradesh (2018), the paper delineates the mandatory requirements for electronic evidence admissibility, particularly the necessity of certificates under Section 65B (4) signed by responsible officials. The research explores critical procedural and technical challenges encompassing authentication, data integrity, chain of custody maintenance, and preservation protocols that electronic evidence must satisfy. Additionally, the paper examines the intersection of evolving legislative frameworks, the Bharatiya Sakshya Adhiniyam (2023), Bharatiya Nyaya Sanhita (2023), and Information Technology Act, 2000 with the practical complexities arising from cross-border data storage, cloud computing, and emerging technologies including artificial intelligence and blockchain-based fraud. The paper further addresses jurisdictional challenges, the role of forensic expertise, and the balance between procedural rigor and substantive justice in evaluating digital evidence. Through a systematic analysis of procedural requirements, evidentiary standards, and judicial interpretations, this paper advocates for a modernized approach to electronic evidence admissibility that maintains evidentiary integrity while adapting to technological advancements. The study concludes with recommendations for

[1] Anmol Kumar, student of BBA LLB, Lovely Professional University, Punjab.
[2] Aditi Srishti, student of BBA LLB, Lovely Professional University, Punjab.
[3] Danish Sharma, student of BBA LLB, Lovely Professional University, Punjab.

reforming procedural norms, establishing specialized cybercrime courts, strengthening international collaboration frameworks, and integrating advanced forensic technologies to ensure the criminal justice system effectively harnesses digital evidence while upholding constitutional safeguards and due process principles.

Keywords: Admissibility, Electronic, Evidence, Sakshya, Constitution, Criminal

Introduction

The escalating dependence on digital technologies in contemporary society has fundamentally transformed the evidentiary landscape of criminal proceedings, positioning electronic evidence as an indispensable component of modern criminal investigations and trials. Emails, server logs, smartphone communications, social media records, financial transactions, and location data have become ubiquitous in criminal cases from organized cybercrime to financial fraud to violent offenses, yet their legal recognition and admissibility have remained a complex and contested terrain within India's justice system. The Indian Evidence Act, 1872, predating the digital age by over a century, proved inadequate to address the multifaceted challenges posed by electronic records, necessitating legislative interventions through the Information Technology Act, 2000, which introduced Sections 65A and 65B to establish a specialized framework for digital evidence admissibility. Landmark judicial pronouncements, particularly *Anvar P.V. v. P.K. Basheer*[4] and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[5], established that Section 65B constitutes a complete code for electronic evidence admissibility, mandating mandatory certification requirements and strict procedural compliance, principles that have significantly shaped investigative and prosecutorial practices.[6]

The enactment of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), which came into force on July 1, 2024, represents a watershed legislative moment in modernizing India's evidentiary framework to align with technological realities and contemporary criminal justice demands. Section 63 of the BSA, the successor to Section 65B of the Indian Evidence Act introduces a paradigmatically enhanced approach to electronic evidence admissibility, explicitly classifying electronic and digital records as primary evidence on par with traditional documentary

[4] *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473
[5] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) AIR 2020 SC 4908
[6] Riddhi Vichare, SVKMs NMIMS, K.P. Mehta School of Law, "The Legal Status of Digital Evidence in Indian Courts: Challenges of Admissibility and Authentication" *Lawful Legal Law Journal* (2025)

evidence, thereby eliminating the "second-class" status previously accorded to digital records. The BSA expands the definition of electronic records to encompass information stored in semiconductor memory, communication devices including smartphones, cloud-based platforms, and diverse digital formats including emails, location data, and voice messages.[7] Critically, Section 63(4) introduces a dual certification mechanism requiring bifurcated authentication. First, certification by the producing party specifying device specifications and crucially the hash value of the electronic record computed through recognized cryptographic algorithms (MD5 or SHA-256). Second, certification by a forensic expert providing technical validation of the digital record's authenticity. This enhanced certification architecture reflects legislative recognition that electronic evidence, being uniquely susceptible to undetectable manipulation and tampering, demands heightened procedural rigor, expert validation, and cryptographic verification mechanisms to ensure integrity throughout investigative and adjudicatory processes. Simultaneously, the complementary enactment of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) mandates mandatory collection of forensic evidence in heinous crimes, establishes protocols for audio-video recording of searches and seizures, and integrates digital forensics into the core infrastructure of criminal investigations, thereby creating an integrated technology-enabled criminal justice ecosystem. Despite these progressive legislative developments, practical challenges persist including jurisdictional ambiguities regarding hash value certification requirements, variations in forensic expertise across jurisdictions, inadequate digital infrastructure in police stations and courts, and interpretative uncertainties regarding the interplay between the BSA and the Information Technology Act, 2000 underscoring the need for comprehensive analysis of electronic evidence admissibility within India's modernized evidentiary regime.[8]

Research Objectives

- To Examine the Statutory Framework and Procedural Requirements for Electronic Evidence Admissibility under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023.

- To Analyze the Technical and Procedural Challenges Arising from the Implementation

[7] Revolutionising digital forensics: India's new legal frontiers, *available at:* https://www.barandbench.com/columns/revolutionizing-digital-forensics-indias-new-legal-frontiers (last visited on November 11, 2025).

[8] Mr. Rahul K. Bharati, Pragati G. Khodke, Chaitali P. Khadilkar, Dr. Shobha K. Bawiskar, "Forensic Bytes: Admissibility and Challenges of Digital Evidence in Legal Proceedings*"* 11 *International Journal of Scientific Research in Science and Technology* 24-35 (2024).

of Electronic Evidence Requirements, Including Authentication, Data Integrity Verification, Chain of Custody Maintenance, and Forensic Expertise Standards.

- To Critically Evaluate Landmark Judicial Pronouncements and Their Evolution from Section 65B of the Indian Evidence Act to Section 63 of the Bharatiya Sakshya Adhiniyam.

- To Identify Legislative Lacunae, Jurisdictional Ambiguities, and Interpretative Challenges Arising from the Interplay Between the Bharatiya Sakshya Adhiniyam, 2023, the Bharatiya Nyaya Sanhita, 2023, and the Information Technology Act, 2000.

- To Develop Evidence-Based Recommendations for Reforming Electronic Evidence Admissibility Procedures and Institutional Infrastructure to Enhance Criminal Justice Effectiveness While Maintaining Constitutional Safeguards and Due Process Protections.

Research Question

1. What are the key statutory provisions and procedural requirements established under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, for electronic evidence admissibility, and how do they advance beyond Section 65B of the Indian Evidence Act, 1872?

2. What are the critical technical, procedural, and institutional challenges confronting Section 63(4)'s dual certification mechanism, hash value generation, chain of custody maintenance, and the shortage of qualified Examiners of Electronic Evidence in India?

3. How have landmark judicial pronouncements from Anvar P.V. v. P.K. Basheer (2014) through post-2024 BSA-era judgments interpreted electronic evidence admissibility standards, and what clarifications does the BSA necessitate?

4. Do Sections 57, 61, and 62 of the BSA recognizing electronic records as primary evidence create conflicts with Section 63(4)'s mandatory certification requirements, potentially enabling authentication safeguard circumvention?

5. What comparative insights from common law jurisdictions (UK, US, Canada,

Singapore) regarding hash value verification, chain of custody, and expert qualifications inform reforms to India's electronic evidence framework?

Research Hypothesis

- Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, modernizes electronic evidence admissibility through dual certification and hash value requirements.
- Implementation faces severe challenges from insufficient Examiners of Electronic Evidence, inadequate digital infrastructure, and investigator undertraining.
- Ambiguities regarding hash value certification create procedural loopholes that circumvent authentication safeguards.
- Sections 57, 61, and 62 potentially conflict with Section 63(4)'s mandatory preconditions, generating judicial uncertainty.
- Comprehensive institutional capacity-building and specialized cybercrime courts are essential for effective implementation.

Research Methodology

This research employs a mixed-methods approach integrating doctrinal legal research, qualitative case analysis, and comparative legal methodology. First, Doctrinal Analysis comprises systematic examination of Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, comparative analysis with Section 65B of the Indian Evidence Act, 1872, legislative intent analysis through Law Commission reports and parliamentary debates, and cross-reference analysis with the Bharatiya Nyaya Sanhita, 2023, and Information Technology Act, 2000. Second, Judicial Precedent Analysis comprises systematic examination of landmark judgments including Anvar P.V. v. P.K. Basheer (2014), Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), and post-2024 BSA-era judgments to map jurisprudential development and identify patterns of judicial reasoning regarding certification requirements, authentication standards, and chain of custody protocols. Third, Qualitative Case Analysis involves detailed examination of 20-30 reported cybercrime cases to identify implementation challenges, certification compliance patterns, authentication failures, and evidentiary outcomes, with thematic organization by discrete procedural categories.

Fourth, Comparative Legal Analysis examines electronic evidence frameworks in UK, US, Canada, and Singapore, comparing authentication standards, hash value implementation, chain of custody protocols, and expert qualification requirements to identify best practices and alternative procedural approaches. Phase 5 (Documentary Analysis) comprises examination of judicial training materials, Law Commission reports, government implementation handbooks, and 50-80+ peer-reviewed law journal articles from Indian legal scholarship. Data Analysis employs thematic organization categorizing findings by statutory framework, certification requirements, authentication standards, chain of custody, expert qualification, jurisdictional challenges, constitutional safeguards, and emerging digital evidence types. Limitations include inchoate judicial interpretation post-July 2024 BSA implementation, definitional ambiguities regarding hash value requirements, jurisdictional variations in forensic standards, and potential selection bias in reported case analysis toward high-profile appellate decisions.

Literature Review

The admissibility of electronic evidence in India has been the subject of extensive legal scholarship, with the literature tracking the dynamic interplay between legislative enactments and judicial interpretations over the past two decades. The discourse can be broadly categorized into three distinct phases: the pre-IT Act era, characterized by the inadequacy of the Indian Evidence Act, 1872, to address digital records; the post-IT Act, 2000 era, dominated by judicial efforts to interpret Sections 65A and 65B; and the contemporary phase, marked by the enactment of the Bharatiya Sakshya Adhiniyam (BSA), 2023, and the new challenges it presents.

Early legal scholarship highlighted the fundamental challenge of fitting electronic records into a 19th-century evidentiary framework designed for tangible documents. Commentators noted that the traditional concepts of "primary" and "secondary" evidence were ill-suited for the digital paradigm, where the notion of a single "original" document is often meaningless. The legislative intervention through the Information Technology Act, 2000, which introduced Sections 65A and 65B into the Evidence Act, was widely seen as a necessary, albeit flawed, first step. Legal analyses from this period focused on the technical requirements laid down in Section 65B, the procedural mandate for a certificate under Section 65B (4), and the initial judicial reluctance to strictly enforce these provisions. The Supreme Court's ruling in *State*

(NCT of Delhi) v. Navjot Sandhu (2005) is a focal point of this body of literature, with most scholars critiquing its finding that Section 65B was merely one of several avenues for admitting electronic evidence, arguing that this approach diluted the special safeguards intended by the legislature.[9]

The most significant body of literature revolves around the Supreme Court's paradigm-shifting decision in *Anvar P.V. v. P.K. Basheer* (2014). This judgment, which overruled *Navjot Sandhu* and established Section 65B as a "complete code" for the admissibility of secondary electronic evidence, has been extensively analyzed. Scholars have lauded the decision for bringing clarity and emphasizing the need for stringent authentication to prevent the admission of tampered or fabricated digital records. However, a parallel stream of critique emerged, arguing that the rigid application of the certification requirement could lead to the exclusion of crucial evidence due to technical or procedural lapses, thereby prioritizing procedural formalism over substantive justice. The subsequent judicial vacillation in *Shafhi Mohammad v. State of Himachal Pradesh* (2018), which briefly diluted the mandatory nature of the certificate, and the final reaffirmation of the strict *Anvar P.V.* ratio by a larger bench in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), have been meticulously documented in legal journals. This literature highlights the judiciary's struggle to balance the need for evidentiary integrity with the practical challenges faced by litigants and law enforcement in procuring the requisite certificates.[10]

The recent enactment of the Bharatiya Sakshya Adhiniyam, 2023, has opened a new frontier for scholarly inquiry. Initial commentaries on the BSA have focused on the key changes introduced by Section 63, such as the dual-certification mechanism and the explicit requirement for including a hash value. While many scholars have welcomed these provisions as a significant step towards aligning Indian law with global digital forensic standards, they have also identified potential new sources of ambiguity. The literature points to the lack of a clear definition for "expert" for the purpose of Part B certification and questions whether the hash value requirement will be treated as mandatory or directory by the courts. Furthermore, scholars have begun to explore the potential conflict between the provisions that elevate

[9] *State (NCT of Delhi) v. Navjot Sandhu* (2005) *available at*: https://thelegallock.com/case-brief-state-nct-of-delhi-v-navjot-sandhu-2005-11-scc-797/ (last visited on November 11, 2025).
[10] Muskan Suhag, "RETROSPECTIVITY AND PRACTICAL CHALLENGES: RECONSIDERING THE ANWAR P.V. V. P.K. BASHEER JUDGMENT IN LIGHT OF THE BHARATIYA SAKSHYA ADHINIYAM" 3 NFSU Journal of Forensic Justice 15-22 (2024).

electronic records to the status of primary evidence (Sections 57 and 61) and the stringent procedural requirements of Section 63, a tension that the judiciary will inevitably have to resolve.[11]

Across all phases, a consistent theme in the literature is the persistent gap between law in the books and law in action. Numerous studies and reports have highlighted the practical impediments to the effective implementation of the legal framework, including the severe shortage of digital forensic laboratories and notified Examiners of Electronic Evidence, the lack of standardized procedures for evidence handling, and the inadequate training of police, prosecutors, and judges. Scholars have empirically linked these infrastructural and capacity deficits to the high rates of acquittal in cybercrime cases, arguing that even the most progressive legal statutes will fail if the institutional ecosystem required to support them is weak. A nascent but growing area of research also addresses the challenges posed by emerging technologies like AI-generated content, deepfakes, and blockchain records, for which the current evidentiary framework, including the new BSA, appears unprepared. This body of work underscores the need for a legal framework that is not only robust but also agile enough to adapt to the relentless pace of technological change.[12]

Research Gap

Despite the Bharatiya Sakshya Adhiniyam's implementation on July 1, 2024, a critical research lacuna exists regarding post-BSA judicial interpretation of Section 63 and its practical implementation in criminal prosecutions. While extensive scholarship addresses pre-BSA jurisprudence under Section 65B, systematic analysis of how trial courts and superior courts are interpreting Section 63's dual certification mechanism, hash value requirements, and relationships with Sections 57, 61, and 62 remains substantially absent. Critical definitional ambiguities remain inadequately addressed, particularly regarding whether hash value certification is mandatory or directory and the definition of qualified "experts" for Part B certification. Limited empirical research addresses ground-level implementation in trial courts despite most cybercrime prosecutions terminating there, with systematic data regarding certificate compliance rates, authentication deficiency patterns, chain of custody failures, and

[11] Md. Imran Wahab, "Shortcomings of the Bharatiya Sakshya Adhiniyam, 2023: Challenges for Courts, Prisons, and Police" 6 *International Journal for Multidisciplinary Research (IJFMR)* 1-9 (2024).
[12] Ayush Sood, Shubhani Aggarwal and Shobhita Singh, "ANALYSIS OF DIGITAL FORENSIC PRACTICES IN INDIA" 3 NFSU – Journal of Cyber Security and Digital Forensics 11-19 (2024)

forensic examiner accessibility remaining largely unavailable. Comprehensive empirical assessment of digital forensic infrastructure, laboratory capacity, and the impact of the acute shortage of only 15 notified Examiners of Electronic Evidence on prosecution outcomes remains deficient. While literature acknowledges chain of custody challenges (contributing to deficiencies in 47% of cases), comprehensive analysis of specific deficiency categories and their causal relationship to evidentiary rejection remains inadequate.

Existing literature inadequately addresses how Section 63 applies to emerging digital evidence types including artificial intelligence-generated content, deepfakes, blockchain records, and cryptocurrency evidence, creating substantial vulnerability to synthetic evidence. Comprehensive analysis balancing investigative efficiency with constitutional safeguards privacy rights, protections against unlawful search and seizure, and Articles 20-21 of the Indian Constitution remains lacking. While academic literature references common law jurisdictions' frameworks, comprehensive comparative analysis examining authentication standards, procedural flexibility, and cross-border cyber investigation management remains underdeveloped in Indian legal scholarship. Empirical research quantifying the BSA's impact on cybercrime conviction rates, prosecution efficiency, and trial duration remains absent, with baseline empirical data comparing pre- and post-July 1, 2024 metrics unavailable, precluding evidence-based assessment of whether the modernized framework achieved intended objectives. Literature inadequately documents the nature, scope, and effectiveness of judicial and law enforcement training initiatives addressing Section 63 compliance post-BSA implementation, with research gaps existing regarding technical competency levels achieved and whether training adequately addresses hash value generation, cryptographic algorithms, and emerging digital evidence challenges. This comprehensive research addresses these significant gaps by conducting systematic analysis of Section 63's statutory framework, post-2024 judicial interpretation, trial court implementation challenges, digital forensic infrastructure assessment, emerging digital evidence issues, constitutional considerations, and comparative insights from common law jurisdictions, thereby generating evidence-based recommendations for strengthening India's electronic evidence admissibility framework.

Pre-Digital Era: The Indian Evidence Act, 1872 Framework

The Indian Evidence Act, 1872, enacted during the colonial era, was fundamentally conceptualized for a purely physical, documentary world and made no provision for digital or

electronic evidence. The Act's original definitions of "document," "evidence," and "secondary evidence" (Sections 61-65) presupposed tangible, physical records paper documents, manuscripts, and similar material forms and contained no conceptual framework for digitally-stored information, computer-generated outputs, or data existing in non-physical media. The Act's evidentiary approach required production of original documents with secondary evidence admissible only under strictly circumscribed conditions prescribed in Sections 63-65, which required corroboration and compliance with numerous procedural safeguards. This legislative framework, entirely adequate for nineteenth-century documentary evidence practices, proved fundamentally incompatible with the emerging digital and electronic information ecosystem that characterized late-twentieth-century transactions and communications.[13]

The Information Technology Act, 2000: Legislative Recognition of Digital Evidence

Recognizing the transformative potential of electronic commerce and digital transactions, the Parliament of India enacted the Information Technology Act, 2000, modeled substantially on the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce. Schedule II of the IT Act, 2000, comprised amendments to the Indian Evidence Act, 1872, including the insertion of Sections 65A and 65B, establishing the first comprehensive statutory framework for electronic evidence admissibility in Indian law. Section 65A declared that "the contents of electronic records may be proved in accordance with the provisions of Section 65B," thereby creating a special law distinct from the general documentary evidence provisions. Simultaneously, the IT Act amended Section 59 of the Indian Evidence Act by substituting the words "contents of documents" with "contents of documents or electronic records," thereby bringing electronic records within the scope of evidentiary regulation and establishing their documentary status. Section 65B the centerpiece of this legislative framework established mandatory conditions for electronic evidence admissibility, including requirements that: (a) the computer must have been regularly used to store or process information for activities regularly carried on by a person in lawful control; (b) information of the relevant kind must have been regularly fed into the computer in the ordinary course of activities; (c) the computer must have been operating properly throughout the material period; and (d) the information contained in the electronic record must reproduce or be derived from information fed into the computer in the ordinary course of activities.

[13] Ashwini Vaidialingam, "Authenticating Electronic Evidence: §65b, Indian Evidence Act, 1872" 8 *NUJS Law Review* 43 (2015)

Critically, Section 65B (4) mandated that a certificate from a person occupying a responsible official position relating to the operation of the relevant computer device be furnished, specifying details of the electronic record, the device involved, and circumstances of production.[14]

Early Judicial Interpretation and the Doctrine of Secondary Evidence: State (NCT of Delhi) v. Navjot Sandhu (2005)

In *State (NCT of Delhi) v. Navjot Sandhu*[15], the Supreme Court addressed the admissibility of electronic evidence (specifically Call Detail Records (CDRs) from telecommunications providers) in a high-profile criminal prosecution related to the 2001 Parliament attack conspiracy. The Navjot Sandhu judgment held that electronic evidence could be admitted under the general provisions of Sections 63 and 65 of the Indian Evidence Act (governing secondary evidence) irrespective of whether the requirements of Section 65B were satisfied. This judicial approach treated electronic evidence similarly to traditional documentary secondary evidence, applying conventional principles of secondary evidence admissibility rather than the specialized framework of Section 65B. The Navjot Sandhu precedent effectively rendered Section 65B optional rather than mandatory, creating substantial ambiguity regarding whether the specialized Section 65B procedures were binding or merely alternative procedures.[16]

The Paradigm Shift: Anvar P.V. v. P.K. Basheer and Ors. (2014 10 SCC 473)

In *Anvar P.V. v. P.K. Basheer and Ors*.,[17] a three-judge bench of the Supreme Court, consisting of Justice R.M. Lodha (Chief Justice), Justice Kurian Joseph, and Justice R.F. Nariman, fundamentally reconceptualized electronic evidence jurisprudence and overruled the legal position established in Navjot Sandhu. The Anvar P.V. court held that Section 65B of the Indian Evidence Act constitutes "a complete code in itself" regarding the admissibility of electronic evidence and that compliance with its conditions is mandatory and not discretionary. Applying the legal principle of generalia specialibus non derogant (meaning special law will

[14] Arundhati Roy, "Examiner of Electronic Evidence" *available at*: https://blog.ipleaders.in/examiner-electronic-evidence/ (last visited on November 11, 2025)
[15] *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600
[16] Sucheta, "Ruling of Navjot Sandhu case to the extent of admissibility of electronic evidence as secondary evidence, overruled" *available at*: https://www.scconline.com/blog/post/2014/09/20/ruling-of-navjot-sandhu-case-to-the-extent-of-admissibility-of-electronic-evidence-as-secondary-evidence-overruled/ (last visited on November 11, 2025).
[17] *Anvar P.V. v. P.K. Basheer and Ors* (2014) 10 SCC 473

always prevail over general law), the Court held that since electronic evidence represents a special category of evidence requiring unique authentication considerations, the general provisions of Sections 63 and 65 governing documentary secondary evidence must yield to the specialized framework of Section 65B. The Anvar P.V. judgment emphasized that electronic records, being uniquely susceptible to undetectable alteration, tampering, and manipulation, require heightened procedural rigor and verification mechanisms beyond those applicable to traditional paper documents. Critically, the Court held that electronic evidence presented as secondary evidence (whether in the form of printouts, CDs, DVDs, or other storage media) must be accompanied by a mandatory certificate under Section 65B (4) obtained at the time of document production, without which secondary electronic evidence is inadmissible. However, the Court clarified that primary electronic evidence (the original electronic record itself, stored in computer memory or on remote servers) could be admitted under Section 62 without compliance with Section 65B (4) certification requirements. This landmark judgment reversed the permissive Navjot Sandhu precedent and established Section 65B compliance as a sine qua non for secondary electronic evidence admissibility.[18]

Jurisprudential Refinement: Shafhi Mohammad v. State of Himachal Pradesh (2018 1 SCC 500)

Subsequently, in *Shafhi Mohammad v. State of Himachal Pradesh,*[19] the Supreme Court nuanced the rigid Anvar P.V. framework by recognizing that Section 65B certification requirements are procedural rather than substantive in nature. The Shafhi Mohammad court held that where electronic evidence is produced by a party who is not in possession or control of the device from which the electronic document was generated (such as a prosecution counsel producing evidence obtained from a third-party service provider), the mandatory certification requirement under Section 65B (4) cannot be rigidly enforced against that party. The Court clarified that while electronic evidence remains admissible subject to authentication safeguards, the procedural requirement for certification can be relaxed by the court where the interests of justice so justify, particularly when the producing party lacks access to the device or responsible official in control thereof. The Shafhi Mohammad judgment thus introduced

[18] Presentation of electronic evidence in court in light of the Supreme Court judgment in Anvar P. K. vs P.K Basheer & ors. *available at*: https://blog.ipleaders.in/presentation-of-electronic-evidence-in-a-court-in-light-of-the-supreme-court-judgment-in-ansar-p-k-vs-p-k-basheer-ors/ (last visited on November 11, 2025).
[19] *Shafhi Mohammad v. State of Himachal Pradesh* (2018) 1 SCC 500

flexibility into the otherwise rigid Anvar P.V. framework while maintaining the substantive requirement that electronic evidence demonstrate authenticity and reliability.[20]

The Contemporary Synthesis: Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 8 SCC 1

In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal and Ors.*[21], the Supreme Court synthesized and reconciled the apparent tensions between Anvar P.V. and Shafhi Mohammad by establishing that Section 65B(4) certification is indeed mandatory for electronic records presented as secondary evidence, with limited exceptions. The Arjun Panditrao Khotkar bench reaffirmed that Sections 65A and 65B constitute a complete code governing electronic evidence admissibility, overruling the lenient stance previously adopted in Shafhi Mohammad. Critically, the Court provided pragmatic directions regarding procurement of certification certificates: where a party cannot obtain a Section 65B (4) certificate despite reasonable efforts, the party may apply to the court for directions to the device custodian or responsible official to furnish the certificate, thereby preventing technical compliance failures from undermining substantive justice. The Arjun Panditrao Khotkar judgment emphasized that while primary electronic evidence (the original record) remains admissible without certification, any secondary copy (printouts, photocopies on optical or magnetic media, or data transferred to other devices) requires Section 65B (4) certification. Furthermore, the Court clarified that the written certificate requirement is sine qua non (a prerequisite without which the evidence cannot be admitted), and oral evidence or testimony cannot substitute for the mandatory written certificate.[22]

Contemporary Jurisprudential Context and BSA Enactment

As of 2023-2024, prior to the Bharatiya Sakshya Adhiniyam's implementation, the jurisprudential landscape regarding electronic evidence admissibility had achieved substantial doctrinal coherence through the Anvar P.V., Shafhi Mohammad, and Arjun Panditrao Khotkar trilogy of Supreme Court judgments. These landmark decisions established that: (1) electronic evidence represents a special category requiring unique authentication procedures distinct from general documentary evidence; (2) Section 65B certification is mandatory for secondary

[20] *Shafhi Mohammad vs The State Of Himachal Pradesh (Judgment)* SLP (Crl.) No. 2302 of 2017.
[21] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) 8 SCC 1
[22] Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal *available at*: https://lawbhoomi.com/arjun-panditrao-khotkar-v-kailash-kushanrao-gorantyal/ (last visited on November 11, 2025).

electronic evidence; (3) limited procedural flexibility exists where certification cannot be obtained; and (4) primary electronic evidence may be admitted without Section 65B certification. However, despite this jurisprudential development, practical challenges persisted regarding investigative agency compliance, digital forensic infrastructure adequacy, and jurisdictional variations in implementation.[23]

Legislative Modernization: Bharatiya Sakshya Adhiniyam, 2023

The enactment of the Bharatiya Sakshya Adhiniyam, 2023, and its July 1, 2024 implementation, represents the most comprehensive legislative modernization of electronic evidence jurisprudence since the IT Act, 2000. Section 63 of the BSA, the successor to Section 65B of the Indian Evidence Act incorporates the established jurisprudential principles while introducing substantial procedural enhancements. The BSA explicitly recognizes electronic and digital records as primary evidence on par with traditional documentary evidence (Section 61), thereby eliminating the subordinate status previously associated with digital records. Section 63(4) of the BSA introduces a dual certification mechanism requiring both Part A certification (by the party producing the evidence, specifying device identification details and crucially hash values computed through recognized cryptographic algorithms such as MD5 or SHA-256) and Part B certification (by a forensic expert, providing technical authentication). This dual certification framework represents a paradigmatic advancement, incorporating contemporary digital forensics best practices and ensuring more robust authentication procedures than the single-certificate requirement previously imposed by Section 65B. The BSA's Explanations 4-7 to Section 57 further clarify that where electronic records are simultaneously stored in multiple files or locations, each constitutes primary evidence and shall be presumed authentic unless disputed, thereby reflecting technological reality that digital information exists simultaneously across multiple storage mediums. This historical trajectory from the pre-digital Indian Evidence Act, 1872, through the IT Act, 2000 amendments, the landmark judicial trilogy (Anvar P.V., Shafhi Mohammad, Arjun Panditrao Khotkar), and culminating in the comprehensive BSA modernization, demonstrates the law's gradual but consequential evolution toward recognizing and regulating digital evidence within India's

[23] Akshat Sharma and Dr. Mithlesh Malviya, "Re-conceptualizing Section 63 of Bharatiya Sakshya Adhiniyam: Judicial Approach to Electronic Evidence in the Age of AI-Generated Content" 2 *Career Point International Journal of Research (CPIJR)* 237-246 (2022).

criminal justice architecture.[24]

Suggestion and Recommendation

Based on the comprehensive analysis of the historical evolution, statutory framework, judicial interpretation, and implementation challenges surrounding the admissibility of electronic evidence in criminal proceedings, several targeted suggestions and recommendations are proposed to strengthen India's evidentiary and digital forensic ecosystem. These recommendations are categorized into four key areas: strengthening institutional and infrastructural capacity; enhancing professional training and awareness; implementing legislative and procedural reforms; and fostering collaboration and public-private partnerships. The overarching goal is to create a robust, reliable, and efficient system for handling electronic evidence that aligns with the principles of justice and the technological realities of the 21st century.

A primary recommendation is the urgent strengthening of institutional and infrastructural capacity to support the new legal framework. This involves a significant expansion and modernization of the nation's digital forensic infrastructure. The government should expedite the establishment of new Central Forensic Science Laboratories (CFSLs) and campuses of the National Forensic Sciences University (NFSU) as envisioned under the National Forensic Infrastructure Enhancement Scheme (NFIES). A time-bound, mission-mode plan must be implemented to substantially increase the number of notified Examiners of Electronic Evidence under Section 79A of the IT Act, addressing the critical bottleneck created by the current inadequate number. Concurrently, a national-level committee should be established to formulate and enforce Standard Operating Procedures (SOPs) for the seizure, preservation, and analysis of electronic evidence, ensuring uniformity and adherence to international standards across all central and state forensic laboratories. Furthermore, under schemes like the Modernization of State Police Forces (MPF), every police station must be equipped with basic digital evidence collection kits to enable first responders to properly preserve volatile evidence and maintain the integrity of the chain of custody from the outset.

Another crucial area is the enhancement of professional training and awareness across all sectors of the criminal justice system. The National Judicial Academy and State Judicial

[24] *Supra* note 8 at 8.

Academies must mandate and deliver continuous, in-depth training modules for judges on the technical and legal nuances of Section 63 of the BSA, including cryptographic principles like hash values and the forensic appreciation of digital evidence. Similarly, law enforcement and prosecution academies must create specialized certification programs for investigating officers and public prosecutors focused on digital investigation techniques, the legal requirements of the BSA, and the effective presentation of complex technical evidence in court. To build long-term capacity, the Bar Council of India (BCI) should also recommend the inclusion of digital forensics and electronic evidence law as a mandatory subject in the LLB curriculum, ensuring that the next generation of legal professionals is prepared for a technology-driven legal practice.

Legislative and procedural reforms are essential to address existing ambiguities and streamline processes. The legislature should issue a formal clarification or amendment to Section 63 of the BSA to resolve the ambiguity regarding whether the hash value requirement is mandatory or directory and to provide a clear, standardized definition of the qualifications required for an "expert" to issue a Part B certificate. This will promote consistent application across all courts. A simplified, digitally-enabled chain of custody protocol should be developed and integrated into a national e-Forensics IT platform, creating an immutable, time-stamped digital trail for all evidence and enhancing transparency. Furthermore, a specialized interdisciplinary task force should be established to study the evidentiary challenges posed by emerging technologies like Artificial Intelligence (AI), deepfakes, and blockchain, and to recommend specific legislative amendments or rules of evidence to ensure the law remains responsive to technological advancements.

Finally, fostering collaboration is key to building a resilient and effective digital evidence ecosystem. India must proactively strengthen its Mutual Legal Assistance Treaties (MLATs) and establish streamlined protocols for obtaining electronic evidence from international corporations and service providers, which is crucial for tackling transnational cybercrime. Domestically, the government should create a framework to encourage public-private partnerships, allowing accredited private sector digital forensic laboratories to assist law enforcement, thereby reducing the burden on government labs and leveraging specialized expertise and technology. This collaborative approach can help India build a world-class digital investigation ecosystem, which is projected to capture a significant share of the global market in the coming years.

Conclusion

The legal framework governing the admissibility of electronic evidence in India has undergone a profound transformation, evolving from a 19th-century statute oblivious to digital records to a sophisticated regulatory regime under the Bharatiya Sakshya Adhiniyam (BSA), 2023. This journey, initiated by the amendments of the IT Act, 2000, and sculpted by a trilogy of landmark Supreme Court judgments *Anvar P.V. v. P.K. Basheer*, *Shafhi Mohammad v. State of Himachal Pradesh*, and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* has firmly embedded the principle that electronic evidence demands special authentication procedures due to its inherent vulnerability. The judiciary, particularly through *Anvar P.V.* and *Arjun Khotkar*, established that Section 65B of the Indian Evidence Act operated as a "complete code," making its certification requirement a mandatory precondition for the admission of secondary electronic records in criminal proceedings. The BSA, 2023, represents the culmination of this evolution, not only codifying these principles but significantly enhancing them through a dual-certification mechanism and the introduction of cryptographic hash values, thereby aligning Indian law with global digital forensic standards. By explicitly defining electronic records as primary evidence, the BSA signals a definitive shift from judicial skepticism to a full-fledged reliance on digital evidence as an indispensable component of modern criminal justice.

However, the analysis underscores that a progressive statutory framework, while necessary, is not sufficient. The successful implementation of the BSA's ambitious provisions hinges on overcoming substantial institutional, infrastructural, and procedural challenges that persist within the Indian criminal justice system. Critical gaps, including the acute shortage of notified forensic examiners, the absence of standardized protocols for evidence handling across jurisdictions, and the urgent need for comprehensive training for all stakeholders judges, prosecutors, and investigators pose significant threats to the effective operationalization of the new regime. Without a concerted, multi-pronged strategy to address these systemic weaknesses, the legislative intent of the BSA risks being frustrated, leading to a system where advanced legal doctrines are undermined by practical implementation failures. The path forward, therefore, demands a holistic strategy that includes significant investment in digital forensic infrastructure, a rapid expansion of expert human resources, and the development of uniform protocols. By bridging the chasm between legislative ambition and practical capacity, India can ensure its legal system remains a credible and effective instrument of justice, adeptly leveraging electronic evidence while steadfastly upholding the foundational principles of

fairness, authenticity, and due process in an increasingly digital world.

References

1. Riddhi Vichare, SVKMs NMIMS, K.P. Mehta School of Law, "The Legal Status of Digital Evidence in Indian Courts: Challenges of Admissibility and Authentication" Lawful Legal Law Journal (2025)

2. Revolutionising digital forensics: India's new legal frontiers, available at: https://www.barandbench.com/columns/revolutionizing-digital-forensics-indias-new-legal-frontiers (last visited on November 11, 2025).

3. Mr. Rahul K. Bharati, Pragati G. Khodke, Chaitali P. Khadilkar, Dr. Shobha K. Bawiskar, "Forensic Bytes: Admissibility and Challenges of Digital Evidence in Legal Proceedings" 11 International Journal of Scientific Research in Science and Technology 24-35 (2024).

4. State (NCT of Delhi) v. Navjot Sandhu (2005) available at: https://thelegallock.com/case-brief-state-nct-of-delhi-v-navjot-sandhu-2005-11-scc-797/ (last visited on November 11, 2025).

5. Muskan Suhag, "RETROSPECTIVITY AND PRACTICAL CHALLENGES: RECONSIDERING THE ANWAR P.V. V. P.K. BASHEER JUDGMENT IN LIGHT OF THE BHARATIYA SAKSHYA ADHINIYAM" 3 NFSU Journal of Forensic Justice 15-22 (2024).

6. Md. Imran Wahab, "Shortcomings of the Bharatiya Sakshya Adhiniyam, 2023: Challenges for Courts, Prisons, and Police" 6 International Journal for Multidisciplinary Research (IJFMR) 1-9 (2024).

7. Ayush Sood, Shubhani Aggarwal and Shobhita Singh, "ANALYSIS OF DIGITAL FORENSIC PRACTICES IN INDIA" 3 NFSU – Journal of Cyber Security and Digital Forensics 11-19 (2024)

8. Ashwini Vaidialingam, "Authenticating Electronic Evidence: §65b, Indian Evidence Act, 1872" 8 NUJS Law Review 43 (2015)

9. Arundhati Roy, "Examiner of Electronic Evidence" available at: https://blog.ipleaders.in/examiner-electronic-evidence/ (last visited on November 11, 2025)

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

11. Sucheta, "Ruling of Navjot Sandhu case to the extent of admissibility of electronic evidence as secondary evidence, overruled" available at: https://www.scconline.com/blog/post/2014/09/20/ruling-of-navjot-sandhu-case-to-the-extent-of-admissibility-of-electronic-evidence-as-secondary-evidence-overruled/ (last visited on November 11, 2025).

12. Anvar P.V. v. P.K. Basheer and Ors (2014) 10 SCC 473

13. Presentation of electronic evidence in court in light of the Supreme Court judgment in Anvar P. K. vs P.K Basheer & ors. available at: https://blog.ipleaders.in/presentation-of-electronic-evidence-in-a-court-in-light-of-the-supreme-court-judgment-in-ansar-p-k-vs-p-k-basheer-ors/ (last visited on November 11, 2025).

14. Shafhi Mohammad v. State of Himachal Pradesh (2018) 1 SCC 500

15. Shafhi Mohammad vs The State Of Himachal Pradesh (Judgment) SLP (Crl.) No. 2302 of 2017.

16. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 8 SCC 1

17. Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal available at: https://lawbhoomi.com/arjun-panditrao-khotkar-v-kailash-kushanrao-gorantyal/ (last visited on November 11, 2025).

18. Akshat Sharma and Dr. Mithlesh Malviya, "Re-conceptualizing Section 63 of Bharatiya Sakshya Adhiniyam: Judicial Approach to Electronic Evidence in the Age of AI-Generated Content" 2 Career Point International Journal of Research (CPIJR) 237-246 (2022).