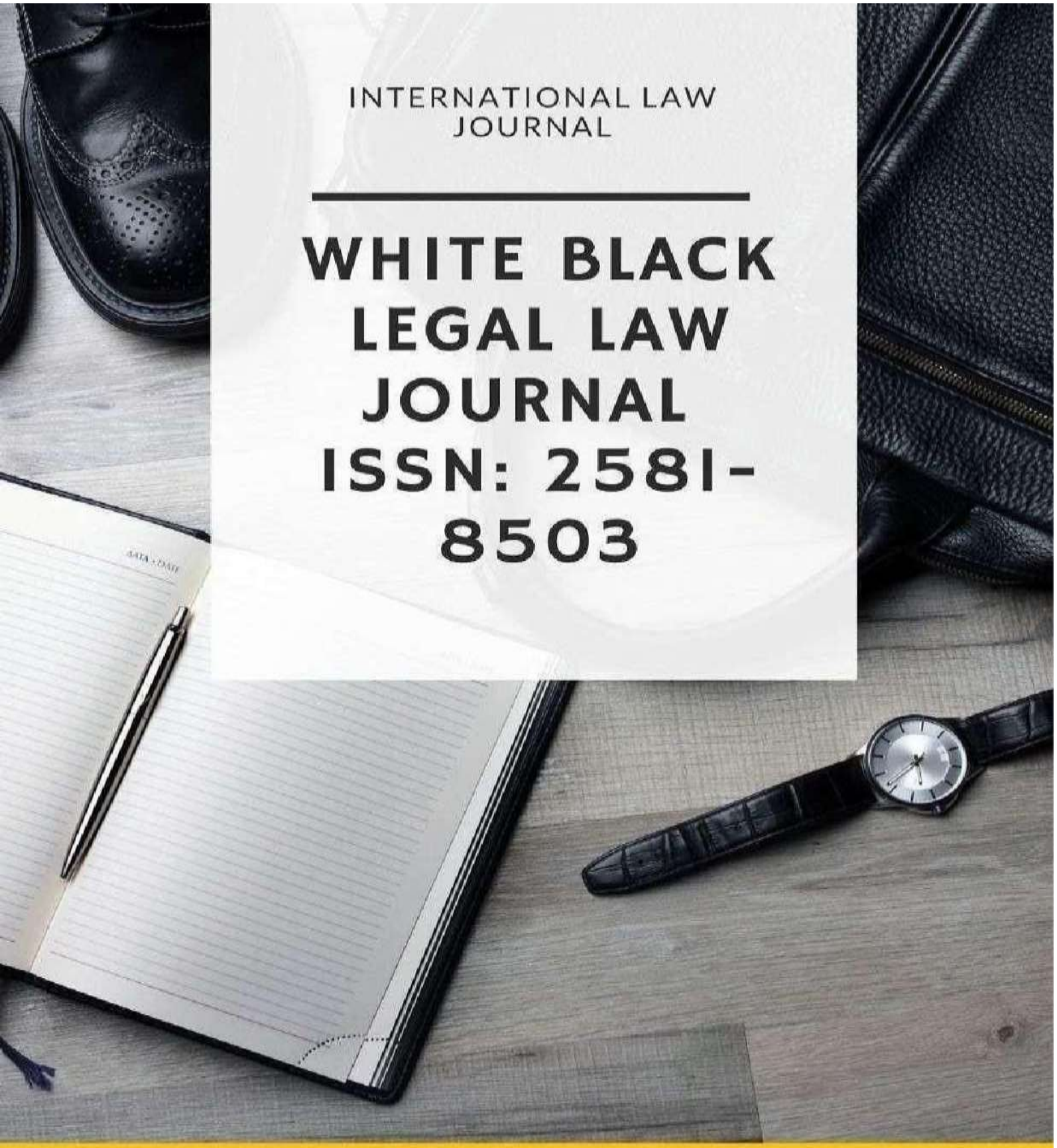

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

DIGITAL EVIDENCE ON TRIAL: INVESTIGATING AGENCY CHALLENGES, JUDICIAL CONFUSION, AND THE QUEST FOR RELIABILITY UNDER INDIA'S NEW EVIDENCE LAW

AUTHORED BY – IMMANUEL
Christ Deemed to be University

ABSTRACT

The admissibility of electronic evidence in the Indian legal system has undergone a significant transformation with the replacement of the Indian Evidence Act, 1872 by the Bharatiya Sakshya Adhiniyam (BSA), 2023. This paper critically examines three intertwined research questions: whether the BSA has resolved the long-standing judicial confusion over mandatory versus supplementary certification under Section 65B (now Section 63); the practical and procedural challenges investigating agencies face in complying with the "original" electronic record requirement, particularly for volatile and cloud-based data; and whether the BSA tilts toward probative value or retains rigorous pre-admission safeguards in the age of AI-generated content and deepfakes.

Adopting a doctrinal legal research methodology, this study analyses statutory provisions, judicial precedents from *Navjot Sandhu* (2005) to *Khotkar* (2020) and post-BSA rulings, official reports, and forensic literature. The findings reveal that while the BSA modernises the framework—expanding definitions to include semiconductor memory and communication devices, introducing a prescribed certificate format with mandatory hash values, and establishing parity between electronic and physical documents under Section 61 it does not fully eradicate confusion. Ambiguities persist regarding primary versus secondary characterisation of electronic records, expert qualifications, certificate production timing, and the dual regime for pending cases under Section 170(2). Investigating agencies face severe infrastructural and capacity deficits, leading to frequent evidence exclusion and low cybercrime conviction rates (around 22% as per NCRB). Normatively, the BSA leans toward balanced modernisation rather than radical flexibility: it strengthens procedural safeguards (dual signatures, expert certification) while extending parity to electronic records. The Supreme Court's recent "twin-test" for AI-generated evidence further signals judicial tightening.

The paper concludes that the BSA provides a progressive statutory foundation, but its

effectiveness depends on legislative rules for expert accreditation, institutional investment in forensic labs and training, judicial guidance on substantial compliance, and technological adoption of blockchain-based evidence management. Without these ecosystem reforms, the gap between legal rigour and on-ground capability will continue to undermine digital justice in India.

Keywords: Electronic evidence, Section 65B IEA, Section 63 BSA, admissibility, certification, cybercrime, secondary evidence, probative value, deepfakes, Bharatiya Sakshya Adhiniyam 2023.

INTRODUCTION:

BACKGROUND: EVOLUTION OF EVIDENCE LAW IN THE DIGITAL AGE

The advent of digital technology has fundamentally transformed how information is created, stored, and transmitted[1]. Unlike traditional documentary evidence paper writings, physical signatures, or tangible objects electronic records exist in binary code, are often invisible to the naked eye, and can be altered without leaving physical traces. Recognising this paradigm shift, the Indian Parliament amended the Indian Evidence Act, 1872 (IEA) through the Information Technology Act, 2000 (IT Act)[2]. These amendments introduced Sections 65A and 65B into the IEA, creating a special regime for the admissibility of electronic records. Section 65A stipulated that the admissibility of electronic records would be governed exclusively by Section 65B. Section 65B, in turn, laid down conditions under which a computer output (such as a printout, copy, or storage in optical/magnetic media) would be deemed a "document" and admissible as evidence without further proof of the original[3].

The rationale behind this special treatment lies in the unique risks posed by electronic evidence. First, volatility data stored in Random Access Memory (RAM), temporary files, or cache disappears upon power loss or system shutdown, requiring immediate forensic acquisition. Second, ease of tampering – metadata, timestamps, and content can be manipulated without apparent alteration, making authenticity difficult to verify. Third, intangibility – electronic records cannot be physically produced in court; they are always represented through a readable output, raising questions about what constitutes the "original". Fourth, chain-of-custody

[1] See generally, Information Technology Act, No. 21 of 2000, §§ 65A–65B (amending the Indian Evidence Act)
[2] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 2(1)(d) (defining "document" to include electronic and digital records) (India)
[3] Indian Evidence Act, No. 1 of 1872, §§ 65A, 65B (repealed) (India).

issues – digital evidence passes through multiple hands (seizing officer, forensic analyst, storage server, cloud provider), and any break in the chain may render it inadmissible. These risks distinguish electronic evidence from traditional documentary evidence, where physical possession and visible alterations provide greater assurance of integrity.

CONTEXTUALISING THE BHARATIYA SAKSHYA ADHINIYAM, 2023

The legal landscape underwent a major overhaul when the Bharatiya Sakshya Adhiniyam (BSA), 2023 received presidential assent in December 2023 and came into force on 1 July 2024, replacing the Indian Evidence Act, 1872. The BSA is part of a trilogy of criminal law reforms alongside the Bharatiya Nagarik Suraksha Sanhita (BNSS) and the Bharatiya Nyaya Sanhita (BNS)[4]. For the first time, the BSA explicitly modernises definitions of "document" and "evidence" to include electronic and digital records. Under Section 2(1)(d) , "document" includes electronic and digital records, while Section 2(1)(e) defines "evidence" to include all statements permitted by the court and all documents (including electronic records) produced for inspection. Moreover, Section 61 clarifies that no document shall be rejected solely because it is in electronic form. These provisions signal a legislative intent to fully integrate digital evidence into the mainstream evidentiary framework.

Crucially, the BSA retains a provision akin to the old Section 65B but re-numbered as Section 63. Section 63(1) declares that any computer output (whether on paper, stored in semiconductor memory, or transmitted via communication devices) shall be deemed a document if produced under conditions of regular use, proper operation, and accuracy. Sub-section (4) mandates a certificate identifying the record, describing its production method, and providing device particulars, signed by a person in charge of the computer or storage device. While the BSA expands the scope of electronic records (e.g., expressly including semiconductor media and multiple networked computers), it also perpetuates the certification requirement that was the epicentre of judicial confusion under the old law.

RESEARCH PROBLEM AND QUESTIONS

Despite the BSA's modernising efforts, three intertwined problems continue to afflict the admissibility of electronic evidence in Indian courts. First, for nearly two decades, courts have grappled with whether the certificate under Section 65B(4) (now Section 63(4) of BSA) is mandatory or merely supplementary to other modes of proof.

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

The Supreme Court in *Anvar P.V. v. P.K. Basheer* (2014) held that the certification requirement is a "complete code" and mandatory, overruling the flexible approach in *State (NCT of Delhi) v. Navjot Sandhu* (2005). However, in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020)[5], the Court reaffirmed the mandatory nature but allowed certificates to be produced at a later stage in the "interest of justice". This oscillation has created uncertainty for litigants and trial courts. The BSA's Section 63 reproduces the same structure, begging the question: has the shift to BSA resolved the confusion, or merely re-enacted it?

Second, investigating agencies face severe practical hurdles in complying with the "original" electronic record requirement. Section 63(2) of the BSA, like its predecessor, conditions admissibility on the computer output having been produced from a device that was used regularly and operated properly. Yet, in cybercrime cases involving volatile data (e.g., RAM contents, live network logs) or cloud-based data stored on foreign servers, seizing the "original" storage medium is often impossible. Police officers frequently lack training in forensic imaging, hashing, and chain-of-custody documentation. As a result, crucial electronic evidence is either not collected or is excluded at trial, undermining prosecutions.

Third, a normative debate persists: should the Indian legal system prioritise probative value (flexibility in admitting electronic evidence, leaving weight to the fact-finder) or procedural strictness (retaining rigorous pre-admission safeguards to prevent tampering)? The BSA's new secondary evidence provisions (e.g., Section 59 allowing oral or electronic statements as secondary evidence) suggest a possible shift towards flexibility. However, the rise of deepfakes, AI-generated content, and sophisticated tampering techniques argues for retaining strong authentication requirements. This paper examines whether the BSA tilts the balance and, if so, whether that tilt is justified.

Accordingly, this research addresses the following three questions:

1. To what extent has the shift from IEA, 1872 to BSA, 2023 resolved the long-standing judicial confusion regarding the mandatory vs. supplementary nature of Section 65B certification for electronic evidence?
2. What are the primary practical and procedural challenges faced by Indian investigating agencies in complying with the "original" electronic record requirement under Section 63 of the BSA, 2023 (and former Section 65B IEA), particularly in cybercrime cases involving volatile or cloud-based data?

[5] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).

3. In light of the BSA, 2023's new provisions on secondary evidence, is the Indian legal system moving towards a more flexible "probative value over procedural strictness" approach for electronic evidence, or does the potential for tampering justify retaining rigorous pre-admission safeguards?

SCOPE AND LIMITATIONS

The scope is limited to Indian domestic law, specifically the IEA (as applicable before 1 July 2024) and the BSA, 2023. Comparative references are made to UNCITRAL Model Law on Electronic Commerce and selected international standards (e.g., US Federal Rules of Evidence, UK PACE) only for illumination. A key limitation is the sparse case law under the BSA as of early 2026; hence, much of the analysis concerning the BSA's impact remains doctrinal and prospective.

RESEARCH METHODOLOGY

This study adopts a doctrinal legal research methodology, involving systematic analysis of statutes (IEA, BSA, IT Act), judicial precedents (from *Navjot Sandhu* to *Khotkar* and post-BSA orders), and official reports (e.g., Law Commission reports, NCRB cybercrime data). An analytical approach is used to compare the pre- and post-BSA frameworks. Additionally, qualitative insights are drawn from forensic literature, police training manuals, and documented challenges in cybercrime investigations.

SIGNIFICANCE

With India witnessing an exponential rise in cybercrimes (over 1.4 million cases in 2024, up 40% from 2022), e-governance initiatives generating vast digital records, and courts moving towards paperless hearings, the admissibility of electronic evidence is no longer a niche concern it is central to the fair administration of justice. A clear, workable framework protects both the accused's right to a fair trial and society's interest in punishing digital wrongdoing. This research aims to contribute to that clarity by critically evaluating the BSA's reforms and proposing actionable solutions.

STATUTORY FRAMEWORK: FROM IEA SECTION 65B TO BSA SECTION 63

1. THE IEA REGIME: SECTIONS 65A AND 65B

1.1 Genesis of the Special Provisions

The Information Technology Act, 2000 introduced Sections 65A and 65B into the Indian

Evidence Act, 1872. Section 65A declares that the contents of electronic records may be proved in accordance with the provisions of Section 65B. This provision established that electronic records would be governed by a special code rather than the general secondary evidence rules contained in Sections 63–65 of the IEA[6]. Thus, Sections 65A and 65B together constituted a "complete code" in respect of electronic documents.

1.2 Admissibility of Computer Output under Section 65B

Section 65B(1) provides that notwithstanding anything contained in the Evidence Act, any information contained in an electronic record which is printed on paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be deemed to be a document, if the conditions mentioned in Section 65B(2) are satisfied. Once those conditions are met, such paper or media shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein.

Section 65B(2) sets out four cumulative conditions for admissibility:

- The computer output must have been produced by a computer that was used regularly to store or process information for any activity regularly carried on;
- The computer was regularly used by the person having lawful control over it;
- The information was of a kind regularly fed into the computer in the ordinary course of the said activity;
- Throughout the relevant period, the computer was operating properly, or if not, any period of malfunction did not affect the accuracy of the record.

A significant expansion is provided by Section 65B(3): where a computer is used over a period of time for the activities described, whether by one or more computers or by different computers in a network, all such computers shall be treated as a single computer, provided the information was stored or processed by that combination of computers regularly. This provision acknowledged that electronic records often originate from multiple interconnected systems, such as servers, workstations, and cloud infrastructure.

1.3 Mandatory Certificate under Section 65B(4)

Section 65B(4) requires a certificate to be produced at the time of adducing electronic evidence. The certificate must:

- Identify the electronic record containing the statement;

[6] Indian Evidence Act, No. 1 of 1872, § 65B(1) (repealed) (India).

- Describe the manner in which it was produced;
- Give particulars of the device involved in the production;
- Deal with all relevant conditions in Section 65B(2).

The certificate must be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities.

The Supreme Court in *Anvar P.V. v. P.K. Basheer* (2014) held that this certificate is mandatory and a condition precedent to admissibility of electronic records. It further ruled that oral evidence cannot substitute for the certificate. In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), a three-judge bench reaffirmed that Sections 65A and 65B constitute a "complete code" and that secondary evidence of an electronic record cannot be admitted unless the requirements of Section 65B are satisfied. The certificate requirement was held to be "sine qua non" for admissibility.

1.4 Primary vs. Secondary Characterization of Electronic Records

A critical ambiguity under the IEA pertained to whether electronic evidence could ever constitute primary evidence, thereby bypassing the Section 65B certificate requirement entirely.

Section 62 of the IEA defines primary evidence as the document itself produced for the inspection of the court. In the context of electronic records, a question arose: what constitutes the "original" document? Is it the storage medium (hard disk, server, mobile device) itself, or is it the binary code stored on that medium? The Supreme Court in *Anvar P.V.* distinguished between an original document contained in the computer itself (primary evidence) and the computer output of that original document (secondary evidence). Under this distinction, Section 65B only applies to make secondary electronic evidence admissible. Primary electronic evidence where the original storage device is produced directly before the court would not require a Section 65B certificate.

However, neither judgment contained a detailed discussion of the meaning of secondary electronic evidence. The traditional dichotomy of "original" and "copy" applicable to paper documents cannot be applied *ipso facto* to electronic records, as there is no clear physical demarcation between an original and its copies. This ambiguity persisted throughout the IEA regime and was never fully resolved by judicial interpretation.

2. THE BSA, 2023: MODERNIZING THE FRAMEWORK

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) replaced the IEA with effect from 1 July 2024, introducing several significant changes to the admissibility framework for electronic evidence.

2.1 Broader Definitions: Section 2(d)

Section 2(d) of the BSA expands the definition of "document" to explicitly include **electronic or digital records**. Under this expanded definition, emails, server logs, documents on computers, laptops or smartphones, messages, websites, locational evidence, and voice mail messages stored on digital devices are all treated as documents. This change codifies what courts had already recognised implicitly, placing electronic records on an express statutory footing with traditional paper documents.

2.2 Parity with Physical Documents: Section 61

Section 61 of the BSA represents a foundational shift. It provides:

"Nothing in this Adhiniyam shall apply to deny the admissibility of an electronic or digital record in the evidence on the ground that it is an electronic or digital record and such record shall, subject to section 63, have the same legal effect, validity and enforceability as other document."

This is a "parity clause" that sweeps away the historical bias towards physical documents and places electronic records on an equal legal footing. However, the clause is expressly **subject to Section 63**, meaning that while electronic records are not to be rejected merely for being electronic, they must still comply with the special admissibility conditions of Section 63.

2.3 The Core Provision: Section 63

Section 63 of the BSA replaces and expands upon Section 65B of the IEA. It has five sub-sections and is accompanied by a Schedule that prescribes a draft form of certificate.

Section 63(1) declares that any information in an electronic record which is printed, stored, recorded or copied in optical or magnetic media produced by a computer, or stored in semiconductor memory or any communication device, shall be deemed to be a document if the conditions in Section 63 are satisfied. The BSA thus explicitly expands the scope to include semiconductor memory (e.g., solid-state drives, RAM chips) and communication devices (e.g., smartphones, tablets, network devices), whereas the IEA was limited to optical or magnetic media.

Section 63(2) retains the four conditions from IEA Section 65B(2): the computer must have

been used regularly to store or process information; it must have been used by the person having lawful control; the information must have been regularly fed in the ordinary course; and the computer must have been operating properly (or any malfunction did not affect accuracy).

Section 63(3) expands the treatment of multiple computers/networks as a single computersubstantially similar to Section 65B(3) of the IEA but with clearer language acknowledging various computer configurations, including standalone computers, networks, and intermediaries.

2.4 Certification under Section 63(4): The Dual Certificate System

The most significant change under the BSA pertains to the certificate requirement. Section 63(4) introduces stricter certification requirements[7]. The certificate must:

- Identify the electronic record and describe the manner of its production;
- Give particulars of the device involved in the production of the electronic record;
- Be submitted at the stage of admission of evidence.

Unlike the IEA, where the certificate could be signed by a "person occupying a responsible official position" alone, Section 63(4)(c) requires the certificate to be signed by both the person in charge AND an expert. The BSA defines an expert as a person with necessary expertise who fills in the technical details of the electronic record.

2.5 Secondary Evidence Provisions

Under the IEA, electronic records admitted under Section 65B were treated as secondary evidence, and the general secondary evidence provisions (Sections 63–65 of IEA) were not available Sections 65A and 65B were held to be a "complete code".

Under the BSA, the framework has been reorganised. Section 59 establishes the best evidence rule, requiring documents to be proved by primary evidence. Section 60 lists cases in which secondary evidence may be given. However, Section 62 provides that the contents of electronic records may be proved in accordance with the provisions of Section 63 thereby preserving the special code approach but embedding it within a broader documentary evidence framework.

The BSA's secondary evidence provisions are now more explicitly integrated with electronic evidence. Notably, electronic records stored in semiconductor memory or communication devices are treated as documents from the outset, making it easier to claim that the production

[7] BSA, supra note 2, § 63(4); see also THE SCHEDULE to BSA [Prescribed Certificate Format – Part A (Party) & Part B (Expert)].

of the storage device itself constitutes primary evidence, thereby bypassing the Section 63 certificate requirement (a point of ongoing debate, as discussed below).

Assessing Resolution of the "Mandatory vs. Supplementary" Confusion

The central question posed in the research framework is: has the shift to the BSA resolved the long-standing judicial confusion regarding whether Section 65B certification is mandatory or supplementary?

3.1 WHAT REMAINS UNCHANGED

The BSA retains the "notwithstanding anything contained" clause in Section 63(1), preserving the special code approach. The certificate under Section 63(4) remains required for admissibility of electronic records that are not primary evidence. The Supreme Court's rulings in *Anvar P.V.* (certificate mandatory, oral evidence insufficient) and *Arjun Panditrao Khotkar* (complete code, certificate sine qua non) remain the interpretive bedrock for Section 63, at least until the Supreme Court directly considers the BSA provisions[8].

The requirement that the certificate be submitted at the stage of admission a key point of ambiguity under the IEA has been retained without significant clarification. Questions such as whether the certificate can be produced after the trial commences, whether an appellate court can permit it belatedly, and what constitutes "substantial compliance" remain unresolved.

3.2 Potential Areas of Clarification under the BSA

First, the addition of the expert certificate in Part B of the Schedule may reduce judicial uncertainty by providing a standardised format. Under the IEA, courts frequently struggled with what the certificate should contain and who could sign it. The prescribed bipartite format, combined with the separate requirements for a hash value, offers a more objective and verifiable standard.

Second, the expanded definition of "document" to include electronic/digital records from the outset may reduce the threshold disputes that plagued the IEA regime. Earlier, litigants could argue that a particular electronic record was not a "document" within the meaning of Section 3 of the IEA and therefore Section 65B did not apply. Under Section 2(d) of the BSA, that argument is substantially weakened.

[8] Anvar P.V., (2014) 10 SCC 473; Khotkar, (2020) 7 SCC 1.

Third, Section 61's parity clause explicitly states that electronic records "shall have the same legal effect, validity and enforceability as other document." This may encourage courts to treat electronic evidence on the same footing as paper evidence, potentially reducing the procedural formalism that characterised IEA jurisprudence.

3.3 Persistent Ambiguities

However, several ambiguities remain unresolved.

Primary vs. Secondary Characterisation: The BSA retains the same ambiguity as the IEA regarding when an electronic record constitutes primary evidence (exempting the Section 63 certificate) versus secondary evidence (requiring it). As academic commentary has noted, "what constitutes an 'original' (or primary evidence) as against a 'copy' (or secondary evidence) in the context of electronic evidence deserves more discussion than has been granted." The BSA contains no definition of "primary electronic evidence" or "secondary electronic evidence," leaving courts to apply the traditional paper-based distinction to inherently intangible digital data.

Certificate Production Timing: The BSA does not address whether the certificate under Section 63(4) can be produced after the commencement of trial, or whether it must accompany the electronic record at the time of filing. Under the IEA, this ambiguity led to conflicting rulings. The BSA's silence on this point may perpetuate the same uncertainty.

Expert Qualification: The BSA requires a certificate to be signed by "an expert" but does not define who qualifies as an expert, what credentials they must possess, or how their independence is to be assured. This lack of definition may itself become a source of litigation.

Primary Evidence Bypass: Explanation 5 to Section 63—which classifies electronic records produced "from proper custody" as primary documents has raised concerns among commentators. As one analysis observes, "production of the §63 certificate should be made mandatory even in this case" to prevent the bypass of essential safeguards. The BSA may thus create a loophole whereby parties can avoid the certificate requirement simply by claiming that an electronic record is produced "from proper custody."

5. IMPLICATIONS FOR THE BALANCE BETWEEN PROBATIVE VALUE AND PROCEDURAL SAFEGUARDS

The BSA's enhancements to the certificate framework dual signatures, mandatory hash values, prescribed format can be interpreted as a legislative choice to strengthen procedural safeguards rather than to relax them. The addition of an expert's certificate imposes a higher

evidentiary burden on the party seeking to adduce electronic evidence. The mandatory hash value requires technical sophistication that many litigants and even some legal practitioners may lack.

At the same time, Section 61's parity clause and the expanded definition of "document" suggest a legislative intent to integrate electronic evidence fully into the mainstream evidentiary framework, reducing the threshold for admissibility in cases where the certificate requirements are met. The overall effect is a balanced approach: electronic evidence is not to be rejected merely for being electronic (probative value), but it must satisfy enhanced authentication requirements (procedural safeguards).

Whether this balance is sustainable in practice particularly in cybercrime cases involving volatile or cloud-based data where seizing the original storage device is impossible and obtaining expert certification may be infeasible is a question addressed in the subsequent sections of this paper.

JUDICIAL INTERPRETATIONS AND RESOLUTION OF CONFUSION

PRE-ANVAR FLEXIBILITY: THE ERA OF JUDICIAL LENIENCY

The interpretive journey of Section 65B began with State (NCT of Delhi) v. Navjot Sandhu (2005)[9], a case arising from the Parliament attack. The Supreme Court considered the admissibility of phone call transcripts obtained from mobile service providers. The evidence was crucial it established the link between the slain terrorist and the architects of the attack. However, the prosecution had not produced a certificate under Section 65B(4).

The Court held that "irrespective of the compliance with the requirements of Section 65-B, which is a provision dealing with admissibility of electronic records, there is no bar to adducing secondary evidence under the other provisions of the Evidence Act, namely, Sections 63 and 65." In other words, electronic records could be proved through general secondary evidence provisions oral testimony of witnesses, production of the original storage device, or other means without necessarily complying with Section 65B's certification requirement. The Court overlooked the non obstante clause in Section 65B, which overrides other sections when the evidence is digital, thereby bypassing the special procedure laid down by Sections 65A and 65B entirely[10].

The *Navjot Sandhu* approach effectively rendered the certification requirement optional. As

[9] state (N.C.T. of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600 (India).
[10] Anvar P.V., (2014) 10 SCC 473.

one commentary observed, the "main legislative idea behind the enactment of section 65B has been vanquished by the Court of Law." This flexibility, while pragmatic, undermined the Parliamentary intent to create a dedicated framework for digital evidence authentication[11].

ANVAR PIVOT: THE COMPLETE CODE DOCTRINE

Almost a decade later, a three-judge bench in Anvar P.V. v. P.K. Basheer (2014) decisively overruled *Navjot Sandhu* to the extent of its statement of law on admissibility of secondary evidence pertaining to electronic records. The Court held that Sections 65A and 65B are special provisions relating to electronic records and constitute a complete code in themselves. Since special law prevails over general law, Sections 63 and 65 of the Evidence Act have no application in the case of secondary evidence by way of electronic record; the same is wholly governed by Sections 65A and 65B.

The Supreme Court ruled that a computer-generated document would be admissible only when accompanied by a certificate under Section 65B, and in its absence, it would be inadmissible. The certificate was declared mandatory and a condition precedent to admissibility. The Court further differentiated between primary and secondary evidence: where the original computer or storage device itself is produced before the court, that constitutes primary evidence and does not require a Section 65B certificate. However, any printed, stored, or copied output from that device is secondary evidence and must comply with Section 65B.

The impact was immediate and severe. Election petitions failed, criminal trials collapsed, and prosecutions were derailed because crucial electronic evidence CCTV footage, call data records, WhatsApp chats was excluded for want of a certificate. The once-flexible approach was replaced with strict procedural formalism, leading to widespread criticism from prosecution agencies and defense practitioners alike.

JUDICIAL BACKLASH AND THE SHAFHI DEVIATION

Despite *Anvar* being a three-judge bench decision, subsequent benches diluted its mandate. In Tomaso Bruno v. State of Uttar Pradesh (2015) , a bench without referring to *Anvar* followed *Navjot Sandhu* and held that secondary evidence of the contents of a document could be led under Section 65 of the Evidence Act.

More significantly, in Shafhi Mohammad v. State of Himachal Pradesh (2018) , a two-judge bench held that the requirement of a certificate under Section 65B(4) is procedural and can be

[11] Khotkar, (2020) 7 SCC 1.

relaxed by the court in the interest of justice, particularly where a party is not in possession of the device from which the document is produced. The Court reasoned that it could not be the law that even where a certificate is impossible to obtain, its absence should result in denial of crucial evidence pointing to the truth. This judgment reintroduced precisely the flexibility that *Anvar* had eliminated, creating a direct conflict between two Supreme Court benches.

CONSOLIDATION IN KHOTKAR (2020): RESOLVING THE CONFLICT

The conflict between *Anvar* and *Shafhi* was referred to a three-judge bench, and in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) , the Supreme Court settled the controversy. The Court held unequivocally that the certificate required under Section 65B(4) is a condition precedent to the admissibility of evidence by way of electronic record, thereby upholding *Anvar* and overruling *Shafhi Mohammad*.

The Court made several critical clarifications.[12] First, it declared that oral evidence cannot substitute for the certificate any other ruling would render the provision otiose. Second, it overruled *Tomaso Bruno* as per incuriam (decided without regard to binding precedent). Third, Sections 65A and 65B were held to be clarificatory and procedural in nature, but still mandatory in application.

Crucially, the Court addressed the timing of certificate production a persistent ambiguity under Section 65B. While the Court reaffirmed that the certificate must be produced at the time of adducing evidence, it held that the requisite certificate need not necessarily be given at the very first instance; it could be produced at a subsequent stage of the proceedings, particularly in cases where it is not forthcoming due to no fault of the party who tried to obtain it. This represented a measured relaxation of the strict *Anvar* position—the certificate remained mandatory, but the Court showed willingness to permit late production where the party was genuinely unable to obtain it earlier.

State of Karnataka v. M.R. Hiremath (2019) , decided just before *Khotkar*, provided additional guidance on the stage of certificate production. The Supreme Court held that failure to produce a Section 65B certificate at the stage when a charge sheet is filed is not fatal to the prosecution. The need for production of such a certificate arises when the electronic record is sought to be produced in evidence at the trial; it is only at that stage that the necessity of production arises. This distinction between the investigation/charge sheet stage and the trial

[12] Nat'l Crime Records Bureau, Crime in India 2023 (2025) (noting cybercrime cases at 86,420 with conviction challenges) (India).

stage allows prosecutions to proceed even if the certificate is not available early, so long as it is produced when the evidence is actually tendered.

POST-BSA TRAJECTORY: EMERGING JURISPRUDENCE

With the Bharatiya Sakshya Adhiniyam, 2023 coming into force on 1 July 2024, courts have begun applying its provisions. Early cases reveal both continuity and emerging challenges.

In a significant post-BSA judgment, a Rajasthan court convicted an accused for theft in December 2025, relying on audio-video recordings of seizure and recovery conducted through the e-Sakshay application, accompanied by certificates under Section 63(4)(c) of the BSA. The Court observed that the electronic evidence, including verified hash values, location data, and in-court playback of recordings, ensured authenticity and ruled out allegations of tampering.

However, the transition has not been seamless. In a Delhi riots case (September 2024), the court noted that despite the repeal of the Indian Evidence Act, certificates for validating the authenticity of digital evidence were still being submitted under the now-defunct Section 65B of the 1872 Act. When certificates under Section 63 of the BSA were later produced, they were found to be incorrect because they did not conform to the prescribed format outlined in the Adhiniyam's Schedule, particularly lacking the mandatory hash value and the second signature from an expert.

The Kerala High Court (March 2025) reinforced the mandatory nature of certification under the pre-BSA framework for cases pending transition, holding that an expert's report under Section 293 CrPC cannot be considered a substitute for a certificate under Section 65B of the Evidence Act. The Court set aside a conviction in a rape and murder case because the prosecution relied on a DVD containing CCTV footage without the requisite certificate, observing: "We are at a loss to understand why the prosecution and the Trial Court had forgone the primary evidence available and have made attempts to rely upon secondary evidence and that too, without proper certification."

The BSA's enhanced certification requirements dual signatures (responsible person + expert), mandatory hash value, and prescribed format pose significant practical hurdles. A key challenge identified is the absence of a clear definition regarding who qualifies as an "expert" capable of validating the authenticity of electronic evidence. Until this ambiguity is resolved, certificate compliance remains uncertain and litigation over the sufficiency of certificates is likely to increase.

EMERGING AI AND DEEPFAKE CHALLENGES

Beyond the BSA's framework, courts are confronting the next frontier: AI-generated and synthetic content. The rise of deepfakes and other synthetically generated content has led Indian courts to increasingly grapple with such evidence.

In a seminal judgment (July 2025), the Supreme Court in State of Maharashtra v. Arjun Sharma established a stringent 'twin-test' for the admissibility of evidence generated by Artificial Intelligence. The framework mandates that AI-generated evidence must satisfy two distinct prongs: authenticity (establishing an unbroken chain of custody for both the data fed into the AI system and the system itself) and reliability (opening the "black box" of the AI system to demonstrate the scientific and technical soundness of the underlying model, including its architecture, training data, bias mitigation methods, and error rates).

The BSA, while modernising procedure, is not synthetically aware it does not distinguish between authentic capture and AI-generated manipulation. This gap is likely to generate future disputes over whether the Section 63 certificate alone suffices for AI-generated content or whether additional safeguards akin to the Arjun Sharma twin-test are required.

The BSA's Section 63 retains the "notwithstanding anything contained" clause and the requirement of a certificate. The Supreme Court's rulings in *Anvar* and *Khotkar* certificate mandatory[13], complete code, oral evidence insufficient remain the interpretive bedrock. The BSA does not alter these substantive conclusions.

However, the BSA provides statutory clarification and modernization in three respects. First, Section 61 establishes parity between electronic and physical documents, sweeping away the historical bias towards paper. Second, the prescribed Schedule format for the certificate, with mandatory hash value and classification into Part A (party) and Part B (expert), offers an objective, verifiable standard that may reduce disputes over what the certificate should contain. Third, the expanded definition of "document" under Section 2(d) to explicitly include electronic/digital records from the outset weakens threshold arguments about whether a particular electronic item constitutes a "document" at all.

Nevertheless, confusion has not been fully eradicated. The BSA retains the same ambiguity regarding primary vs. secondary characterisation of electronic records when does production of the original device exempt the certificate requirement? The BSA contains no definition of "primary electronic evidence" or "secondary electronic evidence," leaving the paper-based distinction to be applied to inherently intangible digital data. The requirement that the

[13] State of Maharashtra v. Arjun Sharma, 2025 SCC OnLine SC

certificate be signed by "an expert" without defining who qualifies as an expert may itself become a significant source of litigation. The BSA does not resolve when the certificate must be submitted—whether it can be produced after trial commences, whether appellate courts can permit it belatedly, and what constitutes "substantial compliance."

Moreover, Section 170(2) of the BSA provides that pending proceedings shall continue under the old IEA, meaning the *Anvar*/*Khotkar* jurisprudence will continue to govern electronic evidence in cases filed before 1 July 2024 for years to come. This creates a dual regime—strict IEA standards for pre-BSA cases, and potentially different interpretations for post-BSA cases. While judicial consistency has improved post-*Anvar*/*Khotkar*, practical application varies across trial courts and high courts. The definitive resolution of these persistent ambiguities awaits Supreme Court pronouncements directly interpreting Section 63 of the BSA, particularly with respect to the primary/secondary distinction, the precise contours of the expert's role, and the circumstances if any under which the certificate requirement may be deemed satisfied despite formal non-compliance.

Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, which replaced and largely mirrors Section 65B of the Indian Evidence Act, 1872, governs the admissibility of electronic records in Indian courts. It provides that computer outputs—whether printed, stored, recorded, or copied in optical, magnetic, semiconductor memory, or any electronic form produced by a computer or communication device—are deemed documents and admissible without further proof of the original, provided specific conditions are met. These include the accuracy and regularity of the system's operation and, crucially under sub-section (4), a certificate identifying the electronic record, describing the manner of its production, detailing the device or process involved, and affirming that it accurately reproduces the original information.

While the BSA modernizes the framework by explicitly encompassing semiconductor memory and communication devices, and by introducing a prescribed certificate format in its Schedule, the core requirement of demonstrating the integrity and authenticity of the "original" electronic record persists. Courts continue to treat many digital outputs as secondary evidence requiring strict certification, with an exception when the actual original device (e.g., the mobile phone, hard disk, or server) is produced before the court, potentially dispensing with the certificate in some interpretations. However, producing the "original" device or storage medium in its pristine form remains highly problematic in practice, especially in cybercrime investigations involving volatile data, remote cloud storage, or rapidly mutable digital footprints.

THE "ORIGINAL" ELECTRONIC RECORD DILEMMA: DEVICE PRODUCTION VS. COPIES AND EXTRACTS

A fundamental challenge arises from the conceptual and practical distinction between primary and secondary electronic evidence. The "original" electronic record is often understood as the data residing on the native device or storage medium (hard disk, SSD, mobile phone internal memory, or server). Investigators are frequently required to seize and produce the actual device to establish it as primary evidence, thereby avoiding or minimizing certification hurdles. Yet, seizing and presenting physical devices in court is fraught with difficulties.

In cybercrime cases, suspects often use multiple devices, encrypted storage, or remote servers. Physical production risks data alteration if not handled with forensic precision. Best practices mandate the use of write-blockers to prevent any write operations during imaging, creation of bit-for-bit forensic images (clones) of the storage media, and verification through cryptographic hash values (e.g., MD5, SHA-256). A matching hash between the original seizure and the working copy mathematically proves non-tampering. However, many state-level police stations and even some district forensic units lack adequate write-blockers, hardware duplicators, or validated forensic toolkits (such as EnCase, FTK, or open-source alternatives like Autopsy).

Producing the actual device in court also raises logistical issues: devices may be needed for ongoing investigations, could be damaged during transit/storage, or might contain mixed personal and evidentiary data, triggering privacy concerns under the Digital Personal Data Protection Act, 2023. When only copies or extracts (e.g., screenshots, exported chat logs, or PDF prints) are submitted, they are treated as secondary evidence, triggering mandatory Section 63(4) certification. Failure to provide a complete certificate detailing the device particulars, production method, and integrity safeguards—leads to frequent judicial rejection.

Common rejection grounds include incomplete technical specifications, unqualified signatories, or gaps in the chain of custody. Investigating officers (IOs) often struggle to articulate complex forensic processes in the certificate, such as the use of Cellebrite UFED or Magnet AXIOM for mobile extraction.

VOLATILE DATA: THE EPHEMERAL NATURE OF EVIDENCE

Volatile data information stored in Random Access Memory (RAM), running processes, temporary files, network logs, or open browser sessions—disappears upon shutdown, power loss, or system reboot. In cases involving malware, live hacking sessions, or real-time communication (e.g., instant messaging in fraud or extortion cases), this data is often the most

probative. Live acquisition requires specialized tools and immediate action at the scene, yet first responders (often uniformed police) frequently power off devices or mishandle them, overwriting critical volatile memory.

The "order of volatility" principle in digital forensics dictates capturing RAM dumps before imaging persistent storage. However, legal authority for such invasive live acquisition under the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, remains procedurally ambiguous in urgent scenarios. While Section 185 BNSS allows warrantless searches in emergencies where evidence may be destroyed, and Section 105 mandates audio-video recording of search and seizure proceedings (preferably via mobile phone, forwarded promptly to the Magistrate), these provisions do not explicitly address live forensic acquisition techniques. Without clear Standard Operating Procedures (SOPs) or judicial guidelines, IOs risk challenges to the legality of acquisition methods during trial.

Preservation is further complicated by the short retention periods of many logs and the technical expertise required to parse them without introducing artifacts.

CLOUD-BASED DATA: JURISDICTIONAL, TECHNICAL, AND TEMPORAL BARRIERS

The proliferation of cloud storage (Google Drive, AWS, Microsoft Azure, Telegram Cloud, etc.) has exponentially increased challenges. Data is often stored on foreign servers, raising sovereignty and jurisdictional conflicts. Indian agencies must typically rely on Mutual Legal Assistance Treaties (MLATs) for content data, a process notorious for delays—often spanning 10 months to over three years. Metadata (e.g., login timestamps, IP addresses) may sometimes be obtained more readily through direct requests to providers or under Section 91 BNSS/Section 69 IT Act, but content access (emails, stored files, chat histories) requires formal international cooperation.

Provider cooperation varies; some platforms delete data upon user request or after inactivity, while encryption (end-to-end in WhatsApp, Signal) renders even obtained data unreadable without decryption keys. Chain-of-custody becomes multi-jurisdictional and difficult to document comprehensively for a Section 63 certificate. Investigators must prove that the downloaded or exported cloud data accurately reflects the original without alteration, often relying on provider-generated logs whose authenticity is hard to verify independently.

In ransomware or phishing cases hosted on overseas bulletproof hosting services, timely preservation requests via MLAT frequently arrive too late. Cross-border encryption and multi-tenancy in cloud environments further complicate forensic imaging.

CYBERCRIME-SPECIFIC

In phishing and online fraud cases (which dominate NCRB statistics), evidence often consists of rapidly deleted emails, fake websites hosted on short-lived domains, or chat logs on platforms that purge data. Suspects may remotely wipe devices upon detection.

Hacking and ransomware frequently involve volatile malware artifacts in RAM and encrypted command-and-control communications stored abroad.

Social media evidence in defamation, extortion, or fake news cases suffers from platform deletions, account suspensions, or API limitations. Screenshots without proper forensic capture and certification are routinely challenged.

In all these, the speed of digital alteration contrasts sharply with the slow pace of investigation and MLAT processes.

NORMATIVE ANALYSIS: PROBATIVE VALUE VS. PROCEDURAL STRICTNESS UNDER BSA

The Bharatiya Sakshya Adhiniyam, 2023, marks a significant legislative attempt to modernize India's evidentiary framework for the digital age. Yet beneath its veneer of reform lies a fundamental normative question: does the BSA tilt toward flexibility valuing probative substance over procedural form or does it double down on pre-admission safeguards in response to mounting fears of digital tampering? The answer is more nuanced than a simple binary choice.

Superficial Flexibility, Substantive Continuity

At first glance, the BSA appears to embrace flexibility. Section 61 introduces a "parity clause," declaring that electronic records shall have the same legal effect, validity, and enforceability as paper records. Section 57 now explicitly recognizes electronic and digital records as "primary evidence" in prescribed form. Section 62 permits the use of electronic record content as evidence, provided the conditions under Section 63 are met. These provisions sweep away the historical bias against digital documents, signaling legislative intent to integrate electronic evidence into the mainstream.

However, this apparent flexibility is illusory when examined against the BSA's certification regime. Section 63(4) imposes requirements that are **substantially more rigorous** than its predecessor. The certificate must now be signed by both the person in charge of the device **and** "an expert," with the certificate following a prescribed format that includes a mandatory hash value. The Supreme Court's consistent jurisprudence—most recently

reaffirmed in *Kum. Shubha v. State of Karnataka* (July 2025) holds that Sections 62 and 63 of the BSA (formerly Sections 65A and 65B) constitute a "complete code," leaving no scope for other provisions to circumvent the certification requirement. The BSA thus represents continuity rather than departure: procedural strictness remains the governing principle.

The Counter-Argument: Heightened Tampering Risks Demand Rigor

The case for retaining and even strengthening procedural safeguards has never been stronger. The proliferation of deepfakes, AI-generated content, and sophisticated manipulation techniques poses an unprecedented threat to evidentiary integrity. A deepfake video is still an "electronic record" under the BSA's technology-neutral text, but the authenticity burden is significantly heavier. The BSA's framework, however, falls short of introducing any significant changes to address the admissibility and authenticity of e-evidence despite repeated judicial remarks over the issue of growing deepfake misuse.

The Supreme Court has responded to this lacuna in *State of Maharashtra v. Arjun Sharma*

These judicial interventions underscore that the BSA's existing framework designed for conventional computer outputs is inadequate for generative AI. As one commentator observes, the BSA's certificate regime "remains a straitjacket for dynamic AI outputs," ill-equipped to handle evidence that emerges from opaque algorithms rather than fixed storage media.

Comparative Insights: Avoiding Both Formalism and Over-Flexibility

Jurisdictional comparisons reveal that India's approach occupies a distinctive middle ground. The United States Federal Rules of Evidence, particularly Rule 902, permit self-authentication for certain electronic records without live testimony, while Rule 901(b)(9) allows authentication through evidence describing a process or system that produces an accurate result. This "process-based" approach emphasizes reliability over formal certification. The UK's Police and Criminal Evidence Act (PACE) similarly adopts a flexible framework, allowing courts to admit computer evidence upon proof of proper operation without rigid certification mandates.

India's BSA, by contrast, retains the strict certification requirement while simultaneously expanding primary evidence recognition for native digital records. This hybrid model flexibility in classification (primary vs. secondary) but rigidity in certification creates a paradoxical landscape: parties may avoid the certificate only by producing the original storage device, a practical impossibility in many cybercrime contexts involving cloud or volatile data.

Balanced Modernization, Not Radical Flexibility

The BSA leans toward balanced modernization rather than radical flexibility. It retains rigorous pre-admission safeguards dual certification, hash values, prescribed formats while extending parity to electronic records and permitting certain primary evidence exceptions. The normative arc is not toward "probative value over procedural strictness" but toward structured reliability. The Supreme Court's twin-test for AI-generated evidence signals a further tightening: the BSA's framework, designed for static computer outputs, is being proactively supplemented by judicial standards to address emergent technologies.

Retaining safeguards is justified given the unprecedented tampering risks of the AI era. Yet excessive strictness, coupled with infrastructure deficits, burdens investigating agencies and delays justice. The BSA provides the statutory architecture; its success depends on institutional reforms training, expert capacity, and judicial guidance that transform procedural rigor from a barrier into an assurance of reliability.

Legislative and Rule-Making Reforms

First, the Ministry of Law and Justice, in consultation with the Ministry of Electronics and Information Technology (MeitY), should issue detailed rules under Section 63 of the BSA specifying the qualifications and accreditation process for “experts” authorised to sign the electronic evidence certificate. Currently, the BSA refers to “an expert” without defining the term, creating uncertainty and potential litigation. A clear framework requiring certification by the National Accreditation Board for Testing and Calibration Laboratories (NABL) or empanelment by the Central Forensic Science Laboratory (CFSL) would resolve this ambiguity.

Second, the government should prescribe standard operating procedures (SOPs) for handling volatile and cloud-based data. These SOPs must address live forensic acquisition of RAM contents, network logs, and temporary files, specifying when and how investigating officers may seize such data without a warrant in exigent circumstances under the BNSS, 2023. For cloud evidence, the SOPs should establish a fast-track mechanism for service providers to respond to Indian judicial orders, modeled on the Mutual Legal Assistance Treaty (MLAT) but streamlined through an online portal akin to the “Sahyog” platform already used for banking fraud cases.

Third, legislative amendments should facilitate cross-border cooperation by empowering Indian courts to issue production orders directly to foreign-based intermediaries that have a business presence in India, under Section 79 of the IT Act, 2000 (as amended). The absence of

such provisions forces agencies to rely on slow MLAT channels, rendering most cloud evidence practically unobtainable. A proposed amendment could require intermediaries operating in India to designate a local point of contact for evidence production, with penal consequences for non-compliance.

Institutional Capacity Building

The shortage of trained forensic experts and inadequate laboratory infrastructure constitute the most binding constraint on effective electronic evidence handling. The government should allocate dedicated funds under the Cyber Crime Prevention against Women and Children (CCPWC) scheme and the Indian Cyber Crime Coordination Centre (I4C) to establish at least one fully equipped digital forensic laboratory in every district court complex. Currently, such labs exist only in major cities, resulting in evidence degradation during transit and months-long backlogs.

Simultaneously, the Bureau of Police Research and Development (BPR&D) should mandate compulsory digital evidence training for all investigating officers, with periodic refresher courses. Training must cover proper seizure techniques (write-blockers, hash value generation, chain-of-custody documentation), use of the e-Sakshya mobile app for tamper-proof evidence collection, and the legal requirements of Section 63 certification. Similar training modules should be integrated into the curriculum of judicial academies for magistrates and sessions judges, who currently lack the technical literacy to assess electronic evidence admissibility.

The National Forensic Science University (NFSU) should be tasked with scaling up the production of qualified forensic examiners. A target of at least 500 examiners per state, with specialized training in volatile data extraction and cloud forensics, is necessary to meet the demand created by the BSA's dual-certification requirement.

Technological Adoption

India should pilot blockchain-based evidence management systems for critical electronic records. A permissioned blockchain, accessible to courts, investigating agencies, and forensic labs, can provide an immutable timestamp and hash log of every electronic document from seizure to production. This would drastically reduce chain-of-custody disputes and automate much of the certification process. The e-Sakshya platform already incorporates basic hashing; extending it to distributed ledger technology is a logical next step.

For detecting deepfakes and AI-generated manipulations, the Centre for Development of

Advanced Computing (C-DAC) should develop and certify forensic tools that can be deployed across state forensic labs. These tools must be capable of generating a "probability of authenticity" score, which courts can use as part of the *Arjun Sharma* twin-test. However, caution is warranted: over-reliance on automated detection tools without judicial oversight risks substituting algorithmic determinations for reasoned adjudication.

CONCLUSION

Investigating agencies face profound practical and procedural challenges in complying with the "original" electronic record requirement under Section 63. Volatile data disappears upon shutdown; cloud-based evidence resides on foreign servers accessible only through slow MLAT processes; and agency-level deficits lack of trained forensic examiners, inadequate laboratory infrastructure, and inconsistent certificate documentation routinely lead to evidence exclusion. The National Crime Records Bureau's cybercrime conviction rate (around 22%) starkly illustrates these failures. While the BNSS introduces electronic trial provisions, they address court procedures, not investigative realities.

The BSA does not move toward a "probative value over procedural strictness" approach. Instead, it balances flexibility with safeguards by expanding primary evidence recognition and parity for electronic records while simultaneously strengthening pre-admission requirements. The normative architecture remains one of *structured reliability*: electronic evidence is not rejected merely for being digital (Section 61), but must undergo rigorous certification, hash verification, and expert scrutiny. In the AI era of deepfakes and generative content, such safeguards are justified. However, excessive strictness without corresponding institutional capacity delays justice a problem the BSA alone cannot solve. The BSA represents genuine progress in modernising India's evidentiary framework for the digital age. It resolves some ambiguities, expands coverage to semiconductor memory and communication devices, and introduces verifiable technical standards. Yet it leaves interpretive space on critical definitions and practical challenges in agency implementation. The system achieves a reasonable balance between evidentiary integrity and utility, but its effectiveness depends on supportive ecosystem reforms: legislative rules on expert qualifications, institutional investment in forensic labs and training, judicial guidance on substantial compliance, and technological adoption of tamper-proof evidence logs. The admissibility of electronic evidence is no longer a niche procedural concern it is central to fair trials, effective cybercrime prosecution, and India's broader digital justice goals. As the nation moves toward paperless courts, e-governance, and digital

governance, the reliability of electronic evidence determines whether the guilty are convicted and the innocent are acquitted. The BSA provides the statutory foundation; building upon it with robust institutions, trained personnel, and adaptive jurisprudence will determine whether India's legal system remains credible in an increasingly digital world.