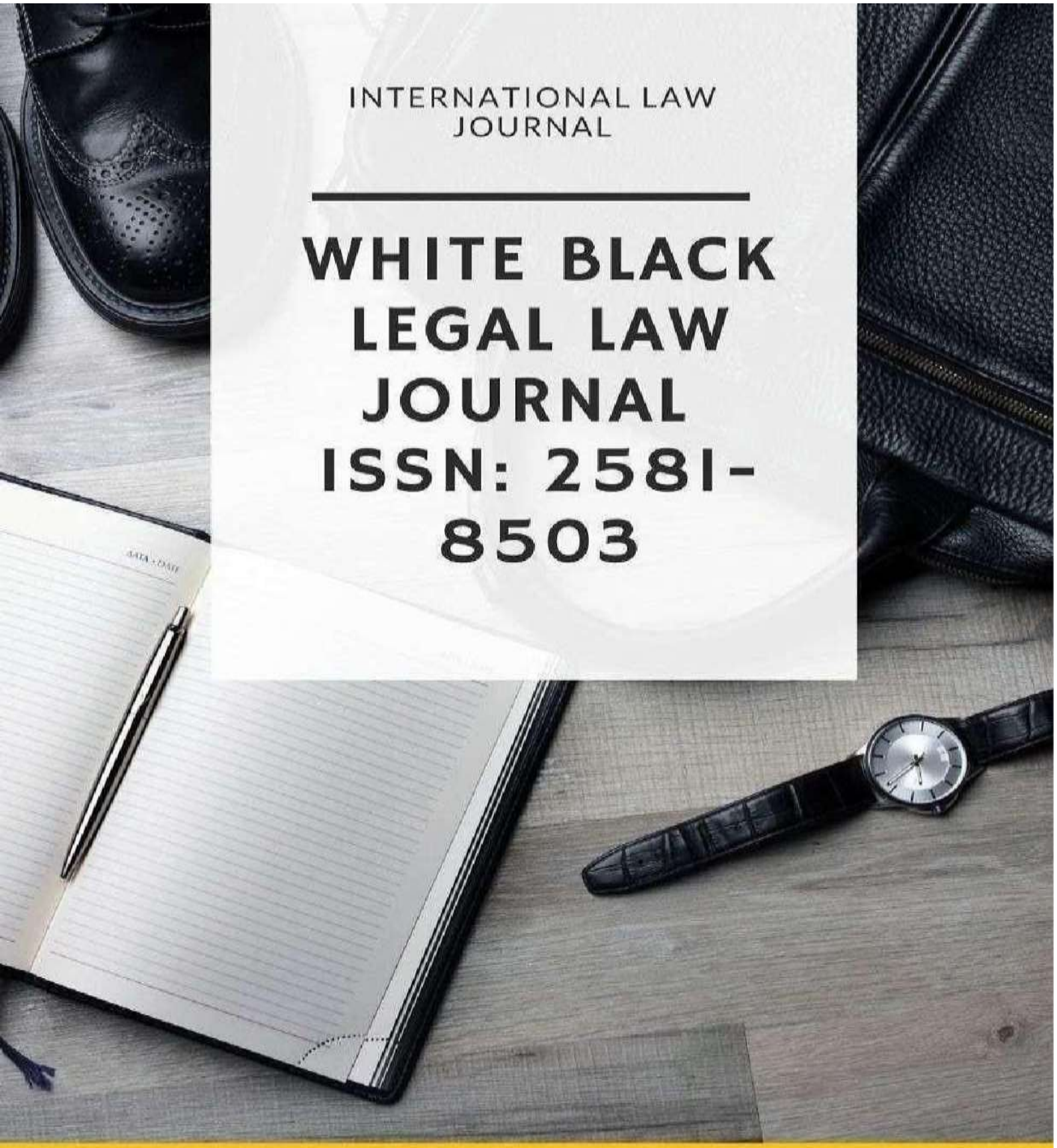

INTERNATIONAL LAW JOURNAL

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.

ELECTRONIC EVIDENCE UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023: MODERNISATION OR A PANDORA'S BOX OF ADMISSIBILITY?

AUTHORED BY – SWATI JOSHI
RESEARCH SCHOLAR
DEPARTMENT OF LAW, JNV UNIVERSITY, JODHPUR (RAJ.)

ABSTRACT

The Bharatiya Sakshya Adhiniyam, 2023 (hereinafter, BSA) is one of the three statutes replacing India's colonial-era criminal laws. It was enforced on **1** July 2024, representing the most ambitious legislative intervention in the law of evidence since the Indian Evidence Act, 1872 (hereinafter, IEA). One of the most contested changes brought by BSA, 2023, is that it reframes electronic and digital records as primary evidence under Sections 57 and 61. Hence, collapsing the longstanding distinction between primary and secondary evidence.

BSA, 2023, replaces the certificate required under Section 65B of the Indian Evidence Act, 1872, with a dual-signatory regime under Section 63(4), now requiring attestation by both the person in charge of the relevant device and a forensic expert. This shall be supplemented by a mandatory schedule format and hash verification. These changes are not merely cosmetic, but they alter the procedural architecture of digital proof and reshape the obligations of parties, practitioners, and courts.

However, these modifications brought by the BSA, 2023, are shadowed by significant uncertainty as the statute does not define who qualifies as an 'expert' for the purposes of submitting a certificate under Section 63. Further, the statute is silent on the admissibility of AI-generated evidence, metadata, cloud-stored data, and encrypted records. It provides no chain-of-custody standards, forensic protocol for digital investigation, and an institutional framework for the forensic science laboratories.

This paper critically examines the provisions of electronic evidence under BSA, 2023, against the backdrop of the Supreme Court's evolving jurisprudence as reflected in the landmark judgments. Drawing on comparative materials from the United Kingdom, Singapore, and the United States, the paper argues that the BSA is a reform that is structurally sound in its broad design but procedurally incomplete in its execution. It concludes with legislative, judicial, and institutional recommendations for translating the BSA's modernising aspiration into

operational reality.

Keywords: *Bharatiya Sakshya Adhiniyam, 2023; Electronic Evidence; Section 63; Section 65B; Digital Records; Certificate of Authenticity; Admissibility*

I. INTRODUCTION

Evidence law is a set of rules that governs how facts are proven in court, determining which kinds of testimony, documents, or evidence are admissible to help a judge reach a decision. For over 150 years, the Indian Evidence Act, 1872, has governed the law of evidence in civil and criminal proceedings. This colonial statute was drafted by Sir James Fitzjames Stephen in an era when the most sophisticated technological artefact in a courtroom might have been a telegraphic message.

The Bharatiya Sakshya Adhiniyam, 2023, was enacted as part of India's comprehensive overhaul of its criminal justice legislation and brought into force on 1 July 2024. It expands the definition of 'document' to expressly include electronic and digital records, grants those records the status of primary evidence, introduces a dual-signatory certificate regime under Section 63, and mandates a standardised schedule format complete with hash verification. While these modifications are noteworthy, it is also important to understand that legislation does not operate in a vacuum. It operates in forensic laboratories with understaffed examiners, in courtrooms where practitioners are still parsing which regime applies to pending proceedings, and in a digital economy producing different forms of evidence such as AI-generated content, cloud-stored data, and encrypted communications.

This paper poses a simple question with a complex answer: *Does the BSA, 2023, genuinely modernise India's evidentiary framework for the digital age, or does it open a Pandora's box of new uncertainties in the area of admissibility of evidence, while leaving the old ones unresolved?*

The paper first traces the evolution of electronic evidence law in India from its origins in the IEA, 1872, and the Information Technology Act, 2000 (hereinafter, IT Act) through the judicial trilogy that culminated in the landmark judgment of *Arjun Panditrao Khotkar*[1]. It then examines the specific provisions of BSA, 2023, and structural departures from the IEA, 1872, and analyses the admissibility and authentication challenges that the new regime generates. Further, a comprehensive study of the case laws on the jurisprudence of electronic evidence,

[1] Arjun Panditrao Khotkar V. Kailash Kushanrao Gorantyal (2020) 7 sec 1.

examining whether the BSA, 2023, resolves or perpetuates the tensions that case law has identified. Lastly, this paper explores a comparative survey of analogous jurisdictions that provide a perspective on the admissibility of electronic evidence and concludes with a set of normative recommendations.

II. THE EVOLUTION OF THE LAW OF ELECTRONIC EVIDENCE IN INDIA

A. The Indian Evidence Act and its digital insufficiency

The IEA, 1872, defined the term 'document' broadly under Section 3 to include*" ...any matter expressed or described upon any substance by means of letters, figures, or marks"*. Courts had, well before the digital age, extended this definition to include film, phonographic records, and photographs.[2] However, the IEA had no conception of a computer-generated record, metadata, server logs, or encrypted communications. When digital technology arrived in Indian courts in the 1990s, the statute offered no structured framework for its reception, and courts improvised with general provisions, producing outcomes that were inconsistent.

Consequently, the Indian Parliament inserted Sections 65A and 65B into the IEA by the IT Act, 2000. Section 65A provided that the contents of electronic records could be proved in accordance with Section 65B. Section 65B(l) created a deeming provision stating that any computer output, whether printed on paper or stored in optical or magnetic media, was *'deemed to be a document'* admissible in evidence without further proof, provided the conditions in Section 658(2) were satisfied. Those conditions required that the computer producing the record was used regularly to store or process information in the lawful course of the relevant activity, the information was regularly fed into it, the computer was operating properly during the material period, and the record was a faithful reproduction of what was fed into it.[3] A certificate from a person in a responsible official position, attesting to these conditions, was required under Section 65B(4).[4]

B. The Judicial Trilogy: From the case of Navjot Sandhu to Arjun Panditrao

The first major judicial engagement with Section 65B, IEA was *State (NCT of Delhi) v. Navjot*

[2] The definition of 'document' under s 3 of the Indian Evidence Act, 1872 (IEA) was held to include maps, plans, and drawings: R v Daye [1908] 2 KB 333. See generally Ratanlal & Dhirajlal, The Law of Evidence (25th edn, LexisNexis 2019) 20-21.
[3] IEA, s 65B(2), inserted by the Information Technology Act, 2000, s 92 and Second Schedule.
[4] IEA, s 65B(4).

Sandhu (2005),[5] also known as the Parliament Attack Case. The Supreme Court held that electronic records could be admitted as secondary evidence even without strict compliance with Section 65B, provided oral evidence was given to prove the relevant facts. This permissive interpretation produced a decade of inconsistent practice: some courts insisted on the certificate, others dispensed with it upon oral testimony, and practitioners were left with no reliable guide to admissibility.

The Supreme Court corrected course in the case of *Anvar PV v. PK. Basheer* (2014),[6] a three-judge bench decision authored by Justice Kurian Joseph. Applying the maxim *generalia specialibus non derogant,*[7] the Court held that Sections 65A and 65B constituted a complete and exclusive code for the proof of electronic records as secondary evidence. The requirement of a verified certificate under Section 65B(4) of IEA was not optional, but a condition precedent to admissibility. Hence, the case of *Navjot Sandhu* was overruled insofar as it suggested otherwise. The Court did carve one exception - where the original device itself was produced as primary evidence, the certificate was unnecessary.

The apparent clarity of the *Anvar* case was disturbed by a two-judge bench in *Shajhi Mohammad v. State of Himachal Pradesh* (2018),[8] which held that the requirement of the certificate under Section 65B(4) could be relaxed where a party was not in possession of the relevant device. The tension between the decision of a three-judge bench and a two-judge bench purported to qualify it as constitutionally indefensible.

This issue was resolved in the case of *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020),[9] where a three-judge bench reaffirmed the judgment of *Anvar PV* and overruled *Shafhi Mohammad.* The Apex court held that the requirement of the certificate under Section 65B(4) is a 'condition precedent' to admissibility, and the trial court has jurisdiction to summon the person responsible for issuing the certificate if a party fails to produce it. The judgment also declared *Tomaso Bruno v. State of Uttar Pradesh* (20l5)[10] per *incuriam* insofar as it had admitted electronic evidence without a certificate. The trilogy thus concluded with a clear rule that if no verified certificate is produced, the evidence of the electronic record cannot be admitted, except in the case of the production of the original device itself.

[5] State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru (2005) 11 SCC 600.
[6] Anvar P.V. v. **P.K.** Basheer and Others (2014) 10 SCC 473.
[7] It is a Latin legal maxim meaning *"general things do not derogate from special things"*. It states that if a conflict exists between a general provision and a specific provision, the specific provision prevails.
[8] Shafhi Mohammad v. State of Himachal Pradesh (2018) 5 SCC 311.
[9] Supra 2.
[10] Tomaso Bruno v. State ofUttar Pradesh (2015) 7 SCC 178. The two-judge bench had admitted electronic evidence without the Section 65B(4) certificate, holding that the certificate requirement could be dispensed with in the interest of justice. This was declared per incuriam in Arjun Panditrao (n 8).

III. ELECTRONIC EVIDENCE UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

A. The New Definitional Architecture

The BSA, 2023, defines the term 'document' under Section 2(1)(d) to include electronic and digital records, bringing them within the primary framework of the statute. Section 57 defines 'primary evidence' and adds four new explanations - Explanations 4 to 7. These explanations represent a principled legislative choice to dissolve the primary-secondary dichotomy that had generated so much uncertainty under the IEA.

Under the old regime, most electronic records presented m court were treated as secondary evidence; copies of an original stored in a computer or server, requiring a verified certificate under Section 65B. Under the BSA, the same records may, depending on the circumstances of their creation and storage, qualify as primary evidence, potentially eliminating the need for any certificate at all. Further, Section 61 of BSA brings electronic and digital records equivalent to other documents, in terms of legal effect, validity, and enforceability, subject to certain conditions under Section 63.

B. Section 63: The New Certificate Regime

Section 63 of BSA corresponds to Section 65B of the IEA but departs from it in three significant respects. *First,* the certificate now requires dual attestation: it must be signed by both the person in charge of the relevant computer or device and a forensic expert.[11] The addition of the expert certificate introduces a layer of technical accountability that the IEA lacked. *Second,* the BSA mandates compliance with a specific format prescribed in the Schedule appended to the Act. The old Section 65B(4) prescribed conditions, but not a format. *Third,* Section 63(4)(c) requires that the certificate be accompanied by a report of the hash value of the electronic record. Hash verification is a standard tool in digital forensics; it generates a unique fingerprint of a digital file that detects any subsequent alteration.

C. *Legislative intent and structural departure*

The parliamentary intent behind the provisions of BSA relating to electronic evidence can be distilled to three propositions. *First,* electronic records are no longer to be treated as a suspect or inferior category of evidence requiring special justification for admission. *Second,* the

[11] BSA, s 63(4)(c) read with the Schedule to the Adhiniyam. The certificate must be in two parts: Part A completed by the 'person in charge' of the device, and Part B completed by 'an expert' as defined under s 39. The certificate must be accompanied by a report of the hash value of the electronic record.

reliability of electronic evidence is to be ensured through procedural rigour, specifically, dual certification, hash verification, and standardised formats; rather than through blanket exclusion. *Third*, the role of the judiciary in policing admissibility is to be assisted by forensic expertise, institutionalising the mechanism of an examiner of electronic evidence under Section 79A of the IT Act as a central element of the evidentiary regime.

Further, the structural intent of the legislature is apparent if these provisions are read alongside Section 39(2) of the BSA. This provision makes the opinion of an Examiner of Electronic Evidence (as referred to in Section 79A of the IT Act, 2000) a relevant fact when a court has to form an opinion on any matter relating to information transmitted or stored in a computer resource or any other electronic or digital form. Digital evidence is to be assessed through a combination of statutory procedure, forensic expertise, and judicial discretion.

IV. ADMISSIBILITY AND AUTHENTICATION CHALLENGES UNDER THE BSA, 2023

A. The Problem of Expert Certificate

The most immediate challenge created by Section 63(4) is the requirement of an expert certificate. The BSA does not define what qualifies as an 'expert' for this purpose, beyond the reference in Section 39(2) to the Examiner of Electronic Evidence under Section 79A of the IT Act, 2000.[12] Section 79A of the IT Act empowers the central government to notify Examiners of Electronic Evidence, who are recognised as experts under Section 45A of the IEA (and its equivalent under BSA). However, the government's notification of such examiners has been limited and geographically uneven. India's network of Forensic Science Laboratories (FSLs) is severely under-resourced: a 2023 survey by the Bureau of Police Research and Development (BPRD)[13] found significant backlogs in the examination of digital evidence, with average turnaround times far exceeding the timelines envisaged by the new criminal laws. In a criminal trial where the prosecution seeks to produce WhatsApp chats, CCTV footage, call data records, or email correspondence, it must now obtain both a device-controller certificate and a forensic expert certificate in the schedule format, with a hash report appended. For public prosecutors handling high-volume caseloads in sessions courts across the country, this is an aspirational standard, not a realistic one. For a private litigant in a commercial dispute seeking to produce email evidence, the obligation to locate, engage, and pay a qualified

[12] BSA, s 39(2).
[13] Bureau of Police Research and Development (BPRD), 'Data on Police Organisations in India' (BPRD 2023).

forensic expert for a certificate is a significant practical burden. The BSA has raised the evidentiary bar without simultaneously raising the infrastructure to reach it.

B. Chain of custody and integrity of digital records

A certificate, however well-drafted, cannot substitute for a robust chain of custody. Digital evidence is uniquely susceptible to alteration; files can be modified, metadata can be manipulated, logs can be deleted, and even hash values can be falsified if the chain of custody is not scrupulously maintained from the moment of seizure to production in court. The BSA provides no protocol for the seizure of digital devices or a rule governing the documentation of access to digital records between seizure and trial.[14]

This silence is constitutionally significant as the right to a fair trial under Article 21 of the Constitution, as elaborated in *Maneka Gandhi v. Union of India* (1978)[15] and *D.K. Basu v. State of West Bengal* (1997),[16] encompasses the right to challenge evidence on grounds of unreliability. If an accused cannot access information about how digital evidence was collected, stored, and transmitted before trial, the right to meaningful cross-examination gets affected. Further, the hash verification can confinn that a file has not been altered after the point at which the hash was generated, but it cannot reveal what happened before that point.

C. Novel Digital Evidence: AI, Cloud, Metadata, and Encryption

Perhaps the most significant gap in the provisions of electronic evidence under BSA is the silence on categories of digital evidence that are increasingly central to both civil and criminal litigation. *AI-generated evidence*, including the content produced by generative AI systems, such as transcripts, translations, or audio-visual reconstructions, raises questions of authorship, reliability, and attribution that the BSA does not address.

Further, *Cloud-stored data* presents a related challenge. Where evidence is stored not on a physical device in India but on a server operated by a foreign cloud service provider, the person 'in charge' of the device for purposes of Section 63(4)(a) may be outside India's jurisdiction entirely. The BSA lacks a treaty-based mechanism for obtaining electronic evidence from foreign jurisdictions.

[14] See ACPO Good Practice Guide for Digital Evidence (5th edn, Association of Chief Police Officers 2011) (UK), which mandates forensic imaging, write-blocking, and hash verification as minimum standards for the handling of digital evidence from point of seizure.

[15] Maneka Gandhi v. Union oflndia (1978) I SCC 248 (SC). The Supreme Court held that 'procedure established by law' in Art 21 of the Constitution must be right, just and fair, not arbitrary or oppressive.

[16] D.K. Basu v. State of West Bengal (1997) 1 SCC 416 (SC).

The BSA treats electronic records as documents but does not specify whether *metadata* is itself an electronic record entitled to admission or requires a separate certificate. *Encrypted communications* present yet another challenge: a message whose content is accessible only through a decryption key may not be produced in decrypted form without the cooperation of the developer of the originating application, something that BSA does not compel.

V. A COMPARATIVE PERSPECTIVE

A. The United Kingdom: Reliability over procedure

The approach of the United Kingdom to the laws of electronic evidence has evolved significantly since the Police and Criminal Evidence Act, 1984 (PACE) introduced the erstwhile Section 69, which required proof that a computer was operating properly before its output could be admitted. Section 69 was abolished by the Youth Justice and Criminal Evidence Act, 1999, because it had proved unworkable in practice.[17] Virtually no witness could credibly testify to the proper operation of complex computer systems over extended periods. The presumption was reversed; electronic evidence is now presumed reliable, and the burden falls on the party challenging it to demonstrate unreliability.

The UK model, which prioritises judicial assessment of reliability over mandatory pre-admission certification, represents a more flexible and less infrastructure-dependent approach than the dual-certificate approach under BSA. Its principal risk is that judges without technical expertise may underestimate the significance of tampering risks in digital evidence. However, that risk may be better managed through adversarial challenge and judicial education than through mandatory forensic certificates that create access barriers.

B. Singapore: The electronic transactions act and presumptive admissibility

Singapore's approach combines a presumptive admissibility framework with a sophisticated legal infrastructure for electronic evidence. The Electronic Transactions Act, 2010, creates a general presumption that computer output is admissible and accurate, displacing the need for elaborate foundational proof. Challenges to the integrity of electronic evidence are resolved through the court's exercise of its general discretion over evidence, assisted by judicial commissioners who are usually technically literate. Singapore has also invested heavily in

[17] Section 69 of the Police and Criminal Evidence Act, 1984 (UK) was repealed by the Youth Justice and Criminal Evidence Act, 1999, s 60. The Civil Evidence Act, 1995, s 1 makes hearsay statements admissible in civil proceedings. See Law Commission of England and Wales, Report No 216, 'Evidence in Civil Proceedings: Hearsay and Related Topics' (1993).

forensic infrastructure, maintaining accredited forensic laboratories to a standard that Indian FSLs have not yet matched.[18]

C. *United States: Federal rules of evidence and the authentication regime*

Under the Federal Rules of Evidence (FRE), electronic records are authenticated under Rule 901, which mandates the proponent to produce *"evidence sufficient to support a finding that the item is what the proponent claims it is."* Specifically, Rule 901(b)(9) permits authentication of a process or system that produces an accurate result to be shown through *"evidence describing the process or system and showing that it produces an accurate result."* Under the US regime, the requirement of a mandatory certificate is unnecessary as authentication is a question of sufficiency, not formality.[19] The landmark judgment in the case of *Lorraine v. Markel American Insurance Co.* (D. Md. 2007)[20] laid out a comprehensive framework for authenticating electronic records that has been widely cited by federal courts.

The comparative survey reveals two divergent paths for India to consider. The UK-US path trades mandatory certification for flexible judicial assessment of reliability, placing the burden of demonstrating unreliability on the challenging party. The Singapore path combines presumptive admissibility with a strong forensic infrastructure. BSA has chosen neither: it retains mandatory certification (as under the IEA) but adds complexity to the certification process, without simultaneously building the forensic infrastructure or providing the judicial guidance needed to make the system work. The choice between procedural formalism and flexible reliability assessment matters less than the quality of the forensic ecosystem in which the rules operate.

VI. RECOMMENDATIONS

A. Define 'Expert' by regulation and accreditation

Parliament should amend Section 63 of BSA, or MeitY should issue rules under the IT Act, 2000, to define the qualifications required of an expert certifying electronic evidence under Section 63(4)(c). At a minimum, such a person should be a government-notified Examiner of Electronic Evidence under Section 79A of the IT Act or hold an equivalent accreditation from a recognised body. The central government should establish an accreditation framework for

[18] Electronic Transactions Act 2010 (Singapore), Part III. See also Singapore Courts, 'Electronic Evidence Practice Guide' (Supreme Court of Singapore 2022), which provides detailed pforrocedural guidance for the production and authentication of electronic evidence.
[19] Federal Rules of Evidence (US) r. 90l(a), 90l(b)(9).
[20] Lorraine v. Markel American Insurance Co. 241 FRD 534 (D Md 2007), per Grimm MJ.

digital forensic examiners, on the model of the UK's Forensic Science Regulator, and publish a public register of accredited examiners.

B. Enact a digital evidence (seizure and custody) procedure

The BSA should be supplemented by a statutory instrument or a High Court rule specifying chain-of-custody requirements for digital evidence from the point of seizure to production in court. These should include: mandatory forensic imaging of seized devices before examination; write-protection of original devices during examination; documentation of every instance of access to digital records; and a requirement that hash values be recorded at the point of seizure and verified at each subsequent stage.

C. *Legislative guidance on novel digital evidence*

The BSA should be amended, or subsidiary legislation should be enacted, to address three categories of digital evidence that are currently not addressed: *AI-generated content* (requiring disclosure of the AI system, its version, and the parameters of the generation request); *cloud-stored evidence* (requiring a bilateral treaty-compatible mechanism for obtaining authentication certificates from foreign service providers); and *metadata* (to be treated as a component of the electronic record to which it relates, and subject to the same certificate regime).

D. Judicial education and uniform protocols

The National Judicial Academy and State Judicial Academies should design and implement a structured programme of judicial education in digital forensics, specifically covering the interpretation of hash values, metadata, forensic imaging reports, and expert certificates under Section 63. Courts will need to develop a principled resolution; in its absence, different benches are likely to reach different conclusions, reproducing exactly the kind of inconsistency that the BSA was intended to cure.[21]

E. Institutional capacity in forensic science laboratories

The gap between the BSA's aspirations and operational reality will close only through sustained investment in forensic infrastructure. The central government should establish a

[21] The Apex Court has issued practice directions: see, for instance, the guidelines for DNA evidence in Murli S. Deora v. Union of India (2001) 8 SCC 765, and the framework for expert evidence in State ofHimachal Pradesh v. Jai Lal (1999) 7 sec 280.

National Digital Forensic Authority to oversee the capacity, accreditation, and output of FSLs nationally, to set minimum standards for digital forensic examination, and to coordinate with state governments on infrastructure investment. The Authority should publish annual reports on caseload, capacity, and backlog, creating accountability for the forensic infrastructure.

VII. CONCLUSION

The Bharatiya Sakshya Adhiniyam, 2023, in its treatment of electronic evidence, represents a sincere and largely well-directed attempt to bring India's law of evidence into the digital age. Its conceptual reframing of electronic records as primary evidence, introduction of dual-signatory certification with hash verification, and institutionalisation of the role of forensic experts are real improvements over the IEA's inconsistently applied regime. However, the modernising aspirations of BSA are only partly realised. The structural gaps may produce inconsistent judicial responses, confusion for the lawyers, and ultimately, the distortion of the objective of finding the truth for which the evidence law exists to serve.

Essentially, BSA represents both modernisation and Pandora's box in different proportions. It is modem in conception but incomplete in execution. It has opened the box of reform, and with it, a new set of interpretive and practical difficulties, without yet providing the tools to manage what it has released. Closing that box requires legislative amendment to define experts and address novel digital evidence, and a sustained national investment in the forensic infrastructure that the BSA presupposes but does not create. Until these complements are in place, the BSA will be a statute of considerable promise and imperfect performance, which is, perhaps, where every serious reform must begin.