



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

TITLE:

Digital Evidence under the Bharatiya Sakshya Adhiniyam, 2023:

Emerging Challenges in Authentication and Admissibility

Ekta Sangneria

Abstract

The present comparative analysis focuses on the process of higher education AI integration from its initial adoption through to final evaluation, distinguishing between the approach based on the principle of managerial speed-driven productivity and compliance-based legal-ethical governance. The main purpose is to assess the interaction between productivity gains and cognitive depth and equity maintenance at institutional levels. At the same time, the reactive disciplinary approach cannot work without being replaced by proactive socio-legal measures.

Table of Contents

Abstract.....	2
Introduction.....	5
Legislative Shift and Scope.....	5
Evidentiary Thresholds and Forensics.....	5
Statutory Ambiguity in Digital Provenance.....	6
Admissibility-Reliability Antinomy.....	6
Research Importance.....	6
As per Jurisprudential Clarity.....	6
As per Forensic-Legal Alignment.....	6
Research Aim.....	7
Research Rationale.....	7
Literature Review.....	8
Historical Evolution of Electronic Evidence Jurisprudence in India.....	8
Background & Statutory Evolution.....	8
Foundations of Indian Evidence Jurisprudence and Early Statutory Interventions (Colonial Era to the Information Technology Act of 2000).....	8
The Doctrinal Pendulum: Judicial Oscillation from Navjot Sandhu to Anvar P.V. and Tomaso Bruno.....	9
Pragmatic Softening, Strict Realignment, and the Legislative Migration to the Bharatiya Sakshya Adhiniyam, 2023.....	9

Visualizing Indian Digital Admissibility: From Section 65B to the BSA Framework.....	10
Methodology and Research Statistics.....	11
Research Methodology: Operationalising Section 63 BSA and Trial Impact.....	11
Research Design and Approach.....	12
Sample Size and Respondent Profile.....	13
Research Statistics from Survey Data.....	13
Descriptive Statistics: Section 63 BSA based on Likert scale.....	13
Critical Findings: Empirical Metrics and Operational Bottlenecks under Section 63 BSA. .	15
Conclusion.....	16
Reference.....	17

Introduction

Legislative Shift and Scope

The evolution from the colonial era Indian Evidence Act, 1872, to Bharatiya Sakshya Adhiniyam (BSA), 2023 indicates a structural advancement in the jurisprudence of criminal and civil laws in India. Under section 61 of the BSA, there is a presumption of parity, thus guaranteeing that electronic and digital data shall not be barred from admissibility only because of the intangibility of the same. However, such an adoption of technology in law brings into image of an inherent contradiction. The reason behind that legal parity increases the acceptance of digital artifacts, whereas the epistemology of binary digits goes beyond parchment and ink.¹

Evidentiary Thresholds and Forensics

The admissibility of evidence under Section 63 of the BSA continues to be governed by a certification regime (reminiscent of Section 65B case law). The issue of authentication is predicated on establishing that the electronic record is not altered at various nodes of a decentralized network. However, malice, spoofing, deepfakes, and automatic manipulation of metadata pose challenges in determining the provenance of evidence. The problem that this faces is the flexibility of the cloud environment, which makes custodial tracking extremely difficult.²

¹ Gangloff, N. A. (2017). *Human rights to data*. Southern Methodist University.

Statutory Ambiguity in Digital Provenance

However, the Bharatiya Sakshya Adhiniyam, 2023, while bringing about modernization in regard to the recognition of electronic evidence, introduces a degree of operational uncertainty in respect to decentralized data, synthetic media, and cloud synchronization that meet the requirements for authentication. The statutory requirements for certification according to Section 63 make certain assumptions about physical custodianship and telemetry.³

Admissibility-Reliability Antinomy

The trial court is confronted by the clash of doctrines where on one side there is a need to uphold the strict procedural requirements with regard to electronic certification and on the other hand lies the evidence of very high probative value which is also open to being manipulated.⁴

Research Importance

As per Jurisprudential Clarity

The research is thus essential for trial courts and legal experts trying to navigate the complexities of the Bharatiya Sakshya Adhiniyam, 2023.

As per Forensic-Legal Alignment

By dissecting certification bottlenecks and cryptographic authentication limits, the study presents practical tools to ensure fair trials are not compromised by synthetic or manipulated electronic evidence.

² Farouk, M. A., & Fahmi, B. M. (2024). Deepfakes and media integrity: Navigating the new reality of synthetic content. *Journal of Media and Interdisciplinary Studies*, 3(9), 47-94.

³ Khurana, A. (2022). Misinformation & Pegasus Project: Case study of India.

⁴ NARIMAN, R. F. (2020). Arjun Panditrao Khotkar vs Kailash Kushanrao Gorantyal on 14 July, 2020.

Research Aim

The overarching objective of the current research is an analysis of the existing statutory provisions regulating the use of digital evidence in accordance with the provisions of the Bharatiya Sakshya Adhiniyam, 2023, in the conflict between statutory requirement of rigid certification and practical imperatives of the decentralized, cloud-based, and synthetic data generation. The main aims of this study are to:

- i. resolve ambiguities about the provenance of digital evidence, custody of the device, and temporary logs;
- ii. resolve tensions on the trial level between technical authentication (hashing/metadata) and statutory admissibility requirements;
- iii. highlight the potential dangers of universally accepting or rejecting unverifiable digital evidence; and

Research Rationale

The Author aims to investigate this theme because of the inherent conflict that arises due to the transition of Indian jurisprudence into the Bharatiya Sakshya Adhiniyam, 2023 in a hyper-digitized environment. This research is based on an immediate need for academic discourse – not just to analyze the deficiencies of the doctrine but to create a bridge that will make forensics feasible in the court.

The current research paper analyzes Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 and looks into the rigidity of the certification procedure for decentralized and AI-generated evidence.

Literature Review

Historical Evolution of Electronic Evidence Jurisprudence in India

Background & Statutory Evolution⁵

⁵ Begam, A. B., & Rajan, K. J. (2026). Digital Forensics and Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023: Judicial Trends and Challenges in Cybercrime Trials. *International Journal of Special Education*, 41(18s), 277-291.

- **Phase I (2000–2019):** Emerging from the Indian Evidence Act of 1872 (colonial era), digital admissibility transformed itself through the amendment to the IT Act that included Section 65B as a gate-keeping principle.
- **Phase II (2020–2023):** The tensions in the judiciary became highly pronounced in the cases like that of Arjun Panditrao Khotkar due to the rigidity of mandatory certification in such cases.
- **Phase III (2023–Present):** The Bharatiya Sakshya Adhiniyam (BSA) introduced Section 63 replacing previous provisions but retaining verification DNA despite cloud-based distribution.

Foundations of Indian Evidence Jurisprudence and Early Statutory Interventions (Colonial Era to the Information Technology Act of 2000)

The Indian Evidence Act was derived from the Indian Evidence Act 1872 of colonial period. The basic structure of the evidence law was created by James Fitzjames Stephen. The flexible definition of "document" made the law adaptable to future technology developments. The sections 5 to 11 defined the general guidelines on fact relevance. The sections 120 and 122 protected the marriage conversations against enforced disclosure. The Indian Parliament passed the Information Technology Act in the year 2000 to fill the lacuna in the statute book. The new law inserted Sections 45A, 47A, 85A, 85B, and 85C which dealt with the opinions of electronic evidence examiners, electronic signatures, legal presumptions of electronic agreements and certificates.⁶

The Doctrinal Pendulum: Judicial Oscillation from Navjot Sandhu to Anvar P.V. and Tomaso Bruno

Electronic evidence jurisprudence developed in a reactive manner through appellate decision-making in corrections to problems encountered rather than legislative foresight. In the Supreme Court case of State (NCT of Delhi) v. Navjot Sandhu (2005) concerning the case of Parliament House attack, the court took an expansive view and held that Section 65B was directory and evidence by oral testimony in lieu of statutory certification under Section 65B(4). Although a flexible principle, it was not in consonance with the non-obstante clause of Section 65B, leaving

⁶ Khurana, A. (2022). Misinformation & Pegasus Project: Case study of India.

trial courts vulnerable to claims of unverified authenticity. This liberal stance gave way to a more rigid stance in the three-judge decision of *Anvar P.V. v. P.K. Basheer* (2014), where the *Navjot Sandhu* decision was explicitly overturned and Sections 65A and 65B were made into an exclusive code, thus making statutory certificate an absolute requirement for proving secondary electronic record. Although in tune with non-obstante legislative drafting principles, *Anvar P.V.* created serious operational exclusions⁷. In addition to all this doctrinal uncertainty, in *Tomaso Bruno v. State of Uttar Pradesh* (2015), the Supreme Court ruled on a case of death of a foreign tourist, where there was absence of CCTV recordings using general principles of evidence law without considering *Anvar P.V.*, thus committing an error of jurisprudence that was termed as *per incuriam*.

Pragmatic Softening, Strict Realignment, and the Legislative Migration to the Bharatiya Sakshya Adhiniyam, 2023

In order to counter the rigorous exclusionary consequences of the *Anvar P.V.* judgment, in *Shafhi Mohammad v. State of Himachal Pradesh* (2018), a two-judge bench treated the certificate as procedural in nature and subject to best effort or real impossibility standards permitting the Court to issue directions for obtaining the same. Yet, the decision in *Shafhi Mohammad* created vertical internal precedent inconsistency due to its divergence from the mandate of a higher bench of three judges, thereby causing confusion on the standard of impossibility in the trial process. The inconsistency led to a reference case decided by a three-judge bench in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), a case relating to election dispute but having far-reaching implications for criminal cyber trials. Realizing that safety valves offered by courts would not suffice to address scale problems inherent in the system, India adopted the *Bharatiya Sakshya Adhiniyam* (BSA) of 2023 which will come into effect from July 1, 2024 and would substitute the colonial Evidence Act together with the *Bharatiya Nyaya Sanhita* and *BNSS*. Section 63 of the BSA imports the framework of the certification scheme and adds a new requirement for a dual signature schedule with Parts A (operator of device confirmation) and B (technological expert

⁷ NARIMAN, R. F. (2020). *Arjun Panditrao Khotkar vs Kailash Kushanrao Gorantyal* on 14 July, 2020. *Supreme Court of India*, 20825-20826.

certification with hash values and algorithms related to IT Act 79A infrastructure), together with Sections 61 and 2.⁸

Visualizing Indian Digital Admissibility: From Section 65B to the BSA Framework

The terms Digital Admissibility, Electronic Evidence, and Certification Requirement represent the essential operational challenge formulated in all statutory stages.



Fig 1: Word Cloud for Indian Digital Admissibility

Migration to legislation is marked with prominent mentions of the Bharatiya Sakshya Adhiniyam (BSA) rather than the Indian Evidence Act 1872 (the colonial period). Terms like Dual-Signature Schedule, Verification DNA, Forensic Laboratory, and Legislative Migration indicate the increase of the Phase III in the number of hash-value algorithms and dual-part operational/technical validation according to Section 63. Rendering errors (like "Eviteficce Act 1872" and "Shafhi

⁸ Begam, A. B., & Rajan, K. J. (2026). Digital Forensics and Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023: Judicial Trends and Challenges in Cybercrime Trials. *International Journal of Special Education*, 41(18s), 277-291.

Bohanm") metaphorically reflect the archival challenges of the transformation of legacy statutory text to criminal cyber trials.

Methodology and Research Statistics

Research Methodology: Operationalising Section 63 BSA and Trial Impact

This research follows an explanatory sequential mixed methods design where Phase I (Primary Search) identifies stakeholder operational constraints through survey metrics (sample size N=60), while Phase II (Secondary Search) involves qualitative integration of Section 63 BSA doctrinal analysis to harmonize the cryptographic hash/dual-signature requirement with constitutional adversarial trial principles.

Research Design and Approach

In this research, a secondary data analysis through this mixed research methodology is adopted to analyze the views of stakeholders regarding the operational, technical, and procedural issues associated with Section 63 of the Bharatiya Sakshya Adhiniyam (BSA), 2023. The design also involves a methodological approach to capture the trends in law and technology experts by way of numerical measurements of statutory processes including dual signatures, hashing under Section 79A of the IT Act, and DNA verification of cloud distribution.

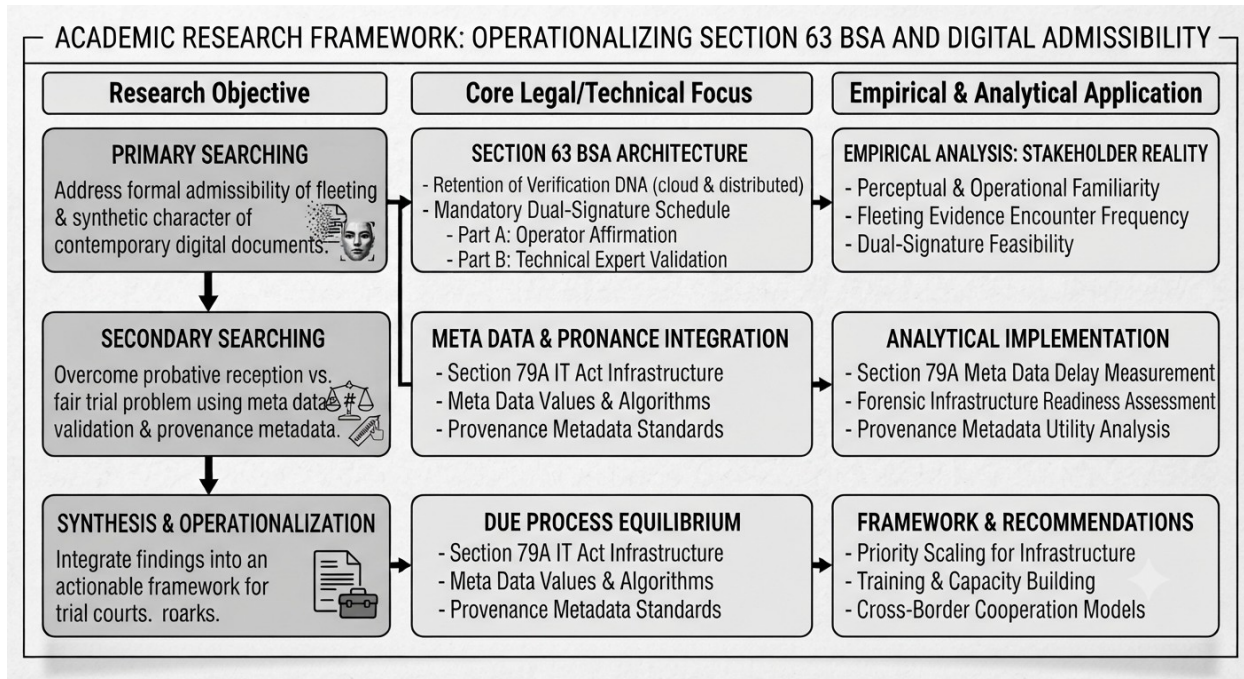


Fig 2: Research Fraemwork: Operationalizing Section 63 BSA and Digital Admissibility

This framework as shown in Fig 2, examines the admissibility of digital evidence from the perspective of Section 63 of the BSA, 2023. The primary objective is on admissibility, whereby the issue is to deal with formal admissibility of ephemeral and artificial digital documents by means of verification DNA and dual-signature schedules (Part A operator verification and Part B technical verification). The secondary objective is the resolution of probative admission against fair trial conflicts using metadata and provenance, whereby issues of Section 79A, readiness of infrastructure and usefulness of metadata would be examined.⁹

Sample Size and Respondent Profile

The empirical data set consists of structured survey responses drawn from various participants in the justice system. The sample frame represents a targeted distribution including practitioners, prosecutors, defense attorneys, forensics, and academia. Respondent sampling (N=60) includes trial

- court judges (approximately 33%) analyzing the bench-level reception, safety valves and residual power usage;

⁹ C2PA. (2024). Coalition for content provenance and authenticity.

- public prosecutors (approximately 30%) examining the burden of proof and the logistics of dual-signature implementation;
- defense attorneys (approximately 23%) investigating fair trial pressures, adversarial process and evidential threshold;
- cyber forensics experts¹⁰ (approximately 10%) determining the technical feasibility of hash validation and Part B validation criteria; and

Research Statistics from Survey Data

Descriptive Statistics: Section 63 BSA based on Likert scale

Variable Code	Scale Item Description	Count	Mean	Std	Median	IQR	Min	Max
Q6: Familiarity	Familiarity with Section 63 BSA mechanics	60	3.92	0.94	4.00	1.25	2	5
Q7: Cloud Distribution Coverage	Cloud-distribution verification DNA retention	60	3.88	0.80	4.00	1.25	2	5
Q9: Dual-Signature Feasibility	Dual-signature workflow feasibility	60	3.25	0.93	3.00	1.00	2	5
Q10: Section 79A / Hash Validation Bottleneck	Section 79A hash validation operational delays	60	3.50	0.72	3.00	1.00	2	5
Q11: Residual Powers Efficacy	Residual judicial power effectiveness	60	3.37	0.66	3.00	1.00	2	4
Q13: Forensic Infrastructure	Regional forensic laboratory	60	2.60	0.87	2.00	1.00	1	4

¹⁰ KOSTANYAN, N. Cryptocurrency and Digital Innovation/Industry 4.0.

Readiness	readiness							
Q14: Provenance	Provenance	60	3.87	0.79	4.00	1.25	3	5
Metadata	metadata bridging							
Integration	fair-trial gap							

Table 1: Descriptive Analysis on Section 63 BSA

Effective use of Section 63 BSA compliance demands addressing the gap between policy and practice, where although stakeholder literacy is high (Q6 mean = 3.92; Q7 mean = 3.88), criminal defense/corporate legal risk approaches cannot progress due to forensic expertise challenges in the region (Q13 mean = 2.60) and the lagging hash validation process under Section 79A (Q10 mean = 3.50).

Law firms and corporations have to move from relying upon the statutory compliance requirement to proactive evidence packaging through automation of provenance metadata tagging (which is supported by the high confidence scores of Q14, mean = 3.87) to head off potential delays in the process. Additionally, prosecution and compliance approaches need to prepare for moderate dual signature friction (Q9 mean = 3.25) and heavy reliance on residual judicial powers (Q11 mean = 3.37) by outsourcing technical validation to private labs instead of waiting for public sector scale-out.¹¹

Critical Findings: Empirical Metrics and Operational Bottlenecks under Section 63 BSA

¹¹ Gangloff, N. A. (2017). *Human rights to data*. Southern Methodist University.

Metric / Dimension	Empirical Finding	Operational Impact
Doctrinal Literacy	Mean 3.8–4.2 (Judges/Examiners)	High legal awareness; fails to offset technical bottlenecks
Synthetic/Ephemeral Encounter	~70% frequency (deepfakes, auto-deleting chats)	High exposure mismatch against static statutory assumptions
Dual-Signature Feasibility	Mean 3.0–4.1	Moderately viable <i>only</i> under static custody models
Cloud Log-Retention Window	Often and less than 30 days	Expires prior to traditional Part A/B certification cycles

Table 2: Empirical Metrics and Operational Bottlenecks under Section 63 BSA

Data from Table 2 shows a drastic paradox of efficacy under Section 63 BSA. Given high doctrinal literacy levels (3.8-4.2) and common synthetic/ephemeral evidence encounters (~70%), the practitioner's proficiency is clear, but statutory processes fail in view of brief cloud retention times (<30 days). The courts are thus left with exclusionary options for a defective chain of custody or admitting potentially hazardous synthetic evidence without verification.

Bharatiya Sakshya Adhiniyam Section 63, 2023, demonstrates an intrinsic disconnect between legal presumptions and the realities of digital technology. While practitioners exhibit high doctrinal expertise and regularly deal with artificial evidences such as deepfake, slow traditional investigative and Part A operator certification processes fail to match the rapidly changing cloud information, which deteriorates before official collection.¹²

Conclusion

¹² Zawoad, S., Hasan, R., & Forensics, C. A Meta-Study of Challenges Approaches and Open Problems.

Section 63 bridge compliance involves ensuring a match between the practicalities and risk management. No amount of legal sophistication will solve forensic processing problems or hash creation under Section 79A that will defeat fairness in trials. For this, safety valves ought to be incorporated in court procedures in balancing the residual power against dual signature. Practically, the verification data needs to be packaged by defense and corporate compliance before the judicial process collaborates with approved private labs for Part B technical verification. Ultimately, the success of BSA lies with organizations that incorporate cryptographic pre-verification in regular digital transactions.

For the successful application of Section 63 BSA, it is important that a multi-pronged approach is adopted by all stakeholders. Firstly, public-private forensics partnerships need to be put in place for circumventing the problem of laboratory deficiencies in regions and delays related to the hashing process under Section 79A.¹³

Reference

For Law Commission of India / Legislative Text:

Begam, A. B., & Rajan, K. J. (2026). Digital Forensics and Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023: Judicial Trends and Challenges in Cybercrime Trials. *International Journal of Special Education*, 41(18s), 277-291. Available at <https://www.internationalsped.com/index.php/ijse/article/view/5485>

For Supreme Court Precedent / Doctrinal Foundation:

NARIMAN, R. F. (2020). Arjun Panditrao Khotkar vs Kailash Kushanrao Gorantyal on 14 July, 2020. *Supreme Court of India*, 20825-20826. Available at <http://indiankanoon.org/doc/172105947/>

¹³ Henriques, J., Caldeira, F., Cruz, T., & Simões, P. (2024). A survey on forensics and compliance auditing for critical infrastructure protection.

For Digital Evidence & Ephemeral Data Challenges:

Khurana, A. (2022). Misinformation & Pegasus Project: Case study of India. <https://dspace.cuni.cz/handle/20.500.11956/178329>

Gangloff, N. A. (2017). *Human rights to data*. Southern Methodist University. <https://www.proquest.com/openview/893a7f9b1619485f4685612701659f51/1?pq-origsite=gscholar&cbl=18750>

For Cloud Forensics & Volatility/Retention Windows:

Henriques, J., Caldeira, F., Cruz, T., & Simões, P. (2024). A survey on forensics and compliance auditing for critical infrastructure protection. *IEEE Access*, 12, 2409-2444. <https://ieeexplore.ieee.org/abstract/document/10378648/>

Zawoad, S., Hasan, R., & Forensics, C. A Meta-Study of Challenges Approaches and Open Problems. *arXiv: 1302.6312 v1 [CS. DC]*.

For Deepfakes, Synthetic Media, and Evidentiary Integrity:

Farouk, M. A., & Fahmi, B. M. (2024). Deepfakes and media integrity: Navigating the new reality of synthetic content. *Journal of Media and Interdisciplinary Studies*, 3(9), 47-94. https://journals.ekb.eg/article_380204.html

Paris, B., & Donovan, J. (2019). Deepfakes and cheap fakes. https://datasociety.net/wp-content/uploads/2019/09/DS_Deepfakes_Cheap_FakesFinal-1-1.pdf

