DIGITAL FORENSICS IN CORPORATE FRAUD INVESTIGATIONS: A LEGAL ANALYSIS UNDER THE INDIAN FRAMEWORK

by

Bhumeshwary Kalyanrav Mahajan

Abstract

The migration of corporate fraud into cloud-distributed, encrypted, and machine-generated forms has outpaced the architecture of Indian evidence law. The Bharatiya Sakshya Adhiniyam 2023 (BSA) modernised the formal treatment of electronic records, granting them evidentiary parity and channelling their admissibility through a structured regime of certification, hash-value disclosure, and expert authentication. This paper argues that, although the BSA represents a genuine doctrinal advance over the Indian Evidence Act 1872 and although the Supreme Court has now confirmed the constitutional validity of its certification framework, the statute remains functionally under-equipped for the distinctive evidentiary realities of digital corporate fraud — cloud and enterprise-resource-planning data outside any single custodian, end-to-end encrypted communications, cross-border storage beyond Indian process, and the emergent threat of AI-generated and deepfaked artefacts. The deficiency is therefore not constitutional but operational and institutional. Adopting a doctrinal method with a comparative dimension, the paper contends that India requires a targeted recalibration of Section 63 for distributed-data contexts, a dedicated cloud-forensics certification regime, and sustained judicial and prosecutorial capacity-building, without which the BSA's digital-first promise will fail at precisely the high-stakes intersection where reliability matters most.

Introduction

1.1 Defining Corporate Fraud in the Digital Age

Corporate fraud, in its classical conception, was a fraud of paper: forged ledgers, falsified balance sheets, and fabricated correspondence. The Indian statutory vocabulary still reflects this lineage, with Section 447 of the Companies Act 2013 defining fraud capaciously to capture any act, omission, concealment, or abuse of position intended to deceive or injure the interests of the company, its shareholders, or its creditors.[1] What has changed is not the legal concept of fraud but its evidentiary substrate. The acts that constitute modern corporate fraud — the diversion of funds, the manipulation of accounts, the issuance of unauthorised instruments — are now planned, executed, and concealed almost entirely through digital systems. The fraud is the same; the trace it leaves is different.

This shift matters because the law of proof, not the law of liability, is where digital corporate-fraud prosecutions increasingly succeed or fail. A fraud may be morally and commercially obvious yet remain legally unprovable if the electronic records that evidence it cannot be authenticated to the standard the law demands. The central concern of this paper is therefore the interface between digital forensic practice and the evidentiary rules that determine whether forensically recovered material can be placed before, and relied upon by, a court.

1.2 The Emergence of Digital Forensics as an Investigative Tool

Digital forensics — the identification, preservation, examination, and presentation of electronically stored information in a manner that withstands legal scrutiny — has moved from a peripheral specialism to the evidentiary core of serious fraud investigation. In the corporate context it encompasses the imaging of servers and devices, the recovery of deleted records, the reconstruction of email and messaging trails, the analysis of enterprise accounting systems, and the tracing of fund flows across institutions and jurisdictions. The discipline's value to the law lies in its claim to reliability: properly conducted, it can demonstrate not merely the content of a record but its integrity over time.

That claim, however, is only as strong as the legal framework that receives it. Forensic soundness and legal admissibility are distinct standards, and a central argument of this paper is that Indian law has yet to align the two for the most demanding category of digital evidence.

1.3 Scope, Objectives, and Research Methodology

[1] Companies Act 2013, s 447.

This paper adopts a primarily doctrinal methodology, analysing the statutory framework of the Bharatiya Sakshya Adhiniyam 2023, the residual operation of the Information Technology Act 2000, the investigative architecture of the Companies Act 2013, and the judicial interpretation of each. It incorporates a focused comparative dimension, drawing on the European Union's e-Evidence Regulation and the United States Federal Rules of Evidence, not to transplant foreign solutions but to illuminate the specific gaps in the Indian regime. The paper is normative in its conclusion: it argues for a defined programme of statutory and institutional reform.

The scope is deliberately confined to corporate fraud rather than electronic evidence at large. This confinement is analytically purposeful: corporate fraud concentrates, in a single category, every feature that stresses the BSA framework — distributed custody, cross-border storage, encryption, and high evidentiary stakes — and therefore serves as the clearest test of the statute's adequacy.

1.4 Significance of the Study in the Current Indian Legal Landscape

The timing of this inquiry is not incidental. The BSA came into force on 1 July 2024, replacing the Indian Evidence Act 1872,[2] and its electronic-evidence provisions have only recently begun to receive authoritative judicial treatment. In May 2026 the Supreme Court delivered its first significant pronouncement on the constitutional validity of the certification regime,[3] leaving the field in a formative state in which scholarly intervention can still shape the trajectory of doctrine and institutional design. This paper seeks to contribute to that formative moment.

2. The Evolution of Digital Forensics in India's Corporate Fraud Context

2.1 From Paper Trails to Digital Footprints — A Conceptual Shift

The evidentiary transformation can be stated precisely. Where the auditor once reconciled physical vouchers, the forensic examiner now images a database; where the investigator once subpoenaed letters, she now reconstructs message threads and metadata. The conceptual significance is that digital records carry, in addition to their content, a layer of forensic metadata — timestamps, access logs, hash values, and system artefacts — that can corroborate or impeach the record's integrity. This dual character is both the promise and the difficulty of digital evidence: it offers a richer basis for proof than paper ever did, while demanding a more exacting and technically literate process of authentication.

[2]Bharatiya Sakshya Adhiniyam 2023 (Act 47 of 2023); brought into force with effect from 1 July 2024.

[3]Pune Bar Association v Union of India, Writ Petition (Civil) No 599 of 2026 (Supreme Court of India, 22 May 2026); reported as 2026 LiveLaw (SC) 551.

2.2 Landmark Indian Corporate Fraud Cases and the Role of Digital Evidence

2.2.1 Satyam: accounting fraud as data fabrication

The Satyam Computer Services fraud, disclosed when chairman B. Ramalinga Raju confessed in January 2009 to inflating the company's accounts — including a cash balance overstated by thousands of crores — was, at its core, a fraud of fabricated data: falsified bank confirmations, fictitious invoices, and manipulated financial records generated and sustained through the company's information systems.[4] Satyam demonstrated, well before the BSA, that the proof of large-scale corporate fraud would increasingly turn on the forensic interrogation of electronic accounting systems rather than the testimony of witnesses to paper.

2.2.2 The PNB–Nirav Modi fraud: systems as the locus of fraud

The Punjab National Bank fraud, which surfaced in early 2018, illustrated the point more sharply. The fraud was perpetrated through the issuance of unauthorised Letters of Undertaking transmitted via the SWIFT messaging network, exploiting the fact that SWIFT was not reconciled with the bank's Core Banking System — so that the fraudulent instruments left no trace in the bank's primary records for several years.[5] Here the locus of the fraud was the gap between two electronic systems, and its detection and proof depended entirely on the forensic reconstruction of message logs and system records. Notably, allegations in the wider proceedings included the destruction of digital evidence — mobile devices and a server — underscoring that the integrity and preservation of electronic records is itself a battleground in corporate-fraud litigation.[6]

2.2.3 IL&FS: governance failure and the disclosure record

The IL&FS crisis of 2018, in which the infrastructure-finance group's defaults exposed deep governance and disclosure failures, prompted investigation by the Serious Fraud Investigation Office and the Ministry of Corporate Affairs and again placed the integrity of the company's electronic disclosure and accounting record at the centre of the inquiry.[7] Taken together, these

[4]On the Satyam fraud generally, see the contemporaneous record of B. Ramalinga Raju's confession (January 2009) and the subsequent conviction of the accused on 10 April 2015 by the Special CBI Court, Hyderabad; fraud dimensions of Rs 5,040 crore in fictitious cash and bank balances, with a total manipulation of approximately Rs 7,136 crore.

[5]On the mechanics of the PNB fraud, see the CBI's First Information Report and charge sheets (2018); the fraud is widely reported in the range of approximately Rs.14,357 crore. , the precise quantum and procedural history against the primary record.

[6]Reported allegations against an associate in the PNB matter included the destruction of digital devices and a server; , against the relevant charge sheet or judicial record.

[7]The IL&FS matter was referred to the Serious Fraud Investigation Office; , the precise scope, dates, and findings of the SFIO investigation against the official record before citation.

matters trace a clear trajectory: the evidence of corporate fraud is now overwhelmingly electronic, and its forensic recovery and authentication are decisive.

2.3 Institutional Response: The Rise of the SFIO and Its Digital Forensic Powers

India's institutional response was the creation of a specialist investigator. The Serious Fraud Investigation Office, originally constituted by a Government resolution of 2 July 2003, was placed on a statutory footing by Section 211 of the Companies Act 2013 as a multi-disciplinary body whose membership, as elaborated in the rules made under that section, expressly encompasses expertise in cyber forensics and information technology.[8] Section 212 empowers the Central Government to assign the investigation of a company's affairs to the SFIO, confers exclusive jurisdiction once a matter is so assigned, and equips its investigating officers with the powers of an inspector, including search, seizure, and (subject to safeguards) arrest.[9]

The Supreme Court has confirmed the breadth of these powers, holding in Serious Fraud Investigation Office v Rahul Modi that the time limit specified in a Government order assigning an investigation is directory rather than mandatory, so that the SFIO's mandate does not lapse on its expiry.[10] The institutional capacity to investigate digital corporate fraud, in short, exists. The argument of this paper is that the evidentiary framework through which the fruits of that investigation must pass has not kept pace.

2.4 Limitations of the Pre-BSA Framework (IEA and IT Act 2000)

Under the Indian Evidence Act 1872, the admissibility of electronic records was governed by Sections 65A and 65B, the latter requiring a certificate as a condition of admitting secondary electronic evidence.[11] The provision proved a fertile source of litigation precisely because its certification requirement, designed for discrete computer outputs, fitted awkwardly onto the realities of networked and distributed data — a tension the courts spent more than a decade attempting to resolve, as Part 6 below describes. The BSA was enacted against this backdrop of doctrinal instability, and the question this paper pursues is whether it has resolved that instability for the corporate-fraud context or merely relocated it.

---

[8]Companies Act 2013, s 211 (establishment of the SFIO; the section expressly contemplates the appointment of persons with expertise in, inter alia, cyber forensics). The SFIO was originally set up by Government Resolution dated 2 July 2003.

[9]Companies Act 2013, s 212; investigating officers exercise the powers of an inspector under s 217, with general search and seizure under s 209, seizure of documents by an inspector under s 220, and arrest under s 212(8).

[10]Serious Fraud Investigation Office v Rahul Modi, 2019 SCC OnLine SC 423, decided on 27 March 2019

[11]Indian Evidence Act 1872, ss 65A and 65B (now repealed).

3. Legal Framework Governing Digital Evidence in India

3.1 The Bharatiya Sakshya Adhiniyam 2023 — Sections 61, 62, and 63 Decoded

The BSA's treatment of electronic evidence rests on three linked provisions. Section 61 establishes the principle of parity: an electronic or digital record shall not be denied admissibility merely because it is electronic, and, subject to Section 63, has the same legal effect, validity, and enforceability as any other document.[12] Section 62 is the channelling provision: the contents of electronic records may be proved in accordance with Section 63.[13] Section 63 is the operative provision, deeming computer output to be a document and rendering it admissible without production of the original, provided the statutory conditions are satisfied.[14]

The BSA's drafting expands the reach of the old regime in two material respects. Section 63 extends to records held in semiconductor memory, in addition to optical and magnetic media, and to records produced by any communication device, not merely a computer — an enlargement that brings smartphones, messaging platforms, and a wide range of devices squarely within the provision.[15]

3.2 Electronic Records as Documentary Evidence — A Paradigm Shift from IEA Section 65B

The conceptual shift effected by Section 61 is significant. By providing that electronic records shall not be denied admissibility on the ground of their electronic character, the BSA reframes the default: electronic records are admissible documentary evidence, subject to the authentication discipline of Section 63. This is a deliberate legislative answer to a long-running interpretive controversy under the old Act about whether Section 65B was the exclusive route for proving electronic records or merely one route among several — a controversy traced in Part 6. The BSA's structure, channelling proof of contents through Section 63 while affirming parity in Section 61, is best read as endorsing a regime in which authenticated electronic records are full documentary evidence.

3.3 The Certificate Requirement, Hash-Value Verification, and Expert Testimony

3.3.1 The statutory certificate and its Schedule

[12]Bharatiya Sakshya Adhiniyam 2023, s 61.

[13]Bharatiya Sakshya Adhiniyam 2023, s 62.

[14]Bharatiya Sakshya Adhiniyam 2023, s 63.

[15]Bharatiya Sakshya Adhiniyam 2023, s 63(1) (extending coverage to semiconductor memory and to records produced by any communication device).

Section 63(4) requires that, where a statement is to be given in evidence by virtue of the section, a certificate in the form specified in the Schedule accompany the electronic record at each instance of its submission.[16] The Schedule divides the certificate into two parts: Part A, to be completed by the party producing the record, and Part B, to be completed by an expert. The certificate must, among other things, disclose the hash value of the record, obtained through a specified algorithm.[17]

3.3.2 Hash values as a substantive safeguard

A hash value is a fixed-length alphanumeric output produced by a cryptographic algorithm from the contents of a file; any alteration of the contents produces a different value, so that an identical hash reliably attests that two records are exact duplicates. Its inclusion in the certificate is intended to anchor the integrity of the record at the point of seizure or extraction. As Part 6 explains, the Supreme Court has characterised this requirement not as an empty formality but as a substantive safeguard against the manipulation to which electronic records are uniquely vulnerable.

3.3.3 The expert and the residual uncertainty

Part B introduces a requirement absent from the old Section 65B: certification by an expert. Who qualifies as such an expert is a question of considerable practical consequence, and one that — as Part 5.5 and Part 6.3 develop — the Supreme Court has expressly left open. The interaction of Section 63(4) with Section 39 of the BSA, which governs the relevance of expert opinion on electronic evidence, is therefore central to the workability of the entire regime.[18]

3.4 Interplay Between the BSA 2023, the IT Act 2000, and the Companies Act 2013

Three statutes operate in combination. The Companies Act 2013 supplies the investigative engine through the SFIO; the IT Act 2000 supplies, in Section 79A, the mechanism by which the Central Government notifies Examiners of Electronic Evidence;[19] and the BSA supplies the evidentiary rules of admission. The points of friction lie at the joints between them — most acutely in the relationship between the BSA's demand for an expert under Section 63(4) and the limited pool of Examiners notified under Section 79A, a tension examined in Part 6.3.

3.5 Comparative Overview — the EU e-Evidence Regulation and the US Federal Rules of Evidence

[16]Bharatiya Sakshya Adhiniyam 2023, s 63(4) and the Schedule thereto.

[17]Bharatiya Sakshya Adhiniyam 2023, s 63(4); the Schedule prescribes Part A (party) and Part B (expert), and requires disclosure of the hash value of the electronic or digital record.

[18]Bharatiya Sakshya Adhiniyam 2023, s 39(1)–(2) (relevance of expert opinion, including the opinion of an Examiner of Electronic Evidence).

[19]Information Technology Act 2000, s 79A (notification of Examiners of Electronic Evidence).

3.5.1 The EU e-Evidence Regulation (2023/1543)

Regulation (EU) 2023/1543, the e-Evidence Regulation, creates the European Production Order and the European Preservation Order, enabling a judicial authority in one Member State to compel a service provider in another to produce or preserve electronic evidence directly, within short timeframes, bypassing traditional mutual legal assistance.[20] The Regulation is directly relevant to the cross-border problem that besets Indian corporate-fraud investigations, because it confronts head-on the question the BSA leaves unaddressed: how to obtain admissible electronic evidence held by a provider beyond the forum's territorial reach.

3.5.2 US Federal Rules of Evidence 902(13)–(14)

The United States addressed the authentication of electronic records through the 2017 addition of Rules 902(13) and 902(14) to the Federal Rules of Evidence, which permit the self-authentication of electronically generated and electronically copied records on the certification of a qualified person, typically through hash-value comparison, dispensing with live foundation testimony where authenticity is not genuinely disputed.[21] The contrast with the BSA is instructive. The American rules use certification to streamline admission while preserving the opponent's right to challenge; the Indian regime uses certification as a precondition of admission. Both pivot on hash values and a qualified certifier, but they allocate the burden of authentication differently — a comparison Part 6.4 develops as a source of reform options.

4. Techniques and Tools in Digital Forensic Investigations

4.1 Core Forensic Processes — Collection, Preservation, Examination, Analysis, Reporting

Digital forensic practice is conventionally organised into a sequence: collection (the forensically sound acquisition of data, typically through bit-for-bit imaging), preservation (the maintenance of integrity, classically through hash verification at acquisition and on each transfer), examination and analysis (the recovery and interpretation of relevant data, including deleted and fragmentary material), and reporting (the documentation of method and findings for legal use). Each stage maps onto a legal requirement: the BSA's hash-value certificate is, in effect, a statutory demand that the preservation stage be evidenced. The alignment between forensic method and legal rule is closest

[20]Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings [2023] OJ L191/118; the Regulation applies from 18 August 2026.

[21]Federal Rules of Evidence (US), r 902(13)–(14), effective 1 December 2017 (self-authentication of certified electronic records and of data copied from an electronic device, by certification of a qualified person, e.g. by hash value).

at this point and, as the following sub-parts show, loosest where the data is distributed, encrypted, or fabricated.

4.2 Forensic Investigation of Corporate Communication Channels

Corporate fraud is frequently negotiated and coordinated through email and messaging platforms, including WhatsApp, Telegram, and Signal. The forensic challenge is twofold. First, much of this communication is held not on a single seized device but on platform servers or in synchronised cloud copies, complicating both acquisition and the identification of a person competent to certify it. Second, the BSA's expansion of Section 63 to records produced by any communication device brings such material clearly within the admissibility regime, but the statute's certification model still presupposes an identifiable custodian and device — a presupposition that messaging data routinely defeats.

4.3 Cloud Forensics — Investigating ERP Systems, Cloud Storage, and Distributed Data

4.3.1 The distributed-custody problem

Enterprise data increasingly resides in cloud-hosted enterprise-resource-planning systems and distributed storage, where no single computer holds the record and no single official controls the relevant device. This is the deepest point of tension with Section 63, whose certificate is framed around a person in charge of the computer or communication device. Where the relevant activity is performed across many machines, Section 63 itself anticipates the difficulty by deeming all such devices to constitute a single computer for the purposes of the section;[22] but this deeming fiction does not resolve the practical question of who, in a multi-tenant cloud environment operated by a third-party provider, is competent to give the certificate.

4.3.2 The limits of statutory deeming

The result is that the most probative evidence in a modern corporate-fraud investigation — the ERP records that show the actual flow of transactions — is also the evidence most vulnerable to an authentication challenge under the current framework. The paper returns to this gap in its reform proposals.

4.4 AI-Assisted Forensic Tools and Their Evidentiary Reliability

Forensic practice increasingly deploys artificial-intelligence and machine-learning tools to triage large datasets, identify anomalous transactions, and cluster communications. These tools raise a

[22] Bharatiya Sakshya Adhiniyam 2023, s 63(3) (treating multiple computers or communication devices used over a period as a single computer or communication device).

reliability question that the BSA does not address: where an inculpatory inference is generated by an opaque algorithmic process, the hash-value certificate authenticates the integrity of the underlying data but says nothing about the reliability of the analytical method applied to it. Indian evidence law contains no developed standard for the reliability of scientific or algorithmic methods of analysis, as distinct from the authenticity of records — a lacuna that becomes acute as forensic tooling grows more sophisticated.

4.5 Chain of Custody in the Digital Environment — Challenges and Best Practices

Chain of custody — the documented, unbroken account of who handled evidence, when, and how — is the connective tissue between forensic method and legal admissibility. In the digital environment it is maintained primarily through hash verification at each transfer and through contemporaneous logging. The BSA's certificate regime can be understood as an attempt to render a portion of the chain of custody statutory and standardised. Its limitation is that it captures integrity at the point of certification but presupposes that the anterior collection was itself sound; where collection occurs in a cloud or cross-border environment, the certificate may attest to the integrity of a copy whose provenance is itself contestable.

5. Challenges in the Admissibility of Digital Evidence in Corporate Fraud Trials

5.1 Encrypted and End-to-End Encrypted Evidence

End-to-end encrypted communications present a structural obstacle: the content is, by design, inaccessible to the platform and therefore unobtainable by ordinary production. Investigators are typically confined to material recoverable from an endpoint device or from unencrypted backups. The evidentiary consequence is that the most relevant communications may be unavailable in admissible form, and that what is recovered may be partial in ways that affect its integrity — and hence its hash-anchored certification — in contested ways.

5.2 Deepfakes and AI-Generated Evidence — A New Threat to Evidentiary Integrity

The maturation of generative technology introduces a threat the BSA's framework was not designed to meet: the fabrication of realistic audio, video, and documentary artefacts. The hash-value certificate authenticates that a record has not been altered since acquisition; it cannot establish that the record was authentic at creation. A deepfaked audio recording, once acquired and hashed, will certify cleanly under Section 63(4) even though it is fabricated. This exposes a conceptual gap between integrity (which the BSA secures) and authenticity of origin (which it does not), and it is in corporate-fraud litigation — where the stakes invite sophisticated fabrication — that the gap is most dangerous.

5.3 Cross-Border and Cloud Data Jurisdiction Issues

Where the relevant data is stored abroad, the Indian investigator confronts the limits of territorial process. The BSA contains no mechanism analogous to the European Production Order for compelling production from a foreign-held service provider, and reliance on mutual legal assistance is notoriously slow relative to the speed at which electronic evidence can be moved or deleted. The comparative material in Part 3.5 is pointed here: the EU has legislated a direct cross-border production mechanism precisely because admissibility rules alone cannot solve an access problem. India's framework addresses admission but not acquisition across borders.

5.4 Gaps in Judicial and Prosecutorial Technical Competence

Even a well-designed framework fails without the institutional capacity to operate it. The certification regime presupposes that judges can assess the sufficiency of a hash-value certificate, that prosecutors can lead and defend expert evidence on forensic method, and that a sufficient pool of qualified experts exists. Each presupposition is, in practice, strained. The competence gap is not a defect in the statute but a condition of its effective operation, and it is one that legislative drafting alone cannot cure.

5.5 The Authentication Problem — Who Certifies the Certifier?

These threads converge on a single question: who is competent to give the Part B expert certificate, and how is the reliability of that expert assured? The BSA requires an expert but does not exhaustively define one; the IT Act provides for notified Examiners under Section 79A, but the pool of such examiners is small. The resulting bottleneck — too few authorised certifiers for the volume of electronic evidence now routine in litigation — is, as Part 6.3 shows, the precise issue that reached the Supreme Court. The authentication problem is therefore not that the BSA's safeguards are too demanding in principle, but that the institutional apparatus required to satisfy them is underdeveloped. This distinction frames the reform argument that follows.

6. Judicial Precedents and Institutional Practice

6.1 Evolution of Indian Case Law on Electronic Evidence — From Anvar P.V. to the BSA Era

6.1.1 Navjot Sandhu and the era of latitude

The trajectory of Indian electronic-evidence jurisprudence is one of oscillation toward, and finally a settling upon, strictness. In State (NCT of Delhi) v Navjot Sandhu the Supreme Court had

permitted electronic records to be proved as secondary evidence without compliance with Section 65B,[23] a permissive position that introduced inconsistency into the lower courts.

6.1.2 Anvar P.V.: certification made mandatory

In Anvar P.V. v P.K. Basheer a three-judge bench overruled that approach, holding that Sections 65A and 65B constituted a complete and exclusive code for proving electronic records and that the Section 65B(4) certificate was mandatory for secondary electronic evidence.[24] The Court reasoned that the certification requirement was not a formality but a guarantee of reliability, given the ease with which electronic records can be altered.

6.1.3 Shafhi Mohammad and Arjun Panditrao: the dilution reversed

A two-judge bench in Shafhi Mohammad v State of Himachal Pradesh subsequently relaxed the rule, suggesting that the certificate could be dispensed with where the party tendering the evidence did not control the device.[25] That dilution was decisively reversed in Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal, where a three-judge bench restored Anvar P.V., held the certificate to be a condition precedent to admissibility, and clarified that a party unable to obtain the certificate may apply to the court to compel its production.[26] The BSA was thus enacted onto a doctrinal foundation of strict certification, and Section 63 is best read as the statutory codification of the Anvar–Arjun Panditrao line.

6.2 SFIO Investigations and Evidentiary Outcomes

The translation of SFIO investigative output into evidentiary outcomes has been uneven, and the difficulty is instructive. Investigations of the scale of the matters described in Part 2 generate vast volumes of electronic material whose admission depends on satisfying, record by record, the certification discipline. Where the data is distributed across systems and custodians, the very thoroughness of the forensic recovery can multiply the points at which an admissibility challenge may be raised. The institutional lesson is that investigative capacity and evidentiary throughput are distinct, and that the bottleneck increasingly lies at the latter.

6.3 Recent Judicial Pronouncements under the BSA 2023

6.3.1 Pune Bar Association v Union of India: the framework upheld

[23] State (NCT of Delhi) v Navjot Sandhu (2005) 11 SCC 600.
[24] Anvar PV v PK Basheer (2014) 10 SCC 473.
[25] Shafhi Mohammad v State of Himachal Pradesh (2018) 2 SCC 801 (subsequently overruled).
[26] Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1.

The most significant judicial treatment of the BSA's electronic-evidence regime to date is Pune Bar Association v Union of India, decided by the Supreme Court on 22 May 2026.[27] The petitioner challenged Section 63(4) and the Schedule as unconstitutionally onerous, contending that the dual requirements of hash-value disclosure and expert certification imposed an unreasonable burden on ordinary litigants. The Court rejected the challenge, holding that the requirements bear a rational nexus to the legitimate object of securing the authenticity and integrity of electronic evidence, and characterising the hash-value disclosure as a substantive safeguard rather than a technical formality. An electronic record, the Court observed, is a unique species of evidence liable to continuous mutation, and the additional safeguards are a proportionate response to that vulnerability.

6.3.2 The expert question left open

Crucially, however, the Court declined to confine Part B certification to Examiners notified under Section 79A of the IT Act. Reading Sections 39(1) and 39(2) of the BSA harmoniously, it held that a person possessing genuine special skill in computer science and cyber forensics may, on satisfaction of the court, also qualify as an expert competent to sign Part B; and it clarified that a restrictive High Court view limiting certification to Section 79A examiners should not be treated as binding.[28] The Court expressly kept the larger question open. Two propositions therefore follow for the present argument. First, the constitutional validity of the certification regime is now settled, and any reform argument premised on the regime being unconstitutionally burdensome is foreclosed. Second, the Court itself has identified the live and unresolved problem as institutional — the identification and adequacy of qualified experts — which is precisely the operational gap this paper addresses.

6.3.3 A residual drafting ambiguity

A further, unresolved interpretive difficulty concerns whether the hash value required by the Schedule attaches to the original record, the produced copy, or both — a question of real forensic consequence on which commentary remains divided and authoritative resolution awaited.[29]

---

[27] Pune Bar Association v Union of India, Writ Petition (Civil) No 599 of 2026 (Supreme Court of India, 22 May 2026); reported as 2026 LiveLaw (SC) 551 (Surya Kant CJI, Joymalya Bagchi and Vipul M Pancholi JJ).

[28] Pune Bar Association v Union of India (n above); the Court read Bharatiya Sakshya Adhiniyam 2023, s 39(1) together with s 39(2) and declined to confine Part B certification to Examiners notified under s 79A of the Information Technology Act 2000. The Court expressly kept the larger question of law open.

[29] On the unresolved question whether the Schedule requires the hash of the original record, the produced copy, or both, see the divergent academic commentary; the point is, as at the date of writing, unsettled and should be flagged as evolving. , the current state of authority.

6.4 Lessons from Foreign Jurisdictions

The comparative frameworks introduced in Part 3.5 yield two transferable lessons. From the United States, the insight is procedural: a certification regime can be designed to streamline admission while preserving the opponent's right to contest authenticity, rather than operating as an absolute precondition that fails an entire body of evidence on a technical defect. From the European Union, the insight is structural: admissibility rules cannot substitute for a mechanism of cross-border acquisition, and a jurisdiction serious about transnational fraud must legislate the latter. Neither model is to be transplanted wholesale, but each isolates a deficiency in the Indian regime that the reform proposals address.

7. Conclusion and Recommendations

7.1 Summary of Key Findings

This paper has argued that the Bharatiya Sakshya Adhiniyam 2023 is a genuine doctrinal advance whose constitutional foundations are now secure, but whose framework is functionally under-equipped for the distinctive evidentiary realities of digital corporate fraud. The deficiency is not, as the unsuccessful petitioner in Pune Bar Association contended, that the certification regime is too demanding; the Supreme Court has held, correctly, that its safeguards are proportionate. The deficiency is operational and institutional. Section 63's certificate presupposes an identifiable custodian and device that distributed cloud and ERP data routinely lack; the hash-value safeguard secures integrity but not authenticity of origin, leaving the framework exposed to AI-generated fabrication; the statute provides no mechanism for cross-border acquisition; and the pool of qualified certifiers is too small to meet the volume of electronic evidence that modern litigation generates.

7.2 Proposed Recalibration of Section 63 for Distributed-Data and Corporate-Fraud Contexts

The first recommendation is a targeted amendment to Section 63 and its Schedule to accommodate distributed-custody data. Because the constitutional validity of the certification model is settled, the reform should preserve the model while clarifying its operation: who may certify cloud and ERP records where no single custodian exists; how the hash requirement applies to copies derived from a distributed source; and how the Part B expert requirement is satisfied where the relevant data is held by a third-party provider. The object is to make the existing safeguards workable in the environments where corporate-fraud evidence actually resides, not to dilute them.

7.3 A Dedicated Cloud-Forensics Certification Framework

The second recommendation is the creation of a dedicated certification framework for cloud and distributed forensic evidence, defining standardised protocols for acquisition and preservation and expanding, through accreditation, the pool of persons competent to certify under Part B. The Supreme Court's holding that experts need not be confined to Section 79A examiners opens the doctrinal space for such an accreditation regime; what is required is the institutional design to populate it.

7.4 Judicial and Prosecutorial Capacity-Building

The third recommendation addresses the competence gap directly. A framework of this technical complexity requires sustained training of the judiciary and prosecutors in the assessment of digital forensic evidence, and the development of a robust market of accredited experts. This is the reform the Supreme Court's reasoning most directly invites, having located the live problem in the identification and adequacy of qualified experts.

7.5 Direction for Future Research

Two questions merit dedicated study. First, the authenticity-of-origin problem posed by generative technology demands a distinct evidentiary response, since integrity-based safeguards are structurally incapable of detecting fabrication at source. Second, the cross-border acquisition gap invites comparative work on whether an instrument analogous to the European Production Order is feasible and desirable within India's constitutional and treaty framework. Resolving these questions is necessary if the BSA's digital-first promise is to be realised at the intersection — digital corporate fraud — where reliable proof matters most.