

**Swami Vivekananda Advanced Journal for Research and Studies**Online Copy of Document Available on: www.svajrs.com

ISSN:2584-105X

Pg. 106–111



Cybercrime Investigation and Admissibility of Electronic Evidence in India

Apurva Bajpai

Department of Law, Dr. Bhimrao Ambedkar University, Agra, U.P.

Prof. (Dr.) Sanjeev Sharma

Department of Law, Dr. Bhimrao Ambedkar University, Agra, U.P.

Accepted: 20/08/2026**Published: 30/08/2026****DOI: <https://doi.org/10.5281/zenodo.23470234>**

Abstract

Electronic evidence connects cybercrime investigation with adjudication, but legal recognition of digital records does not establish their integrity, authorship or truth. This article examines the Indian framework through a doctrinal analysis of the Bharatiya Sakshya Adhiniyam 2023, the Bharatiya Nagarik Suraksha Sanhita 2023 and the judicial development of electronic-evidence certification. It argues that admissibility should be understood as one stage in an evidentiary process extending from lawful acquisition to meaningful courtroom challenge. Particular attention is given to the savings provision preserving the earlier Evidence Act for specified pending matters, the relationship between primary electronic records and computer output, and the two-part certificate prescribed by section 63. The Supreme Court's May 2026 order in *Pune Bar Association* is examined without treating its qualified observations about expert certification as a final resolution of every interpretive question. The article develops a record-specific approach integrating provenance, documented transformations, appropriately qualified expertise and fair disclosure. It concludes that neither formal certification nor technological verification can replace judicial evaluation: trustworthy electronic proof requires a demonstrable connection between the record collected, the exhibit produced and the factual inference sought.

Keywords: *Electronic Evidence; Cybercrime Investigation; Bharatiya Sakshya Adhiniyam; Section 63 Certificate; Chain of Custody; Digital Forensics*

1. Introduction: From Digital Record to Legal Proof

A cybercrime investigation may generate an abundance of digital material without producing legally persuasive proof. A payment entry, message export or device extraction can be relevant while leaving unresolved whether the material is complete, whether it was altered, and whether the accused authored or controlled it. The recurrent conceptual error is to collapse these questions into the single question of admissibility. This article instead distinguishes *legal admissibility*, *integrity*, *attribution* and *probative weight*. A record may satisfy one dimension while remaining vulnerable on another.

The Bharatiya Sakshya Adhiniyam 2023 (BSA) recognises electronic and digital records and establishes a special framework for proving their contents.¹ Recognition does not dispense with scrutiny. Indeed, treating technology as inherently reliable would invert the justification for certification: safeguards designed to permit trustworthy proof would become reasons to avoid examining it. The article's central question is how investigation and adjudication can be connected so that the courtroom exhibit remains demonstrably linked to its source and can be meaningfully contested.

The methodology is doctrinal, supplemented by a non-binding technical reference on forensic integrity. Statutes, authoritative judicial decisions and official materials available on 22 September 2026 form the research base. No empirical measurements of laboratory capacity or judicial compliance are claimed. The analysis distinguishes the law applicable to saved proceedings from the new statutory framework, identifies questions not conclusively resolved by authority, and advances institutional proposals as proposals rather than existing legal commands. Its contribution is an integrated account of electronic proof, not a catalogue of devices or cybercrime techniques.

2. The Applicable Evidence Regime and the Continuing Role of Precedent

The BSA's commencement did not make every reference to section 65B of the Indian Evidence Act 1872 (IEA) obsolete. Section 170 preserves the earlier regime for the applications, trials, inquiries, investigations, proceedings and appeals specified as pending immediately before commencement.² The governing question is therefore procedural and temporal, not merely whether evidence is tendered

after 1 July 2024. Research that substitutes section 63 for section 65B throughout an older case can erase the very savings rule that determines the applicable law.

Under the IEA, *Anvar PV* treated the special electronic-record provisions as controlling proof of secondary electronic material rather than permitting reliance on ordinary secondary-evidence rules to bypass certification.³ *Arjun Panditrao* reaffirmed that position, overruled the contrary relaxation in *Shafhi Mohammad*, and clarified the treatment of an original device produced and proved by its owner or operator.⁴ These decisions explain the distinction between production of an original record and reliance on computer output. They remain directly material within the saved regime; their reasoning elsewhere must be assessed against the BSA's actual language.

The same jurisprudence also resists a crude opposition between mandatory certification and access to justice. *Arjun Panditrao* addressed defective or withheld certificates through judicial assistance and considered the implications of later production for a fair criminal trial.⁵ The conceptual lesson is that a party's inability to obtain cooperation from a third-party custodian requires procedural attention, not an assumption that the record is either automatically admissible or permanently unusable. Under the BSA, however, this reasoning must be reconciled with the revised certificate language rather than transplanted without analysis.

3. Investigative Acquisition: Authority, Preservation and Scope

The Bharatiya Nagarik Suraksha Sanhita 2023 (BNSS) expressly addresses production of electronic communications and devices through section 94.⁶ A production demand nevertheless needs a defined evidentiary purpose. Requesting a particular transaction history is conceptually different from acquiring every file on a device. The investigator should identify the alleged conduct, the relevant period, the probable source and the relationship between the material sought and the proposition to be proved. This record-specific approach reduces unnecessary collection while making later explanations of provenance more precise.

Section 105 BNSS requires audiovisual recording of the searches and seizures within its stated scope, while section 193(3)(i) requires the police report to address the sequence of custody of an electronic device.⁷ These provisions can complement each other without performing identical functions. A recording

can document what was seized; a custody history can identify subsequent possession and handling. Neither, by itself, establishes that an extracted file is complete or that a displayed conversation was generated by the accused. The source, acquisition process and later transformations must remain separately intelligible.

The forensic process described by the United States National Institute of Standards and Technology distinguishes collection, examination, analysis and reporting, with continuing attention to integrity and custody.⁸ Used here as a technical reference rather than Indian law or a substitute for a criminal-investigation protocol, that distinction helps explain why seizure and examination should not be treated as a single event. Access can change a live system; a working copy may differ from the original storage medium; an exported report may omit information present in the underlying extraction. Each relevant intervention should have an identifiable purpose and documented consequence.

Forensic attendance is not a universal statutory requirement for every cybercrime. Section 176(3) BNSS links its crime-scene provision to offences punishable with seven years or more and to the relevant State notification.⁹ Its application cannot be inferred from the technological character of an allegation alone. An offence carrying a lower maximum sentence may nevertheless raise complex forensic questions. The distinction exposes a policy issue: the need for technical assistance may depend on evidentiary complexity even where the statutory trigger is framed by penal seriousness.

Overseas cloud storage introduces a further separation between legal authority and practical access. Section 112 BNSS provides for judicial requests for evidence abroad.¹⁰ Such a request should seek both the relevant material and the information necessary to explain its extraction and custody. Obtaining a readable file without sufficient contextual records can leave the prosecution with data that cannot adequately establish its own provenance. Conversely, indiscriminate requests for entire accounts may create avoidable privacy disputes and obscure the genuinely relevant evidence.

4. Section 63: Certification, Primary Records and Expert Participation

4.1 The relationship between the record and its output

The BSA expands the treatment of primary electronic evidence in the explanations to section 57,

including specified simultaneous storage and records produced from proper custody, subject to the statutory qualifications.¹¹ Section 63, meanwhile, regulates computer output through conditions concerning regular use, ordinary-course information, operation of the relevant system and reproduction or derivation of the information.¹² These provisions should be read together. Characterising a document as “digital” does not answer whether the exhibit is an original record, an extraction, a converted file or a printout.

The interpretive difficulty is especially visible where a litigant characterises an exported copy as another original because electronic information can exist in several locations. A construction making every copy primary would risk depriving the computer-output safeguards of meaningful operation. The opposite construction, requiring identical treatment for every original and derivative record, would understate the significance of section 57. The appropriate analytical starting point is therefore the exhibit’s actual origin and production history. A reasoned, record-specific ruling is preferable to a categorical exemption based solely on a device being brought to court.

Section 63(4) links the certificate to each instance at which the electronic record is submitted for admission and requires the prescribed identifying and system-related particulars.¹³ This language gives the producer a reason to maintain a stable relationship between the certificate, the source and the particular exhibit. A generic certificate describing “electronic records” cannot usefully explain which export, version or compilation is being tendered. Equally, a certificate’s existence should not be mistaken for proof that the assertions contained in a message are true.

4.2 The Schedule and the qualified 2026 judicial clarification

The Schedule contains Part A for the party and Part B for the expert, with fields identifying the device or digital source, hash values and the associated hash report.¹⁴ The statutory text and form need to be reconciled: a party’s signature cannot responsibly supply factual assertions about a third-party system outside that party’s knowledge. The account of production should identify which person can speak to which process. Independent expertise and operational knowledge serve different evidentiary functions, even when both contribute to the same certificate.

The Supreme Court’s order in *Pune Bar Association*, dated 22 May 2026, is important but requires careful characterisation. The Court found a

rational connection between the hash and expert-certification requirements and the legislation's objective. Reading section 39(1) alongside section 39(2), it observed that a person whose special skill in computer science and cyber forensics is established to the court's satisfaction may also be relevant as an expert. It directed that the Madras High Court's exclusive requirement of a notified section 79A examiner should not be treated as binding. However, it expressly refrained from a conclusive opinion on that issue and kept the question of law open.¹⁵ The order therefore neither supports an exclusive government-laboratory rule nor warrants presenting every privately issued certificate as conclusively sufficient.

The institutional implication is a need to establish competence rather than merely to append a professional label. The court should be able to understand the expert's qualifications, relevant experience, examination undertaken and limitations. Notification under section 79A of the Information Technology Act 2000 has a statutory significance, but the 2026 order makes it particularly important not to conflate that status with an already settled monopoly over Part B certification. Transparent reasons are essential wherever the adequacy of a proposed expert is disputed.

Expert participation nevertheless raises an access problem that formal compliance alone cannot resolve. A requirement applied without attention to cost, availability and the question actually requiring expertise may burden modest claims while adding little explanatory value. The answer is not to dispense with a statutory condition. Rather, institutions should develop accessible certification arrangements and distinguish routine verification from a contested forensic examination. The expert should disclose the material examined, the method used and any dependence on information supplied by the producing party. These proposed safeguards would make expertise answerable to a defined evidentiary task, instead of treating the signature as an independent source of credibility.

5. Integrity, Attribution and the Limits of Technical Assurance

A hash value assists comparison of specified digital data; it is not an account of the historical truth of those data. Suppose an altered recording is first acquired and then hashed. Later matching values may support continuity from acquisition, but they cannot establish that the recording was unaltered beforehand. Likewise,

two differently encoded versions of the same audiovisual content can have different hashes. The legal inference therefore depends on what was hashed, when, using which method, and how the tendered exhibit relates to that object. A hash report should answer a bounded integrity question, not be used as a universal certificate of authenticity.

Custody must also follow the relevant digital objects, not merely the physical device. A log showing that a telephone moved from the police station to a laboratory does not explain how an examiner produced a spreadsheet, selected messages or generated a PDF report. The NIST guidance emphasises documentation of acquisition and handling.¹⁶ Building on that principle, an intelligible production history should identify the source object, acquisition, examination copy and courtroom derivative. Material transformations should be reproducible or adequately explained, with limitations openly stated rather than concealed behind the appearance of precision.

For example, a laboratory may acquire a message database and later generate a searchable PDF for court. Comparing the PDF's hash with the database's hash would address unlike objects, not demonstrate tampering. The appropriate explanation identifies each object separately and documents the extraction and conversion connecting them. Where the conversion suppresses attachments, time-zone information or deleted-entry indicators, its limits should be stated. This hypothetical illustrates why forensic transparency requires an account of transformations, not merely a list of apparently authoritative numerical values.

Attribution remains a separate inquiry. A device's registered owner may not be the operator at the relevant time; a compromised account can transmit a message without its holder's participation. Section 90 BSA itself withholds a presumption about the person who sent an electronic message.¹⁷ This supports disciplined separation between proof that a communication passed through a system and proof that the accused authored it. Corroborative circumstances may resolve the issue, but an attractive screenshot, a contact name or a successfully verified hash cannot independently answer the question of human responsibility.

The probative inquiry must finally consider completeness. A selected exchange may omit replies that alter its meaning; a transaction report may exclude reversals or related entries. These are analytical risks rather than findings that any particular record was manipulated. The evidentiary task is to identify the

relevant whole against which a selection can be evaluated. A certificate can assist proof of the selected material's production without establishing that the selection fairly represents the underlying event.

6. Privacy, Disclosure and Meaningful Adversarial Scrutiny

The privacy principles recognised in *Puttaswamy* require attention to lawful authority, legitimate purpose and proportionality when the State intrudes upon personal information.¹⁸ Applied to digital investigation, those principles support an articulated relationship between the alleged offence and the scope of examination. This is an application of the constitutional framework, not a claim that the judgment prescribed a particular forensic technique. Searching an entire personal archive should not become the unreasoned default merely because the storage medium has been lawfully acquired.

The ability to challenge electronic material is also central to fair adjudication. Section 230 BNSS provides for supply of the specified police-report documents and addresses electronic supply and inspection of voluminous material.¹⁹ It should not be overstated as an unconditional entitlement to every item in every forensic image. Nevertheless, furnishing only a rendered output may leave a material dispute about extraction or completeness unanswered. Depending on the issue and the governing law, controlled inspection, relevant exports or appropriately supervised expert access can reconcile effective challenge with third-party privacy.

Procedural repair should also be distinguished from reconstruction of missing history. A later certificate may explain an adequately recorded production process; it cannot create a contemporaneous record of an undocumented intervention merely by asserting that all procedures were followed. The distinction suggests a proportionate judicial response: identify whether the defect concerns formal presentation, missing operational knowledge or an unexplained alteration, and consider whether further evidence can genuinely answer it. Any opportunity to supplement proof should preserve the opposing party's ability to inspect and respond. This proposed approach accommodates curable defects without converting judicial assistance into permission to assume the integrity of disputed material.

The distinction between admission and weight should remain visible in judicial reasons. A finding

that the production requirements are satisfied does not determine disputed authorship, contextual completeness or credibility. Conversely, a technical objection should identify the defect and its consequence rather than rely on the bare possibility that digital evidence can be altered. Meaningful scrutiny requires both sides to articulate testable propositions: the prosecution must explain the evidentiary chain, and a challenge should engage the particular record and inference rather than technology in the abstract.

7. Institutional Implications and Conclusion

Three institutional measures follow from this analysis. First, investigation files should contain a concise evidence map connecting each source, derivative, certificate and proposed factual inference. Secondly, certificate preparation should begin when the relevant custodian and production process are identifiable, rather than being postponed until an admissibility objection arises. Thirdly, courts should distinguish disputes about source classification, certificate adequacy, expert competence and ultimate evidentiary weight. These measures are proposed working practices; they do not purport to replace statutory requirements or judicial discretion.

Their practical value is that they allocate questions to the persons able to answer them. The seizing officer explains acquisition; the custodian explains the system and production; the expert explains examination and technical limits; and the court determines the permissible inference. An institutional habit of asking one witness to establish all four matters risks obscuring rather than resolving evidentiary gaps. The objective should be an intelligible record of responsibility, not an accumulation of signatures.

The development of Indian electronic-evidence law is therefore neither a simple replacement of section numbers nor a progression towards automatic technological trust. The saved IEA regime, the BSA's primary-record provisions, section 63 and the qualified 2026 order must each be given their proper scope. Reliable adjudication depends on a demonstrable connection between lawful collection, identifiable production, competent explanation and effective challenge. Certification is indispensable where the governing law requires it, but it is not a substitute for proof of authorship or truth. A mature evidentiary framework preserves this distinction throughout the investigation and the trial.

References

1. Bharatiya Sakshya Adhiniyam 2023 (BSA), ss 2(1)(d)-(e) and 61-63.
2. BSA, s 170(2); Ministry of Home Affairs, Notification SO 849(E) (23 February 2024), appointing 1 July 2024 as the commencement date.
3. *Anvar PV v PK Basheer* (2014) 10 SCC 473 [14]-[24].
4. *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1 [72](a)-(b).
5. *Arjun Panditrao* (n 4) [49]-[56].
6. Bharatiya Nagarik Suraksha Sanhita 2023 (BNSS), s 94(1).
7. BNSS, ss 105 and 193(3)(i).
8. Karen Kent and others, *Guide to Integrating Forensic Techniques into Incident Response* (NIST Special Publication 800-86, National Institute of Standards and Technology 2006) 3-1-3-7. The report is a technical reference, not a statement of Indian law.
9. BNSS, s 176(3).
10. BNSS, s 112.
11. BSA, s 57, explanations 4-7.
12. BSA, s 63(1)-(3).
13. BSA, s 63(4).
14. BSA, sch, pts A-B.
15. *Pune Bar Association v Union of India* (Supreme Court, Writ Petition (Civil) No 599 of 2026, 22 May 2026) [4]-[7]. The question concerning expert qualification was expressly left open in para 7.
16. Kent and others (n 8) 3-4-3-5 and 4-6-4-7.
17. BSA, s 90.
18. *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 (DY Chandrachud J).
19. BNSS, s 230 and its provisos.

Disclaimer/Publisher's Note: The views, findings, conclusions, and opinions expressed in articles published in this journal are exclusively those of the individual author(s) and contributor(s). The publisher and/or editorial team neither endorse nor necessarily share these viewpoints. The publisher and/or editors assume no responsibility or liability for any damage, harm, loss, or injury, whether personal or otherwise, that might occur from the use, interpretation, or reliance upon the information, methods, instructions, or products discussed in the journal's content.
