



International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023: Admissibility, Authenticity and Challenges in Criminal Trials

Manudev Patidar

ABSTRACT –

A modern criminal trial rarely proceeds without a phone record, a chat, a CCTV clip or a forensic image of a seized device. The Bharatiya Sakshya Adhiniyam, 2023 (BSA), in force since 1 July 2024, replaced the Indian Evidence Act, 1872 and gave electronic and digital records an express place in the definitions of "document" and "evidence", a clearer rule on primary evidence, and a restructured certificate requirement in section 63 that corresponds to the old section 65B. This paper examines how far the new law resolves the questions that troubled courts for two decades: when an electronic record is admissible, how its authenticity is proved, and what happens when the prescribed certificate is missing or defective. It traces the line from *Anvar P.V.* to Arjun Panditrao Khotkar, analyses the changes made by the BSA and its Schedule (including the requirement of a hash value and an expert's co-signature), and considers chain of custody, expert opinion, presumptions and the constitutional limits of privacy and self-incrimination. It argues that the BSA improves clarity on admissibility but leaves authenticity, the harder problem, to forensic practice and judicial scrutiny, and that deepfakes, cloud data and uneven forensic capacity now strain a framework built around the certificate. The paper concludes with proposals for reform.

Keywords: Bharatiya Sakshya Adhiniyam; electronic evidence; section 63 certificate; authenticity; chain of custody; digital forensics; criminal trial.

1. Introduction

The evidence in a present-day criminal case is as likely to sit on a phone, a server or a surveillance recorder as in a witness's memory. Call detail records place people near a scene, chat messages show intention, CCTV footage shows movement, and forensic images of seized devices show what was deleted. Yet such evidence has an uncomfortable property: it can be altered without a trace by anyone with the right tools, and a court that sees only a printout or a clip cannot tell by looking whether it is genuine. The law of evidence has to solve this problem without either excluding useful material or admitting fabricated material.

India's first answer was section 65B of the Indian Evidence Act, 1872, inserted in 2000. It allowed a computer output to be admitted as a document on conditions and on a certificate from a person responsible for the device. For two decades the Supreme Court swung between treating that certificate as an absolute precondition and as a technicality that could be excused. The Bharatiya Sakshya Adhiniyam, 2023 (BSA), which came into force on 1 July 2024, replaced the 1872 Act and addressed electronic records more directly, in definitions, in the rule on primary evidence, and in a restructured section 63 with a prescribed form of certificate in the Schedule.

This paper asks whether the BSA actually solves the problem that section 65B left behind. Three distinctions shape the inquiry. *Admissibility* asks whether a court may look at the record at all. *Authenticity* asks whether the record is what it claims to be and has not been altered. *Weight* asks how much the court should rely on it once it is in. Statutes and certificates mostly address the first; the second and third depend on forensic practice and judicial judgment. A framework that is strict on admissibility and silent on authenticity can exclude honest evidence on a missing form while admitting a doctored file that carries a correctly completed one.

The argument has three parts. First, the BSA brings real clarity: it treats electronic records as documents, it clarifies primary evidence, and the Supreme Court has recently upheld the new certificate in *Pune Bar Association v. Union of India* (2026). Second, the certificate remains a proxy for authenticity and not a guarantee of it. Third, developments such as synthetic media, cloud storage and cross-border data are testing a framework designed around a single computer in a single place, and the system's real constraint is forensic and institutional capacity.

2. Research design

The study is doctrinal. It reads the text of the BSA, the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) and the Information Technology Act, 2000 (IT Act) together, compares the BSA with the Evidence Act, and analyses the Supreme Court's decisions on electronic evidence from *Anvar P.V.* onward. It does not collect empirical data on forensic laboratory backlogs or on rates of exclusion for want of a certificate; where it refers to practice, it relies on judicial observations and published commentary.

Three questions guide the inquiry.

1. What has the BSA changed in the rules on admissibility and proof of electronic records, and what has it left unchanged?

2. How do courts test authenticity and chain of custody in criminal trials, and does the certificate help or distract?
3. Where does the present framework fail, for example on new technology, constitutional limits or capacity, and what reform is needed?

The scope is criminal trials, although the BSA applies to civil proceedings as well and some of the leading cases arose in civil or election disputes. Section numbers follow the enacted BSA, with the corresponding Evidence Act section noted. Because the Supreme Court decided *Pune Bar Association* only in May 2026, and because the law is moving quickly, the analysis should be read as at October 2026 and checked against later decisions.

3. Conceptual framework

Relevance, admissibility, authenticity and weight. The law of evidence moves a fact through four gates. A fact must be relevant to the issue. It must then be admissible, which means no rule excludes it and, where the fact is a document, the rules on how documents are proved have been followed. It must be authentic, meaning the thing offered is what the party says it is. Finally, the court assigns weight, deciding how far to believe it. Electronic evidence strains every gate, but the second and third are where the law has concentrated, usually in the form of a certificate or an expert report.

Why electronic records are different. Three features set them apart from paper. They are *volatile*: data can be overwritten, auto-deleted or altered by routine use of the device. They are *mutable without visible trace*: a changed file may look identical to the original. And they are *dependent on a system*: a message or log has meaning only in relation to the software, network and clock that produced it. A traditional document can usually be authenticated by a witness who recognises the signature or hand. An electronic record needs proof about a process.

Primary and secondary evidence. The original document is primary evidence, and a copy or oral account of its contents is secondary, to be used only where the original cannot be produced for stated reasons. In the electronic context this distinction is awkward, because a file copied bit by bit is for most purposes identical to the original, and the "original" may be a transient state on a server that nobody can produce in court. The BSA tries to deal with this by deeming certain electronic copies to be primary evidence and by creating a special route for the rest.

Procedure and truth. There is a general tension in rules of this kind. A strict formal rule protects against fabricated evidence and makes admissibility predictable. It can also exclude reliable evidence because someone forgot a form. A flexible approach does the opposite. The Supreme Court's decisions swing between these poles, and the BSA's design is best read as an attempt to move towards the first while adding technical content to the form, the hash value and expert declaration, so that the formality has real forensic substance.

Constitutional overlay. Electronic evidence also raises questions about how it was obtained. A phone seized and searched, a password demanded, a location history requested from a service provider: each engages privacy (*K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1), the privilege against self-incrimination under Article 20(3), and the fair-trial guarantee under Article 21. These are taken up in Part 10.

4. From the Evidence Act to the BSA

The Information Technology Act, 2000 amended the Evidence Act to add section 65B, with sections 22A, 45A, 47A, 65A, 67A, 73A, 85A to 85C, 88A and 90A and a definition of electronic record. For a decade little was litigated. The leading cases then fall into a clear sequence.

Case	Citation	What it held
R.M. Malkani v. State of Maharashtra	(1973) 1 SCC 471	Tape-recorded conversations admissible if relevant, authentic and untampered; courts should be cautious
Ram Singh v. Col. Ram Singh	1985 Supp SCC 611	Conditions for admissibility of recordings: voice identified, accuracy proved, no tampering, relevance
State (NCT of Delhi) v. Navjot Sandhu (Parliament attack case)	(2005) 11 SCC 600	Cell-phone records could be proved by other means even without a section 65B certificate
Anvar P.V. v. P.K. Basheer	(2014) 10 SCC 473	Overruled <i>Navjot Sandhu</i> ; section 65B is a complete code, certificate mandatory for electronic records adduced as secondary evidence
Tomaso Bruno v. State of U.P.	(2015) 7 SCC 178	Adverse inference where available CCTV footage was withheld by the prosecution
Sonu v. State of Haryana	(2017) 8 SCC 570	Objection to admissibility of call records must be raised at trial, not first on appeal
Shafhi Mohammad v. State of H.P.	(2018) 5 SCC 311	Certificate not needed where the party does not hold the device; procedural, relaxable
State of Karnataka v. M.R. Hiremath	(2019) 7 SCC 515	Absence of certificate is curable; a procedural defect
Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal	(2020) 7 SCC 1	Three-judge bench overruled <i>Shafhi</i> ; restored <i>Anvar</i> ; certificate mandatory for secondary electronic evidence, but not where the original device is produced; court may direct production of certificate at the appropriate stage
Pune Bar Association v. Union of India	WP (C) 599/2026, decided 22 May 2026 (2026 SCC OnLine SC 1297)	Upheld section 63(4) BSA and the Schedule; hash value and expert certification are valid safeguards; Part B not confined to section 79A examiners

The pattern is worth stating plainly. The law started in the 1970s with a cautious but flexible approach to recordings, loosened with *Navjot Sandhu*, was

tightened sharply by *Anvar*, loosened again by *Shafhi* and *Hiremath*, and tightened again by *Arjun Panditrao*, which is the pre-BSA law. The BSA was enacted against this background of oscillation. Its drafting choice, to prescribe the form of the certificate and add content to it, is an attempt to end the uncertainty by making the requirement more detailed and more demanding at once.

5. The BSA architecture

The BSA integrates electronic records into the main body of the law and no longer treats them as a special insertion. The table sets out the principal provisions and their Evidence Act counterparts.

BSA provision	Subject	Evidence counterpart	Act What changed
s. 2(1)(d)	"Document"	s. 3	Expressly includes electronic and digital records, emails, server logs, messages, website and locational evidence, voice mail
s. 2(1)(e)	"Evidence"	s. 3	Oral evidence expressly includes statements given electronically
s. 39	Opinions of experts	ss. 45, 45A	Expert opinion in any field; opinion of Examiner of Electronic Evidence (IT Act s. 79A) is relevant
s. 57	Primary evidence	s. 62	Explanations treat multiple stored copies and simultaneous recordings as primary evidence
s. 61	Equal legal effect	New in this form	An electronic or digital record is not to be denied admissibility merely because it is electronic
s. 62	Contents of electronic records	s. 65A	Contents proved in accordance with s. 63
s. 63	Admissibility of electronic records	s. 65B	Deemed document; conditions in s. 63(2); certificate in the form of the Schedule with hash value and an expert's declaration
ss. 85 to 90, 93	Presumptions on electronic agreements, records, signatures, messages and old records	ss. 85A to 85C, 88A, 90A	Largely carried over

Definitions (section 2). The inclusion of electronic and digital records in the definition of "document" matters because it removes any argument that they are a special category outside the main rules. It also makes electronic records capable of being the subject of the presumptions that attach to documents. The extension of "evidence" to cover statements made electronically gives statutory footing to witness examination by video link, which the BNSS develops further.

Primary evidence (section 57). The Explanations to section 57 are among the most practically useful changes. Where an electronic or digital record is created or stored in more than one file, each such file is primary evidence. Where such a record is produced from proper custody, it is primary evidence unless disputed. Where a video recording is simultaneously stored in electronic form and transmitted or transferred, each stored recording is primary evidence. Where a record is stored in multiple storage spaces in a computer resource, each such automated storage, including temporary files, is primary evidence. The upshot is that a party who can produce the device or storage medium on which the record was created may offer it as primary evidence and avoid the certificate regime, a route recognised by the Supreme Court in *Arjun Panditrao* when it said that the certificate is not needed where the original device itself is produced and proved by its owner.

Equal legal effect (section 61). Section 61 directs that nothing in the Adhinyam is to deny admissibility to an electronic or digital record on the ground that it is such a record, and that it has the same legal effect, validity and enforceability as any other document. This is a statement of equality. It does not make electronic records self-proving: section 62 and section 63 then say how the contents are to be shown.

The special rule for secondary electronic evidence (section 63). Where the record is not produced as primary evidence, as is usual with printouts, copies on disc or extracts from a device the party does not control, section 63 treats the information as also a document and admissible without further proof of the original if the section's conditions are met, and the record is accompanied by the prescribed certificate. The conditions in section 63(2) track those of section 65B: the device must have been regularly used for the relevant activities, information of that kind regularly fed into it, the device operating properly, and the information reproduced derived from what was so fed. Part 6 examines the certificate in detail.

Assessment. The architecture is more coherent than the Evidence Act. Electronic records are inside the definitions, primary evidence is clarified, and there is a single route for the rest. The weakness is not in the structure but in what it assumes: that a record produced from a single, identifiable computer resource, by a person who can sign for it, is the typical case.

6. The section 63 certificate and the Schedule

What the BSA requires. Section 63(4) requires that, in any proceeding where a statement in respect of an electronic record is to be given in evidence, a certificate in the form set out in the Schedule must accompany the record. The Schedule has two parts. Part A is to be completed by the party producing the record. It identifies the device or source (computer, storage media, DVR, mobile, flash drive, server, cloud or other), its make, model and identifiers, states that the device was in lawful control and operating properly during the relevant period, and records the hash value of the electronic record. Part B is to be completed by an expert, who certifies the same matters about the record and its hash value.

What is new compared with section 65B. Under the Evidence Act the certificate was signed by a person occupying a responsible position in relation to the device and described the manner of production and the device's operation. The BSA adds two things: a prescribed form, and the requirement of the hash value together with an expert's declaration. The hash value is a short string generated by an algorithm from the contents of a file. If even one bit of the file changes, the hash changes. It therefore serves as a fingerprint that allows later verification that the file produced in court is the file that was collected.

The constitutional challenge. In *Pune Bar Association v. Union of India* (writ petition (civil) 599 of 2026, decided 22 May 2026), a three-judge bench led by the Chief Justice upheld section 63(4) and the Schedule. The petitioners argued that the requirement of a hash value and an expert imposes an undue burden on ordinary litigants. The Court held that a hash value is the equivalent of an electronic fingerprint and a reliable way of identifying and verifying digital data, and that the expert's certification gives an additional layer of authenticity to secondary electronic evidence. It found the requirements neither arbitrary nor unreasonable.

Who can sign Part B. The more practical holding concerns the expert. A Madras High Court decision had read section 39(2) of the BSA, which makes the opinion of an Examiner of Electronic Evidence under section 79A of the IT Act relevant, as meaning that only such notified examiners could sign Part B. The Supreme Court disagreed with that reading, because it overlooked section 39(1), and held that, in addition to notified examiners, a person with special skill and expertise in computer science or cyber forensics may sign Part B if the court is satisfied about their credentials on the basis of unimpeachable material. It said that the Madras view should not be treated as binding precedent. The effect is to avoid a bottleneck: there are very few notified examiners, and a rule that only they could sign would have made the certificate unobtainable in many cases.

Mandatory or curable? Under the Evidence Act the position, after *Arjun Panditrao*, was that the certificate is mandatory for secondary electronic evidence, but that a court may allow it to be produced at a later stage, before the trial is concluded, and may direct a party or an authority to supply it where the device is in their custody. There is no reason to think the BSA changes this. The Supreme Court in *Pune Bar Association* treated the new section as an improvement on, and continuation of, the old regime. The courts, however, are likely to be less indulgent of a certificate that omits the hash value or lacks Part B, since those are the safeguards the Court has said justify the section. A defect in the certificate that goes to the integrity of the record will weigh differently from a missing signature.

Practical difficulties. Four recurring problems should be noted.

- *The certificate describes a process but not the truth of the content.* An expert's declaration can show that a file is the same as the one collected, and not that the statements within it are true or that the person named as sender actually wrote them.
- *Timing of the hash.* A hash generated long after seizure proves only that the file has not changed since the hash was taken. The safeguard is meaningful only if the hash is generated at the time of collection and recorded in the seizure documents.
- *Third-party and opposite-party devices.* Where the record sits on a device or platform controlled by someone else, such as a service provider or the accused, the party relying on it cannot truthfully complete Part A. The courts have dealt with this by directing production, but the form assumes control.
- *Cost and access.* A requirement to obtain a forensic expert's signature for every message or clip adds expense and delay for litigants with limited means, which is the burden the petitioners in *Pune Bar Association* complained of, and the one the Court's flexible reading of "expert" only partly relieves.

7. Authenticity, chain of custody and expert opinion

A correctly completed certificate does not prove that an electronic record is authentic. It proves, at best, that a person with responsibility for the device and an expert say the record was produced as described. Courts still have to decide, on all the evidence, whether the record is what it purports to be. Three tools do most of the work.

Chain of custody. The prosecution needs to show where the device or data was found, who seized it, how it was sealed and stored, who had access, when images were made, and how the data reached the court. Gaps invite the inference that the record was altered. The Supreme Court has repeatedly required this showing for physical exhibits, and the same logic applies, with more force, to data. The BNSS builds some of it into the investigation. Section 105 requires audio-video recording of the process of search and seizure, with the recording sent to the Magistrate. Section 176(3) requires, for offences punishable with seven years or more, that forensic experts visit the scene to collect evidence and that the process be videographed. These provisions are meant to produce a contemporaneous record against which an electronic exhibit can later be tested.

Hash values and forensic imaging. Standard forensic practice is to create a bit-for-bit image of the seized device, using a write-blocker so the original is not changed, and to record the hash of both the original and the image. If the two match, the image is a faithful copy and can be examined without touching the original. Any later change is detectable. The BSA's Schedule writes this practice into the certificate. Its value depends on whether the hash is recorded at the time of seizure and whether the investigating agency documents the tools and procedure. A hash computed for the first time on the eve of trial proves very little about what happened in between.

Expert opinion (section 39). Section 39 admits the opinion of experts on points of science, art or other fields, and treats the opinion of an Examiner of Electronic Evidence under section 79A of the IT Act as relevant. After *Pune Bar Association*, the court may also act on the evidence of a person with special skill in computer science or cyber forensics, if satisfied about their credentials on unimpeachable material. Courts then have to decide how much deference to give. The general rule that an expert's opinion is not binding and must be tested by cross-examination applies, and judges are not forensic scientists. Cross-examining an expert effectively requires the defence to have access to the expert's working material, tools and logs.

Corroboration and internal consistency. In practice, authenticity is often settled by comparing the electronic record with other evidence: a call record against tower data, a chat against a witness's account, a video against the physical scene. Courts have long said that tape recordings and similar material should be received with caution and need corroboration from circumstances (*R.M. Malkani*; *Ram Singh*). That caution is even more appropriate now

that audio and video can be synthesised.

Adverse inference. Where the prosecution has custody of CCTV or other electronic material that would show what happened and does not produce it, the court may draw an adverse inference. In *Tomaso Bruno v. State of U.P.* (2015) 7 SCC 178 the Court criticised the failure to produce available footage and treated it as weakening the prosecution case. The same principle should apply to withholding of call data, logs or device images.

Assessment. The BSA gives courts better statutory tools but does not resolve the underlying difficulty, which is that authenticity is a question of fact answered by forensic work and cross-examination. A trial court that treats the certificate as the end of the inquiry will admit unreliable material, and a court that treats its absence as the end will exclude reliable material. The real discipline comes from the stages before trial: the quality of seizure, imaging and documentation.

8. Presumptions and proof of electronic records

Once an electronic record is admitted, the BSA, like the Evidence Act, provides a set of presumptions that spare the proponent from proving certain matters. They are presumptions of fact or of law about particular categories of record and are generally rebuttable. The BSA carries these over with minor changes in numbering.

Subject	BSA provision (approximate)	Evidence Act counterpart	Effect
Electronic agreements	s. 85	s. 85A	Presumption that an agreement in electronic form concluded by affixing digital signatures is so concluded
Electronic records and electronic signatures	s. 86	s. 85B	Presumption that a secure electronic record has not been altered since a specific time; that a secure electronic signature was affixed by the subscriber with intent to sign
Electronic signature certificates	s. 87	s. 85C	Presumption that the information listed in a certificate is correct
Electronic messages	s. 90	s. 88A	Presumption that a message forwarded by an originator through an electronic mail server corresponds to the message fed into the computer for transmission; no presumption on who sent it
Electronic records five years old	s. 93	s. 90A	Presumption of genuineness where the record is produced from proper custody

Limits of the presumptions. Three points should be noted. First, the presumption of integrity for a "secure" record depends on the record having been secured by a prescribed procedure, which is rarely the case with routine messages or files. Second, the presumption for electronic messages is expressly limited: it presumes that the message corresponds to what was fed into the computer, and not that any named person sent it. Identity of the sender must be proved separately, by phone ownership, SIM registration, account credentials, content or other circumstantial evidence. Third, the presumption for five-year-old records is of limited use in criminal trials, which usually concern recent events.

Burden in criminal cases. The prosecution carries the burden of proving guilt beyond reasonable doubt, and a presumption about the integrity of a record does not relieve it of proving that the accused performed the act. A WhatsApp message established as genuine and unaltered still has to be linked to the accused, through ownership of the number and device, access, content and corroboration. Courts need to insist on that second step in every case.

9. Categories of electronic evidence

Different kinds of electronic evidence raise different problems. The table summarises the typical route to admission and the usual points of attack, and the paragraphs below take the main categories in turn.

Category	Usual route to admission	Typical defence challenge
CCTV and surveillance footage	Original DVR produced with owner's evidence (primary), or certificate for a copy	Gaps and overwriting; time-stamp accuracy; identification from poor images
Call detail records and tower data	Certificate from the service provider; evidence of its officer	Certificate missing or by wrong person; tower location is approximate; objection raised too late
Emails, chats, social media	Certificate with hash for extracts; device or account evidence	Authorship; account access by others; edited screenshots
Audio and video recordings	Voice identification; source device; certificate for copies	Editing; poor audibility; consent and legality of recording
Location and app data	Provider disclosures; forensic extraction from device	Accuracy; cloud and foreign servers; reliance on automated inference
Forensic images of seized devices	Examiner's report with hash; chain of custody	Integrity of imaging; contamination; access to tools and logs

CCTV and surveillance. If the prosecution produces the original recorder and a witness who can speak to its operation, the footage is primary evidence and no certificate is needed. Where only a copy is produced, a certificate is required. The recurring practical problem is the retention period of

recorders, which routinely overwrite recordings within days or weeks. Prompt seizure and imaging are therefore decisive. A failure to preserve available footage can lead to an adverse inference (*Tomaso Bruno*).

Call detail records and tower data. Courts rely heavily on these to place persons and establish links. The records are produced by the service provider, and the certificate should come from a person in a responsible position there. In *Sonu v. State of Haryana* (2017) 8 SCC 570 the Court held that an objection that the certificate was missing cannot be raised for the first time on appeal when the evidence was received at trial without objection, because the defect might have been cured had it been raised. Tower location data is approximate and should be treated as indicative, not as precise proof of position.

Emails, messaging and social media. For a chat or post, the record is usually a screenshot or an extract from a seized phone. A screenshot, standing alone, proves little, since it can be edited and shows nothing of metadata. Proper proof involves a forensic extraction from the device or account, the hash, and evidence linking the account or number to the accused. The presumption in section 90 applies only to the correspondence of the message with what was fed into the system, not to authorship.

Audio and video recordings. The established rule is that a recording is admissible if relevant, if the voice is identified, if the recording is shown to be accurate and not tampered with, and if the original is produced or accounted for (*Ram Singh*). The BNSS also allows the court to direct an accused or witness to give a voice sample (section 349) without the need for an arrest. A recording obtained by a participant is generally admissible, though the manner of obtaining it may affect its weight.

Location and app data, and device extractions. Data from mobile applications, wearable devices, vehicle systems and cloud accounts raise new difficulties: the data is often held by foreign companies, is generated automatically and may be a probabilistic inference and not a recorded fact. Courts will increasingly need to understand how a particular figure was generated before relying on it.

Electronic proceedings. The BNSS permits many steps, including examination of witnesses, to be conducted through audio-video electronic means (section 530 and related provisions), and the BSA's definition of evidence recognises statements given electronically. This widens access but requires standards for identity verification, absence of coaching, and security of the link.

10. Constitutional dimensions

The rules on admissibility say what a court may accept. Another body of law governs how the material may be collected.

Privacy. After *Puttaswamy*, a person's phone, cloud account and communications fall within the zone of privacy, and any intrusion must satisfy legality, a legitimate aim and proportionality. A mobile phone holds a very large amount of personal information, and searching one is not like searching a pocket. The BNSS lets a court or officer require production of documents and things, expressly including electronic communication devices and digital evidence (section 94), and permits seizure under section 106 and search with recording under section 105. The text gives no specific limit on scope, retention or return of imaged data. Courts will have to supply proportionality by requiring that demands for devices be tied to the offence and by limiting examination to relevant data.

Self-incrimination and compelled access. Article 20(3) protects an accused from being compelled to be a witness against themselves. In *Selvi v. State of Karnataka* (2010) 7 SCC 263 the Court held that narco-analysis, brain mapping and polygraph tests, if compelled, violate that protection, and distinguished physical samples. Whether compelling a suspect to disclose a password, or to unlock a device by fingerprint or face, is testimonial is unsettled in India. Some High Courts have addressed it, usually allowing biometric unlocking as analogous to a physical sample while treating disclosure of a passcode as closer to testimony, but there is no authoritative Supreme Court ruling. Voice samples were held to be obtainable without violating Article 20(3) in *Ritesh Sinha v. State of U.P.* (2019) 8 SCC 1, and the BNSS now provides for them expressly.

Evidence obtained illegally. Indian law has traditionally admitted relevant evidence even when obtained by an irregular search, subject to the court's discretion and to constitutional limits (*R.M. Malkani*). Electronic evidence intensifies the issue because a single device can yield a large mass of unrelated private data. The better approach, which Indian courts have not yet clearly adopted, is to look at the seriousness of the violation and whether the privacy intrusion was proportionate in deciding whether to exclude or to discount the material.

Fair trial and equality of arms. The accused is entitled to a fair opportunity to challenge electronic evidence. That includes timely access to the forensic image, the hash report, the tools used and the expert's working notes. The BNSS provides for supply of documents to the accused, including in electronic form, but it does not say that the accused must receive a working copy of the seized data or access to independent forensic examination. Without this, the defence cannot test the prosecution's expert, and the statutory safeguard of the hash becomes a one-way assurance.

11. Challenges

Synthetic media and deepfakes. The BSA's certificate model assumes that the main risk is that a genuine record has been altered after creation. It does not address the risk that the record was fabricated from the start. A hash computed on a deepfake video proves only that the same deepfake was presented in court. As voice cloning and video synthesis become cheap, the court's reliance on a certificate may become a source of false assurance. The answer lies in provenance: where and when the recording was first made, on what device, with what metadata, and whether independent sources corroborate it. These questions go to authenticity and weight, and not to the certificate. Courts will need access to detection experts and should be slow to treat recordings, especially of a single contested conversation, as self-proving.

Cloud, platform and cross-border data. The certificate presupposes a device and a person in control of it. Much modern evidence sits in accounts held by foreign companies, spread across servers in several countries, and accessible to the user only through an application. A person who relies on a

message in a cloud-based service may not be able to say anything about the "computer" that produced it. The BNSS provides for requests to foreign authorities, and mutual legal assistance treaties exist, but the process is slow and the data may be deleted or unavailable before it arrives. The BSA has not created a mechanism for certifying records obtained directly from a platform, such as a standard certificate from the service provider's officer, and practice is likely to develop by improvisation.

Forensic capacity. The entire system depends on forensic examiners, tools and laboratories. The number of examiners notified under section 79A of the IT Act is small, and State forensic laboratories, where they exist, carry large backlogs. The Supreme Court's flexible reading of Part B in *Pune Bar Association* reduces the bottleneck, but widens the field of those who may sign, and with it the burden on the trial judge to assess their credentials. The risk is that the quality of electronic proof will vary sharply between a well-resourced metropolitan court and a district court with no access to an examiner.

Formalism. The certificate is a form, and forms attract technical objections. Experience under section 65B shows the risk: cases decided on whether a certificate was signed by the right person or filed at the right time, rather than on whether the record was genuine. The Court's attempt in *Arjun Panditrao* to allow later production and judicial direction was a response to this problem, and the BSA's more detailed form increases the chances of defects. A mechanism to cure formal defects, with the court satisfying itself on authenticity by other means, would protect against excluding sound evidence.

Unequal access and the defence. The prosecution generally controls the seized devices and the forensic work. Unless the accused is given an effective way to obtain a copy of the data and to have it independently examined, the safeguards are asymmetrical. This is a fair-trial issue and not only a matter of convenience.

Privacy and over-collection. The ability to seize and image a whole device encourages collection of far more than the investigation needs. Without rules on scope, retention, deletion and return of data, the electronic evidence regime risks becoming a surveillance regime.

Judicial familiarity. Many trial courts handle electronic evidence through the same habits as paper: marking an exhibit, taking a printout, accepting a certificate. Training judges and prosecutors on digital basics is, in the end, as important as the text of section 63.

Assessment. Taken together, these challenges show that the BSA's response to electronic evidence is better at the entry stage than at the verification stage. It tells parties what to file. It does not tell courts how to be sure.

12. Recommendations

For Parliament and rule-making authorities

1. Provide a short statutory or rule-based procedure for curing defects in the section 63 certificate, so that a court may admit a record where authenticity is otherwise established, while keeping the hash value and expert declaration as the default.
2. Notify minimum qualifications for experts who may sign Part B, and publish a register of accredited forensic examiners, so that courts do not have to assess credentials from scratch in every case.
3. Provide a standard certificate for records obtained from online platforms and service providers, signed by a responsible officer of the provider, to supplement the device-centred Schedule.
4. Add rules on collection and handling of digital evidence: scope of searches of devices, retention periods, deletion of irrelevant data and return of devices, guided by proportionality.
5. Provide that the accused is entitled to a working forensic copy of seized data, and to independent examination at public cost where the accused is unable to afford it.
6. Consider specific provisions on synthetic media, requiring a party who relies on a contested recording to show provenance, and permitting courts to call for detection expertise.

For courts

7. Treat the certificate as a gateway to admissibility and not as proof of authenticity. Require the prosecution to show chain of custody, the time and manner of hashing and the link between the record and the accused.
8. Require records of seizure and imaging to be placed on the file, using the video recording and forensic visit under the BNSS, and draw adverse inferences where available electronic evidence is withheld.
9. Decide admissibility objections at the time the evidence is tendered, so that defects can be cured while a remedy is available, and refuse belated objections that could have been cured (*Sonu*).
10. Treat tower data, screenshots and automated app inferences as indicative, not conclusive, unless supported by corroboration.

For the executive and the judiciary's administration

11. Expand the number of notified examiners and forensic laboratories, publish backlog data, and establish district-level forensic access.
12. Standardise seizure protocols for police, including write-blocking, imaging, hashing at the scene and logging, and train police, prosecutors and judges on them.
13. Require time-bound preservation of CCTV and other volatile data in public places and public offices, and set clear rules on retention periods.

13. Conclusion

The Bharatiya Sakshya Adhiniyam made electronic evidence a regular part of the law of proof. It places electronic and digital records in the definition of a document, clarifies when a copy is primary evidence, states that electronic records are not to be denied effect because of their form, and prescribes a standard certificate with a hash value and an expert's declaration for secondary records. The Supreme Court's decision in *Pune Bar Association v. Union of India* in May 2026 has confirmed the validity of that scheme and eased its most awkward requirement by allowing qualified forensic experts, and not only notified examiners, to sign Part B.

That is real progress on admissibility. Parties now know what to file, and courts have a statutory basis for requiring more than a printout. But the more difficult question is authenticity, and the BSA's answer, a certificate, is a procedural proxy. A certificate can show that a file is the one that was collected, and cannot show that it was genuine when collected, that the statements in it are true, or that the person named wrote them. Deepfakes, cloud data, cross-border platforms and uneven forensic capacity all press on that gap.

The next phase of reform should therefore shift from form to substance: standard procedures for collection and imaging, accredited experts, defence access to data, rules on privacy and retention, a curative mechanism for technical defects, and courts that test provenance and chain of custody and do not rest on the certificate. If this is done, the Adhiniyam's attention to electronic records can make criminal trials both fairer and more reliable. If it is not, the risk is that the certificate becomes the new ritual, easy to produce and hard to rely on.

REFERENCES

Statutes and constitutional provisions. Bharatiya Sakshya Adhiniyam, 2023, sections 2(1)(d), 2(1)(e), 39, 57, 61, 62, 63, 85 to 90, 93 and the Schedule. Indian Evidence Act, 1872, sections 22A, 45A, 62, 65A, 65B, 85A to 85C, 88A and 90A. Bharatiya Nagarik Suraksha Sanhita, 2023, sections 94, 105, 106, 176, 349 and 530. Information Technology Act, 2000, section 79A. Constitution of India, Articles 20(3) and 21.

Cases cited.

Case	Citation	Point
R.M. Malkani v. State of Maharashtra	(1973) 1 SCC 471	Tape recordings; caution; illegally obtained evidence
Ram Singh v. Col. Ram Singh	1985 Supp SCC 611	Conditions for admissibility of recordings
Selvi v. State of Karnataka	(2010) 7 SCC 263	Compelled scientific tests and Article 20(3)
State (NCT of Delhi) v. Navjot Sandhu	(2005) 11 SCC 600	Cell-phone records without certificate (overruled)
Anvar P.V. v. P.K. Basheer	(2014) 10 SCC 473	Section 65B certificate mandatory
Tomaso Bruno v. State of U.P.	(2015) 7 SCC 178	CCTV footage; adverse inference
K.S. Puttaswamy v. Union of India	(2017) 10 SCC 1	Privacy
Sonu v. State of Haryana	(2017) 8 SCC 570	Timing of objection to call records
Shafhi Mohammad v. State of H.P.	(2018) 5 SCC 311	Certificate relaxed (overruled)
State of Karnataka v. M.R. Hiremath	(2019) 7 SCC 515	Certificate defect curable
Ritesh Sinha v. State of U.P.	(2019) 8 SCC 1	Voice samples
Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal	(2020) 7 SCC 1	Certificate mandatory; production of original device
Pune Bar Association v. Union of India	WP (C) 599/2026, decided 22 May 2026; 2026 SCC OnLine SC 1297	Validity of s. 63(4) BSA; Part B expert

Secondary sources consulted for recent developments.

- [Hash value is an electronic fingerprint; Section 63\(4\) BSA certificate requirement is valid: Supreme Court](#) (SCC Online Blog, 8 July 2026)
- [Supreme Court Rejects Challenge To S.63\(4\) BSA Mandating Hash Value Disclosure For Electronic Evidence](#) (LiveLaw, 2026 LiveLaw (SC) 551)
- [Expert in computer science and cyber forensics competent to sign Section 63\(4\) BSA certificate](#) (Verdictum, 28 May 2026)
- [Supreme Court of India clarifies scope of expert certification under Section 63\(4\) BSA](#) (JSA Prism, June 2026)
- [Section 63\(4\) BSA: Supreme Court clarifies that Part B is not confined to Section 79A examiners](#) (LawWeb, 28 May 2026)
- [Pune Bar Association v. Union of India, order of 22 May 2026](#)
- [Unseen Burden of Electronic Evidence](#) (LiveLaw)
- [How to fulfill requirements of admissibility of electronic evidence under the BSA](#) (LiveLaw)