IOSR Journal of Multidisciplinary Research (IOSR -JMR)
ISSN: 3048-7439 Volume 3, Issue 5, Series 1, Sep. - Oct. (2026), PP 34-44
www.iosrjournals.org

Admissibility and Reliability of Digital Evidence in Indian Criminal Proceedings: A Doctrinal Analysis of Legal Frameworks and Judicial Developments

Quanta Saikia, LLM
Department of Juridical Studies, Mahapurusha Srimanta Sankaradeva Vishwavidyalaya, Guwahati Unit.
Orchid id :0009-0009-1220-3861

Abstract
The proliferation of digital technology has transformed the character of evidence produced before criminal courts in India, with mobile-phone data, CCTV recordings, electronic messages, emails and social-media content increasingly forming the backbone of the prosecution and defence case alike. Unlike conventional documentary or oral evidence, digital evidence is intangible, easily duplicable and vulnerable to alteration, which raises distinct questions of authenticity, integrity and evidentiary weight. This paper undertakes a doctrinal analysis of the legal framework governing the admissibility and reliability of digital evidence in Indian criminal proceedings, with particular reference to the Bharatiya Sakshya Adhiniyam, 2023 (BSA), which replaced the Indian Evidence Act, 1872 with effect from 1 July 2024 (Bharatiya Sakshya Adhiniyam, 2023). The study traces the statutory evolution from Section 65B of the former Evidence Act to Sections 61–63 of the BSA, and examines the doctrinal trajectory of judicial pronouncements, beginning with State (NCT of Delhi) v. Navjot Sandhu (2005), through Anvar P.V. v. P.K. Basheer (2014), Tomaso Bruno v. State of Uttar Pradesh (2015) and Shafhi Mohammad v. State of Himachal Pradesh, (2018), culminating in the authoritative restatement of the law by a three-judge bench in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020). Employing a doctrinal methodology based on statutes, judicial decisions and secondary legal literature, the paper identifies the continuing centrality of certification requirements, the practical difficulties of chain-of-custody preservation, the shortage of trained forensic personnel, and the emerging challenge posed by deepfakes and synthetically generated media (Legal Service India, 2026a; Mondaq, 2026a). The paper concludes that while the BSA has consolidated and clarified the statutory position, the evidentiary value of digital material continues to depend not on its electronic character alone but on demonstrable authenticity, integrity and statutory compliance, and it proposes measures to strengthen forensic infrastructure, judicial training and procedural safeguards.

Keywords: *Digital Evidence, Criminal Proceedings, Bharatiya Sakshya Adhiniyam, Judicial Developments, Digital Forensics*

Date of Submission: 31-08-2026 Date of Acceptance: 07-09-2026

I. Introduction

The investigation and adjudication of crime in India have undergone a decisive shift over the past two decades on account of the pervasive presence of digital devices and networked communication in everyday life. Mobile telephones, closed-circuit television (CCTV) systems, electronic mail, instant-messaging applications such as WhatsApp, social-media platforms, global positioning system (GPS) and cell-tower location data, and cloud-based storage now routinely generate material that is directly relevant to establishing the facts in issue in a criminal trial. Investigating agencies increasingly rely on call-detail records, chat logs and surveillance footage to establish presence, association, motive and sequence of events, while courts are called upon with growing frequency to determine whether such material has been properly proved and may safely be relied upon.

Digital evidence differs from traditional documentary or oral evidence in several material respects. It is intangible in its native form and requires an intermediating device or software to be perceived; it can be copied without any loss of apparent quality, making it difficult to distinguish an original from a copy; it can be altered, spliced or fabricated without leaving obvious physical traces; and its evidentiary value is frequently bound up with metadata, hash values and technical processes that are unfamiliar to lawyers, judges and, at times, investigators. These characteristics generate a distinct set of legal problems concerning authenticity (whether the record is what it purports to be) and reliability (whether the process by which it was generated, stored and produced in court inspires sufficient confidence to be acted upon).

Indian courts have grappled with these questions for over two decades, producing a body of case law marked by significant doctrinal oscillation, particularly around the certification requirement earlier contained in

Section 65B of the Indian Evidence Act, 1872 (Anvar P.V. v. P.K. Basheer, 2014; Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, 2020; State (NCT of Delhi) v. Navjot Sandhu, 2005). The enactment of the Bharatiya Sakshya Adhiniyam, 2023, which came into force on 1 July 2024 as part of a broader overhaul of India's criminal law statutes alongside the Bharatiya Nyaya Sanhita, 2023 and the Bharatiya Nagarik Suraksha Sanhita, 2023, provided an opportunity to consolidate and refine this framework (Bharatiya Sakshya Adhiniyam, 2023). Sections 61 to 63 of the BSA now form the principal statutory basis for the admissibility of electronic and digital records in criminal proceedings (Bharatiya Sakshya Adhiniyam, 2023, ss. 61–63). At the same time, the emergence of new technological threats most notably deepfakes and other forms of synthetically generated media has introduced fresh doctrinal and practical challenges that the existing framework was not originally designed to address (Mondaq, 2026a). Against this background, a systematic doctrinal examination of the legal architecture governing digital evidence, read together with the relevant judicial developments and existing scholarship, is both timely and necessary.

II. Review of Literature

A fair amount has now been written on the BSA's treatment of digital evidence, and it is worth pausing to see where this literature agrees, where it pulls in different directions, and what it leaves unanswered before turning to the statute and the case law in detail.

Comparative doctrinal studies. Anthal (2025) compares the BSA's admissibility provisions with those of the erstwhile Indian Evidence Act, 1872, and finds that the new statute keeps the substance of the old certification regime intact, even as it places digital evidence within a wider regulatory landscape that now also touches cybersecurity and data governance. Ganguli (2024) reaches much the same conclusion from a slightly different angle: renumbering and minor drafting changes aside, the certification-based architecture inherited from Section 65B has carried over largely unchanged, which is why the pre-BSA case law still matters for interpreting Sections 61 to 63.

Forensic and technical standards. Bharati and Nagarale (2025) look at the same transition from the forensic side. They note that treating electronic records as being on the same footing as paper documents does simplify how such evidence is submitted, but it also raises the stakes for forensic verification, since a court now has less reason to treat a printout or a copied file with automatic suspicion and more reason to ask whether it was properly examined. This is a useful reminder, taken up again in Section 8 of this paper, that admissibility and technical reliability are not the same question.

Constitutional and procedural critique. Kanishka and Sharma (2026) are more cautious about how much the BSA actually changes in practice. Their reading is that the statute reflects a genuine intent to accommodate digital records, but that authenticity disputes, gaps in chain of custody, and the risk of manipulation remain live problems that no amount of drafting can fix on its own the outcome, in their view, depends far more on judicial interpretation and institutional capacity than on the text of Sections 61 to 63. A similarly cautious note is struck in a doctrinal review published in the Indian Journal of Law (2026), which walks through the statutory pathway to admissibility and points out that authentication is, in the end, a fact-specific exercise that a certificate can support but not replace.

Intersection with data-protection law. A newer strand of writing places digital evidence law alongside the Digital Personal Data Protection Act, 2023. A study in the GLS Law Journal (2026) flags a genuine tension here: investigators want to collect and retain as much electronic material as might later prove relevant, while data-protection law pushes the other way, toward collecting only what is necessary and for a stated purpose. The paper suggests the two regimes will have to be read together as enforcement practice develops, since neither is likely to yield outright to the other.

Forensic infrastructure and chain of custody. A separate strand of writing looks past the statute book to the practical machinery through which digital evidence actually reaches a courtroom. Wahab (2026) surveys the role of central and state forensic science laboratories and notes that these institutions remain the practical bottleneck through which almost all contested digital material must pass before certification. This is borne out by recent commentary on staffing at India's forensic laboratories, which points to a large share of sanctioned scientific posts lying vacant and calls for statutory turnaround timelines for forensic reports (Budding Forensic Expert, 2026b). A related piece goes further and argues that chain-of-custody failures, rather than any shortage of evidence as such, are what most often cause forensic material to be thrown out at trial, and that India still has no uniform national protocol for documenting custody (Budding Forensic Expert, 2026a). Writing on the same theme, Legal Service India (2026b) sets out the collection, hashing and write-blocking steps that investigators are expected to follow to keep an electronic record intact, while Srishti (2025) and Legal Blur (2026) both observe that the new criminal codes place greater demands on forensic capacity than the system currently has the staff and laboratories to meet.

Deepfakes and synthetic media. The most recent literature has begun to grapple with content that is not merely altered but generated outright. With the notification of the Information Technology (Intermediary Guidelines and

Digital Media Ethics Code) Amendment Rules, 2026, which impose labelling and traceability obligations on "synthetically generated information" and a three-hour takedown window for certain categories of harmful AI content, commentators have started to ask how this new regulatory layer interacts with the certification regime under Section 63 (Mondaq, 2026a). Mondaq (2026b) makes the point squarely: a deepfake is not automatically inadmissible, since it is treated as an ordinary electronic record for evidentiary purposes, but proving its authenticity is harder, and traceability logs generated under the IT Rules may in time become a useful, though not a substitute, source of corroboration. Legal Service India (2026a) documents a related but distinct line of cases, in which the Delhi and Bombay High Courts have granted interim injunctions against unauthorised deepfakes of well-known individuals on personality-rights grounds, illustrating that Indian courts are already handling synthetic-media disputes even in the absence of a dedicated evidentiary provision for them.

Read together, this literature points to the same conclusion from several directions: the certification jurisprudence built up under Section 65B has carried over into Sections 61 to 63 of the BSA more or less intact, and the harder problems now lie outside the statute itself, in forensic capacity, judicial familiarity with technical concepts, and the treatment of synthetic media. A bibliometric study of research output on digital evidence more generally has also noted that scholarship in this area has grown quickly but remains fragmented across disciplines, with legal and forensic-science literature rarely citing each other (Chhatrapati et al., 2021) — a pattern that shows up in the Indian material surveyed here as well. What the existing studies tend not to do is bring these strands together. Comparative drafting studies, forensic-standards commentary, data-protection analyses and deepfake writing have so far developed largely in parallel, each addressing one piece of the picture. This paper tries to close that gap by reading the case law from Navjot Sandhu (2005) to Arjun Panditrao Khotkar (2020) against the BSA framework and the more recent literature together, and by drawing out reform measures that follow from doing so.

III. Objectives of the Study

1. To examine the legal framework governing the admissibility of digital evidence in Indian criminal proceedings.
2. To analyse the requirements for authentication and proof of electronic records under the Bharatiya Sakshya Adhiniyam, 2023.
3. To examine the judicial approach towards digital evidence, tracing its doctrinal evolution through leading Supreme Court decisions.
4. To identify major challenges concerning the reliability and integrity of digital evidence in contemporary criminal practice.
5. To suggest measures for strengthening the evidentiary framework for digital evidence in India.

IV. Research Questions

1. What legal requirements govern the admissibility of digital evidence in Indian criminal proceedings?
2. How does the Bharatiya Sakshya Adhiniyam, 2023 regulate electronic and digital records?
3. How have Indian courts interpreted the requirements relating to authentication and certification of electronic evidence?
4. What factors affect the reliability and evidentiary value of digital evidence?
5. What legal and procedural reforms can strengthen the use of digital evidence in criminal trials?

V. Research Methodology

This paper adopts a doctrinal legal research methodology and relies exclusively on secondary sources of law. No primary data, survey, questionnaire, interview or experimental material has been collected or is presented in this study; the analysis is confined to statutory text, judicial precedent and published legal scholarship. The following categories of sources have been examined:

- The Bharatiya Sakshya Adhiniyam, 2023, particularly Sections 56 to 66, which deal with documentary evidence, electronic records and their proof (Bharatiya Sakshya Adhiniyam, 2023).
- The Bharatiya Nagarik Suraksha Sanhita, 2023, insofar as it bears upon investigation, search, seizure and forensic examination of digital material (Bharatiya Nagarik Suraksha Sanhita, 2023).
- The Information Technology Act, 2000, which first extended legal recognition to electronic records and digital signatures in India (Information Technology Act, 2000).
- Reported decisions of the Supreme Court of India and High Courts on the admissibility, certification and evidentiary weight of electronic records.
- Government reports and materials published by law-related institutions and forensic bodies (National Crime Records Bureau, n.d.).
- Peer-reviewed legal journals, law-review articles and doctrinal commentary, including recent scholarship on the statutory transition to the BSA, on forensic infrastructure, and on deepfakes and synthetic media as evidence (Anthal, 2025; Bharati & Nagarale, 2025; Budding Forensic Expert, 2026a, 2026b; Ganguli, 2024; GLS Law

Journal, 2026; Indian Journal of Law, 2026; Kanishka & Sharma, 2026; Legal Service India, 2026a, 2026b; Mondaq, 2026a, 2026b; Wahab, 2026).

The doctrinal method has been adopted because the research questions concern the interpretation and systematisation of legal rules rather than the measurement of social behaviour; a doctrinal approach is therefore the method best suited to mapping statutory text onto judicial interpretation and identifying areas of continuing uncertainty. The BSA came into force on 1 July 2024, and Sections 61 to 63 thereof are the provisions most directly relevant to the admissibility of electronic and digital records (Bharatiya Sakshya Adhiniyam, 2023, ss. 61–63); these are analysed together with the corresponding line of authority developed under the predecessor provision, Section 65B of the Indian Evidence Act, 1872, which continues to inform the interpretation of the new provisions (Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, 2020).

VI. Concept of Digital Evidence

Digital evidence may be understood as any probative information that is stored, transmitted or received in binary form and that is capable of being used to establish a fact in issue. It is a species of the wider category of electronic evidence, which itself falls within the still broader statutory category of a "document." Under the BSA, an electronic or digital record is expressly brought within the definition of a document, and Illustration (vi) to the definition clause specifically recognises emails, server logs, documents stored on computers, laptops or smartphones, messages, websites and voicemail messages as documents for evidentiary purposes (Bharatiya Sakshya Adhiniyam, 2023, s. 2, illus. vi).

Digital evidence encountered in Indian criminal proceedings today spans a wide and continually expanding range of sources, including CCTV and surveillance footage, mobile-phone data such as call records, SMS and application data, instant-messaging and chat records including WhatsApp and similar platforms, electronic mail, social-media content, audio and video recordings, GPS and cell-tower location data, files stored on computers and external storage media, and data held on remote or cloud-based servers. Each of these categories raises overlapping but not identical evidentiary concerns: CCTV footage, for instance, is frequently challenged on grounds of continuity and chain of custody (Tomaso Bruno v. State of Uttar Pradesh, 2015), while chat and social-media evidence more often raises questions of attribution — that is, whether the record can reliably be linked to the person alleged to have authored it. What is common across all these categories, however, is that the record cannot be perceived directly by the court; it must be reproduced through a device or intermediary process, and it is this feature that has historically justified special statutory treatment distinct from the ordinary rules for documentary evidence.

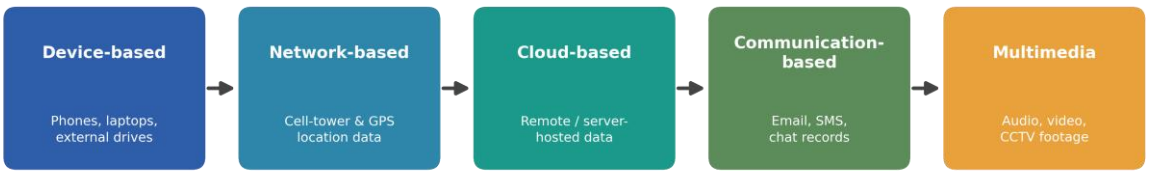

Figure 1. Classification of Digital Evidence

VII. Legal Framework in India

7.1 Historical Background: The Indian Evidence Act, 1872 and the Information Technology Act, 2000

The Indian Evidence Act, 1872, in its original form, made no provision for electronic records, since it predated the existence of computers by more than a century. Recognition of electronic documents was introduced only through consequential amendments made by the Information Technology Act, 2000, which inserted Sections 65A and 65B into the Evidence Act to govern the special procedure for proving the contents of electronic records (Information Technology Act, 2000). Section 65B required that secondary evidence of an electronic record be accompanied by a certificate, executed by a person occupying a responsible official position in relation to the device, attesting to specified conditions concerning the regular use of the device and the manner in which the record was produced. This certificate requirement, intended to safeguard against the ease with which digital material can be altered, became the focal point of over two decades of judicial controversy, discussed in Section 9 below.

7.2 The Bharatiya Sakshya Adhiniyam, 2023

of electronic signatures, extending the certification-based approach to digitally signed records (Bharatiya Sakshya Adhiniyam, 2023, s. 66). Read together, Sections 61 to 63 and 66 form a The Bharatiya Sakshya Adhiniyam, 2023 received presidential assent on 25 December 2023 and came into force on 1 July 2024, repealing the Indian Evidence Act, 1872 in its entirety (Bharatiya Sakshya Adhiniyam, 2023). The BSA retains the substantive architecture of the earlier certification regime while consolidating and refining it. Three provisions are of particular significance for digital evidence in criminal proceedings.

Section 61 provides that nothing in the Adhiniyam shall be used to deny the admissibility of an electronic or digital record merely on the ground that it is electronic or digital, and that such a record shall, subject to Section 63, have the same legal effect, validity and enforceability as any other document (Bharatiya Sakshya Adhiniyam, 2023, s. 61). This is essentially a non-discrimination clause: it places an electronic record on the same evidentiary footing as a paper document, subject to compliance with the specific conditions in Section 63.

Section 62 provides that the contents of an electronic record may be proved in accordance with Section 63, thereby linking the general recognition of electronic records in Section 61 to the specific procedural conditions that follow (Bharatiya Sakshya Adhiniyam, 2023, s. 62).

Section 63 is the operative provision governing admissibility. It provides that information contained in an electronic record — whether printed on paper, stored or copied on optical or magnetic media or semiconductor memory, or otherwise produced by a computer or communication device is deemed to be a document and is admissible without further proof or production of the original, provided the conditions specified in the section are satisfied (Bharatiya Sakshya Adhiniyam, 2023, s. 63). Sub-section (4) requires that a certificate be furnished along with the electronic record at each instance it is submitted for admission, identifying the record, describing the manner of its production, and giving particulars of the device involved (Bharatiya Sakshya Adhiniyam, 2023, s. 63(4)). Section 63, as commonly construed, contemplates certification by the person responsible for the operation of the relevant device and, in specified circumstances, by an independent expert, together with the inclusion of hash-value information in the certificate schedule a refinement intended to strengthen the technical assurance of integrity that the certificate provides (Bharatiya Sakshya Adhiniyam, 2023, sch.).

Section 66 of the BSA deals with proof coherent scheme: electronic records are not to be treated as inherently suspect, but their admission as substantive proof without production of the original is conditioned on compliance with a certification mechanism designed to establish the integrity of the process by which the record was generated and preserved.

Table 1. Evolution of the Legal Framework Governing Electronic Evidence in India

Period/Statute	Key Provision	Core Requirement
Indian Evidence Act, 1872 (original)	No specific provision	Electronic records not contemplated; general rules of documentary evidence applied by analogy
Information Technology Act, 2000 (amendments)	Sections 65A & 65B inserted into the Evidence Act	Special procedure for secondary evidence of electronic records; certificate under Section 65B(4) required
Bharatiya Sakshya Adhiniyam, 2023 (in force 1 July 2024)	Section 61 — non-discrimination clause	Electronic/digital record not inadmissible merely for being electronic
Bharatiya Sakshya Adhiniyam, 2023	Section 62 — proof in accordance with Section 63	Links general recognition to specific procedural conditions
Bharatiya Sakshya Adhiniyam, 2023	Section 63 — admissibility of electronic records	Certificate identifying the record and device particulars, with hash value per Schedule; certification by device custodian and, where applicable, an expert
Bharatiya Sakshya Adhiniyam, 2023	Section 66 — electronic signatures	Proof of digitally signed records

Table 2. Key Provisions of the Bharatiya Sakshya Adhiniyam, 2023 Relating to Digital Evidence

Section	Heading	Substance
Section 61	Electronic or digital record	Bars denial of admissibility solely on the ground that a record is electronic or digital; equates legal effect with other documents, subject to Section 63

Section 62	Special provisions as to evidence relating to electronic record	Contents of an electronic record may be proved in accordance with Section 63
Section 63	Admissibility of electronic records	Deems computer output to be a document; lays down conditions (regular use, proper operation, accuracy) and a mandatory certificate under sub-section (4)
Section 64	Rules as to notice to produce	General notice-to-produce requirements extended to electronic records where applicable
Section 66	Proof as to electronic signature	Governs proof of records authenticated by electronic signature

VIII. Authentication and Reliability of Digital Evidence

Admissibility under Section 63 of the BSA establishes only the threshold condition for a record to be received in evidence; it does not, by itself, determine the weight that a court will attach to it (Bharatiya Sakshya Adhiniyam, 2023, s. 63). Authentication and reliability are distinct, if related, inquiries. Authentication concerns whether the record is genuinely what it is represented to be, for instance, that a given video was indeed recorded by the CCTV system at the location and time alleged, or that a chat log genuinely originated from the device and account attributed to the accused. Reliability concerns the broader question of whether the process of generation, storage, transfer and preservation of the record inspires sufficient confidence for the court to act upon its contents.

Several technical and procedural elements bear directly on these questions. Hash values cryptographic digests generated from the content of a file allow a court or forensic examiner to verify that a record produced in court is bit-for-bit identical to the record originally seized, since even a trivial alteration to the underlying data changes the resulting hash value; the Schedule to Section 63 of the BSA specifically contemplates the inclusion of such technical particulars in the certificate (Bharatiya Sakshya Adhiniyam, 2023, sch.). Metadata, comprising information such as the time of creation, the device identifier and the geographic coordinates embedded within a file, similarly assists in establishing provenance, although metadata is itself capable of manipulation and is not conclusive on its own. Device identification, involving the association of a record with a specific handset, SIM card or account, is frequently established through subscriber and call-detail records obtained from telecommunication service providers. Digital forensic examination, typically conducted at a state forensic science laboratory or an equivalent institution, provides the technical foundation upon which certification and expert opinion evidence rest (Bharati & Nagarale, 2025).

A further requirement, of long standing in Indian criminal procedure and reinforced in decisions concerning circumstantial evidence generally, is the maintenance of an intact chain of custody — a documented, unbroken record of every person who has handled a piece of digital evidence from the moment of seizure to its production in court (Tomaso Bruno v. State of Uttar Pradesh, 2015). Any unexplained gap in this chain, or any indication that the original device or storage medium was not properly preserved, exposes the evidence to challenge on grounds of possible tampering or substitution, and may in appropriate cases justify an adverse inference against the party responsible for its custody.

Figure 2. Digital Evidence Lifecycle

Each stage in this lifecycle affects the ultimate reliability of the evidence; a lapse at any single stage for instance, improper preservation after collection can undermine the value of otherwise sound forensic examination and certification carried out subsequently.

Table 3. Types of Digital Evidence and Their Common Evidentiary Concerns

Type of Digital Evidence	Typical Source	Principal Evidentiary Concern
CCTV/surveillance footage	Private or public surveillance systems	Chain of custody; continuity; best-evidence considerations
Mobile-phone data	Handsets, service providers	Device identification; subscriber attribution
Chat/instant-messaging records	WhatsApp and similar platforms	Authorship attribution; risk of spoofing or editing
Email	Email service providers, servers	Header authenticity; server log verification
Social-media content	Platform servers, archived pages	Account attribution; volatility of online content
Audio/video recordings	Recording devices, phones	Editing/splicing; voice or image authentication
GPS/location data	Devices, cell-tower records, applications	Accuracy; corroboration with other records
Cloud/server data	Remote servers, service providers	Jurisdictional access; custodial control

Table 4. Requirements for Establishing the Reliability of Digital Evidence

Requirement	Function
Authenticity	Establishes that the record is what it purports to be
Integrity	Confirms the record has not been altered since creation or seizure
Hash value verification	Provides a cryptographic check to detect alteration
Metadata analysis	Assists in establishing time, device and location of creation
Source/device identification	Links the record to a specific device or account
Digital forensic examination	Provides expert technical validation of the above elements
Chain of custody	Documents unbroken custody from seizure to production in court
Section 63 certificate	Statutory precondition for admission of computer output without the original

IX. Judicial Developments

The Indian judiciary's engagement with electronic evidence has been marked by considerable doctrinal movement, principally concerning the mandatory or directory character of the certificate requirement. This section traces that development through the leading decisions of the Supreme Court, whose reasoning continues to inform the interpretation of the corresponding provisions of the BSA.

9.1 State (NCT of Delhi) v. Navjot Sandhu (2005)

In its early encounter with electronic evidence in the Parliament attack case, the Supreme Court took a comparatively permissive approach, holding that secondary evidence of electronic records, including call records, could be proved even without strict compliance with the certificate procedure, provided there was other evidence establishing their genuineness (State (NCT of Delhi) v. Navjot Sandhu, 2005). This approach was significant in linking electronic material to the conspiracy in that case, but it left the precise scope of the certification requirement unsettled for the following decade.

9.2 Anvar P.V. v. P.K. Basheer (2014)

A three-judge bench decisively altered this position in Anvar P.V. v. P.K. Basheer (2014), an election petition concerning the use of compact discs containing recorded speeches and songs as evidence of corrupt electoral practices. The Court held that Sections 65A and 65B of the then Evidence Act constituted a complete and self-contained code for the proof of electronic records, and that secondary evidence of an electronic record could not be adduced through oral testimony or by treating a computer printout as primary evidence in the absence of a Section 65B(4) certificate (Anvar P.V. v. P.K. Basheer, 2014). The Court expressly overruled the more permissive approach taken in Navjot Sandhu (2005), holding that the electronic evidence in that case was inadmissible for want of the requisite certificate, with the consequence that the appellant's allegations of corrupt practice could not be sustained.

9.3 Tomaso Bruno v. State of Uttar Pradesh (2015)

In Tomaso Bruno v. State of Uttar Pradesh (2015), a criminal appeal arising from a conviction based substantially on circumstantial evidence, the Supreme Court held that CCTV footage capable of establishing the presence or absence of the accused at the scene constituted the best evidence available to the prosecution, and that its non-production without adequate explanation entitled the court to draw an adverse inference under Section 114, illustration (g), of the Evidence Act. The decision underscored the evidentiary primacy of contemporaneous digital records over oral testimony describing their contents, while also illustrating that the acquisition and preservation of such evidence at the investigation stage is as important as its subsequent proof at trial.

9.4 Shafhi Mohammad v. State of Himachal Pradesh (2018)

A two-judge bench in Shafhi Mohammad v. State of Himachal Pradesh (2018) sought to relax the position in Anvar (2014), holding that the requirement of a Section 65B(4) certificate was procedural rather than a mandatory condition of admissibility, and that it could be dispensed with where the party seeking to rely on the electronic record was not in possession of the device from which it originated. This introduced fresh uncertainty into the law, since it appeared to conflict with the earlier three-judge bench ruling in Anvar (2014).

9.5 Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)

The resulting conflict was authoritatively resolved by a three-judge bench in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), an election dispute concerning CCTV recordings of the filing of nomination papers. The Court held that the certificate under Section 65B(4) is a condition precedent to the admissibility of secondary evidence by way of an electronic record, reaffirmed Anvar (2014) as correctly decided, and held Shafhi Mohammad (2018) to be per incuriam. The Court clarified that the certificate requirement does not apply where the electronic record is produced as primary evidence that is, where the original device itself is produced before the court and further held that a party unable to obtain the certificate from a person in possession of the device is not without remedy, since an application can be made to the court to summon such a certificate (Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, 2020). The Court also issued general directions to investigating agencies and courts concerning the preservation of electronic evidence and the timely furnishing of certificates during trial. This decision continues to guide the interpretation of the corresponding certification requirement under Section 63 of the BSA.

9.6 Continuing Judicial Engagement

Since the BSA came into force, courts have continued to apply the certification-based framework to newer categories of digital evidence, and the reasoning developed under Section 65B remains highly persuasive in interpreting Sections 61 to 63 of the BSA, given the substantial continuity between the two regimes (Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, 2020; Bharatiya Sakshya Adhiniyam, 2023, ss. 61–63). The emergence of deepfake and other AI-generated media has begun to generate fresh judicial and scholarly attention, particularly following the framing of rules concerning synthetically generated information under the information technology regulatory framework, which impose traceability and labelling obligations on intermediaries. Commentators have observed that such technical provenance mechanisms may in future assist litigants in discharging the burden of establishing authenticity, even as the underlying statutory certification requirement under Section 63 continues to apply (Mondaq, 2026a, 2026b).

X. Conclusion

The path this paper has traced, from the interpretive uncertainty of Navjot Sandhu (2005), through the strict certification requirement affirmed in Anvar (2014), the temporary relaxation attempted in Shafhi Mohammad (2018), to its authoritative resolution in Arjun Panditrao Khotkar (2020), shows that Indian courts have never treated the certification of electronic records as a mere technicality. It has consistently been read as a real safeguard against the particular ease with which digital material can be altered or fabricated. The Bharatiya Sakshya Adhiniyam, 2023 has not displaced this line of reasoning; Sections 61 to 63 largely restate it, and the case law built up under the old Section 65B still does most of the interpretive work for the new provisions.

What the case law and the literature reviewed in this paper agree on, from different directions, is that being electronic does not by itself make a record more or less trustworthy. An electronic record is admissible on the same footing as any other document, but how much weight a court gives it still depends on ordinary things: whether it is authentic, whether custody was maintained without gaps, whether the certificate and any forensic examination behind it were done properly (Bharati & Nagarale, 2025; Kanishka & Sharma, 2026). The problems that keep coming up in this paper, a shortage of trained forensic staff, judges and lawyers who are not always comfortable with hash values and metadata, and a still-open question over how to treat deepfakes, are not the kind of thing a statute can fix by itself.

The suggestions set out in Section 11, from building up forensic capacity and standardising the Section 63 certificate to a more direct regulatory response to synthetic media, are aimed at that gap between what the law now says and what the system is actually equipped to do. As criminal trials in India rely more and more on digital material, whether the safeguards built up by the courts continue to mean anything in practice will come down to whether forensic infrastructure, judicial training and basic procedural discipline keep pace with the technology the law is now being asked to govern.

XI. Suggestions

The analysis above, and the concerns raised in the literature discussed in Section 2 (Bharati & Nagarale, 2025; Kanishka & Sharma, 2026), point to a fairly consistent set of gaps between what the BSA promises on paper and what the system can currently deliver. The following measures are suggested to help close that gap:

1. Strengthening forensic infrastructure: Expanding the network of state and regional forensic science laboratories and cyber-forensic units, filling vacant scientific posts, and setting statutory turnaround timelines for forensic reports, so that certification and hash-value verification under Section 63 can be completed without undue delay (Budding Forensic Expert, 2026b; Wahab, 2026).
2. Judicial and prosecutorial training: Institutionalising regular, structured training for judges, public prosecutors and defence counsel on the technical aspects of digital evidence — hash values, metadata, cloud architecture and

chain-of-custody documentation — so that certification and expert evidence can be meaningfully evaluated rather than accepted or rejected pro forma.

3. Standardising the Section 63 certificate: Prescribing a uniform, model certificate format and clear timelines for its issuance at the point of seizure, in line with the directions issued in Arjun Panditrao Khotkar (2020), to reduce the recurring difficulty of certificates being sought or contested belatedly at trial.

4. Digital evidence management systems: Adopting standardised, auditable digital evidence management systems at the police-station and forensic-laboratory level to create a tamper-evident, time-stamped record of custody from seizure to production in court, since the absence of a uniform national chain-of-custody protocol remains one of the more common reasons forensic material is challenged or rejected at trial (Budding Forensic Expert, 2026a; Legal Service India, 2026b).

5. Capacity building at the investigation stage: Developing clear standard operating procedures, consistent with the search-and-seizure provisions of the Bharatiya Nagarik Suraksha Sanhita, 2023, for the seizure, imaging and preservation of digital devices by trained personnel at cyber cells and police stations.

6. Statutory and regulatory response to synthetic media: Extending specific provisions or subordinate rules addressing the authentication of deepfakes and AI-generated content, building on the traceability and labelling obligations that the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 already impose on intermediaries (Mondaq, 2026a, 2026b).

7. Harmonisation with data-protection law: Issuing clarificatory guidance on how the collection, storage and certification of electronic evidence under the BSA is to be reconciled with the data-minimisation and purpose-limitation principles of the Digital Personal Data Protection Act, 2023 (GLS Law Journal, 2026).

8. Access to forensic expertise for indigent accused persons: Ensuring that legal-aid mechanisms extend to funding independent forensic examination and expert testimony, so that the ability to contest or rely upon digital evidence does not depend on the financial means of the accused.

9. International and cross-border cooperation: Streamlining mutual legal assistance procedures for the timely retrieval of cloud-stored or foreign-hosted electronic evidence, an area of growing practical significance given the volume of data held outside Indian jurisdiction.

10. Periodic statutory review: Establishing a mechanism for the periodic review of the Schedule to Section 63 and related rules, so that certification requirements keep pace with evolving storage technologies, encryption standards and forms of digital communication.

References

[1]. Anthal, D. (2025). Digital evidence's admissibility under the Bharatiya Sakshya Adhiniyam (BSA): A comparison with the Indian Evidence Act (IEA) 1872.

[2]. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

[3]. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

[4]. Bharati, R. K., & Nagarale, S. (2025). Digital forensic science and evidentiary standards in the Bharatiya Sakshya Adhiniyam (BSA) 2023: A legal examination of admissibility. Indian Journal of Law and Technology, 15.

[5]. Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023).

[6]. Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023).

[7]. Budding Forensic Expert. (2026a). Why forensic evidence still gets rejected in Indian courts — and what needs to change.

[8]. Budding Forensic Expert. (2026b). The backlog crisis: India's forensic labs are drowning — and justice is paying the price.

[9]. Chhatrapati, D., Chaudhari, S. P., Mevada, D., Bhatt, A., & Trivedi, D. (2021). Research productivity and network visualization on digital evidence: A bibliometric study. Science & Technology Libraries. https://doi.org/10.1080/0194262x.2021.1948486

[10]. Free Law. (2025). Forensic and electronic evidence 2025: Chain of custody, DNA, and admissibility. https://www.freelaw.in/legalarticles/Forensic-and-Electronic-Evidence-2025-Chain-of-Custody-DNA-and-Admissibility

[11]. Ganguli, P. (2024). Admissibility of digital evidence under Bharatiya Sakshya Sanhita: A comparative study with the Indian Evidence Act.

[12]. GLS Law Journal. (2026). Admissibility of digital evidence under Bhartiya Shakhya Adhiniyam, 2023: Balancing data privacy and challenges in light of the DPDP Act, 2023. GLS Law Journal, 8(2), 23–36.

[13]. Indian Journal of Law. (2026). Electronic evidence in Indian law: Admissibility, authentication and evidentiary value. https://law.shodhsagar.com/index.php/j/article/view/184

[14]. Information Technology Act, 2000 (Act No. 21 of 2000).

[15]. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026.

[16]. Kanishka, & Sharma, N. (2026). Electronic evidence under Bharatiya Sakshya Adhiniyam: A critical analysis. Indian Journal of Law and Legal Research, 7(6). https://www.ijllr.com/post/electronic-evidence-under-bharatiya-sakshya-adhiniyam-a-critical-analysis

[17]. Legal Blur. (2026). The future of forensic and cyber law trials under new criminal codes in India. https://legalblur.com/the-future-of-forensic-and-cyber-law-trials-under-new-criminal-codes-in-india/

[18]. Legal Service India. (2026a). Deepfake evidence in Indian courts: Legal challenges, admissibility, authentication & burden of proof. https://www.legalserviceindia.com/Legal-Articles/deepfake-evidence-indian-courts-admissibility-authentication-burden-proof/

[19]. Legal Service India. (2026b). The digital forensic investigation process: Chain of custody and evidence preservation. https://www.legalserviceindia.com/Legal-Articles/the-digital-forensic-investigation-process-chain-of-custody-and-evidence-preservation/

[20]. Mondaq. (2026a). IT Rules 2026 deepfake regulation: Three hour takedowns and AI labelling obligations. https://www.mondaq.com/india/new-technology/1760554/it-rules-2026-deepfake-regulation-three-hour-takedowns-and-ai-labelling-obligations

[21]. Mondaq. (2026b). Deepfakes as evidence: Authenticity, chain of custody and Section 65B in the age of IT Rules 2026. https://www.mondaq.com/india/new-technology/1763744/deepfakes-as-evidence-authenticity-chain-of-custody-and-section-65b-in-the-age-of-it-rules-2026
[22]. National Crime Records Bureau. (n.d.). Crime in India reports. Government of India. https://ncrb.gov.in
[23]. Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.
[24]. Srishti. (2025). The impact of forensic science on the legal system in India. Journal of Forensic Science Research. https://www.forensicscijournal.com/journals/jfsr/jfsr-aid1072.php
[25]. State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
[26]. Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178.
[27]. Wahab, M. I. (2026). Forensic laboratories: The role and functions of central and state institutions. Legal Service India. https://www.legalserviceindia.com/Legal-Articles/forensic-laboratories-the-role-and-functions-of-central-and-state-institutions/