Digital Forensics and Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023: Judicial Trends and Challenges in Cybercrime Trials

[1]A. Barsad Begam, [2]Dr. K.J. Rajan, [3]Akash. J

[1]Research Scholar; Sub Judge; Sri Vaikundam, Tamil Nadu, India. Email id: jgbarsad@gmail.com.

[2]Dean, School of Law, Joy University, Vadakkankulam, Tirunelveli, Tamil Nadu, India.

Email id: advrajan73@gmail.com.

[3]BPR&D- Junior Research Fellow, Department of Criminology and Criminal Justice, MS University, Tirunelveli, TN, India. Email ID: akash.j.msu@gmail.com; ORCID id: 0009-0003-0179-3831

HOW TO CITE:
A. Barsad Begam, K. J. Rajan, Akash. J. (2026). Digital Forensics and Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023: Judicial Trends and Challenges in Cybercrime Trials.

International Journal of Special Education, 41(18s), 277-291

ABSTRACT:

The replacement of the Indian Evidence Act, 1872 by the Bharatiya Sakshya Adhiniyam, 2023 ('BSA') marks a consequential moment in Indian evidence law, arriving at a time when cybercrime prosecutions increasingly turn on the reliability of digital forensic material. This article examines, first, the statutory architecture governing digital forensics and the admissibility of electronic evidence under the BSA read together with the Information Technology Act, 2000 ('IT Act') and the Bharatiya Nagarik Suraksha Sanhita, 2023 ('BNSS'); and second, the judicial trends that continue to shape how courts receive and evaluate such evidence in cybercrime trials. The research problem addressed is that legislative re-codification has not, of itself, resolved the doctrinal uncertainties that attended Section 65B of the former Evidence Act, and that courts remain confronted with unresolved questions of certification, timing, chain of custody, and the appreciation of technically complex material. Adopting a doctrinal and analytical methodology grounded in statutory interpretation and case-law analysis, the article traces the transition from State (NCT of Delhi) v Navjot Sandhu through Anvar P.V. v P.K. Basheer, Tomaso Bruno v State of Uttar Pradesh, Shafhi Mohammad v State of Himachal Pradesh and Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal, and assesses the extent to which Section 63 of the BSA consolidates or merely re-labels this jurisprudence. The comparative dimension situates Indian practice against the authentication regimes of the United Kingdom, the United States, Singapore, Australia and the European Union. The principal findings are that the BSA introduces incremental refinements — notably a dual-signature certificate and statutory flexibility where certification is genuinely unobtainable — without addressing structural

weaknesses in forensic laboratory capacity, cross-border data access, or judicial training in technical appraisal. Where no verified empirical data exists on a given point — for instance, the operational rate of certificate compliance nationally — the article expressly acknowledges this evidentiary gap rather than supplying invented figures. The article's original contribution lies in reading the BSA, the IT Act and the BNSS as a single interlocking evidentiary-procedural regime, rather than as three separately administered statutes, and in deriving from that reading a reform agenda addressed to forensic accreditation, judicial capacity-building and cross-border cooperation.

Keywords: Bharatiya Sakshya Adhiniyam 2023; electronic evidence; digital forensics; cybercrime; chain of custody; comparative evidence law; Bharatiya Nagarik Suraksha Sanhita

Introduction

India's exposure to cybercrime has grown in step with the expansion of its digital economy, and criminal investigation and adjudication have had to adapt to a fact pattern in which the decisive evidence is rarely a physical object and almost always an electronic record — a server log, a WhatsApp export, a CCTV file, a cell-site data dump, or a forensic image of a hard disk. Successive editions of the National Crime Records Bureau's *Crime in India* series and the periodic advisories issued by the Indian Cyber Crime Coordination Centre (I4C) and CERT-In record a rising volume of cyber-enabled offences, though current empirical evidence on the precise scale, year-on-year, is limited by definitional inconsistencies across reporting agencies and is not restated here in numerical form to avoid attributing unverified figures to these sources.

The Bharatiya Sakshya Adhiniyam, 2023, which repealed and replaced the Indian Evidence Act, 1872 with effect from 1 July 2024, [1] forms part of a wider recodification of Indian criminal law that also produced the Bharatiya Nyaya Sanhita, 2023 and the Bharatiya Nagarik Suraksha Sanhita, 2023. The stated legislative purpose of this recodification was to modernise a body of law substantially inherited from the colonial period and to embed technology more explicitly within investigative and evidentiary procedure. For electronic evidence specifically, the change of principal consequence is the migration of the certification regime from Section 65B of the former Evidence Act to Section 63 of the BSA, accompanied by a Schedule prescribing a two-part certificate format requiring both a device-operator's affirmation and an expert's technical certification, including a hash value and the algorithm used to generate it. [2]

The premise of this article is that legislative recodification, without more, does not resolve the doctrinal difficulties that had accumulated around Section 65B in the two decades following its insertion by the Information Technology Act, 2000. Those difficulties — concerning whether the certificate is a condition precedent to admissibility or a matter going only to weight, the stage at which it must be furnished, and the treatment of evidence where a certificate is genuinely unobtainable — were substantially settled, so far as the pre-2024 law was concerned, by the Supreme Court in [3]*Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*[3]. Because Section 63 of the BSA substantially re-enacts the structure of Section 65B, the interpretative overlay built up through that line of

1. The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023) received presidential assent on 25 December 2023 and was brought into force, together with the Bharatiya Nyaya Sanhita, 2023 and the Bharatiya Nagarik Suraksha Sanhita, 2023, with effect from 1 July 2024 by notification of the Ministry of Home Affairs.

2. Bharatiya Sakshya Adhiniyam 2023, s 63(4) and the Schedule thereto (Part A and Part B of the certificate).

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

authority remains relevant, but it has not been definitively tested against the new statutory text, and the changes that do exist — in particular the dual-certificate requirement — raise fresh questions of their own.

The existing literature on electronic evidence in India is extensive on Section 65B and its case law, but comparatively thin on the operative detail of Section 63 of the BSA read together with the search-and-seizure and forensic provisions of the BNSS, and on how the two statutes interact in the specific context of cybercrime trials rather than civil, matrimonial or election disputes, which dominate the reported case law under the former regime. This article addresses that gap by treating the BSA, the IT Act and the BNSS as components of a single evidentiary-procedural architecture and by examining that architecture specifically through the lens of cybercrime adjudication, where the volume, technical complexity and cross-border character of the evidence place the greatest strain on the certification and chain-of-custody framework.

Concept of Digital Forensics

Digital forensics may be defined as the application of scientifically validated methods to the identification, preservation, collection, examination and presentation of data derived from digital devices, undertaken in a manner that preserves the evidential integrity of that data for use in legal proceedings. The discipline grew out of computer security practice in the 1980s and 1990s and has since differentiated into specialised sub-fields — computer forensics, mobile device forensics, network forensics, cloud forensics and, more recently, forensic techniques directed at artificial-intelligence-generated content — each governed by broadly similar principles of integrity but requiring distinct technical methods.

Chain of custody, forensic imaging and hash values

The chain of custody is the documented, unbroken record of every person who has held, transferred or examined a piece of evidence from the moment of seizure to its production in court. For digital evidence, the chain of custody must additionally record the forensic imaging process — the creation of a bit-for-bit copy of the source medium so that the original device need not itself be repeatedly handled or altered — and the hash value computed both before and after the imaging process. A hash value, generated by an algorithm such as SHA-256, functions as a unique digital fingerprint of the data set: if the hash values of the original and the copy match, the copy can be treated as an exact, unaltered reproduction of the original, and any subsequent divergence in hash values signals tampering or corruption. [4]

Metadata — information about a file's creation date, modification history, author, geolocation or device identifier, embedded within the file itself rather than in its visible content — performs an evidentiary function distinct from the file's substantive content: it can corroborate or undermine a claim about when and by whom a document was created, and its manipulation is a recurring vector of evidentiary fraud, discussed further in Section 8 below.

Categories of digital evidence

Cloud evidence presents distinctive difficulties because the data is not physically located at the site of seizure and may be distributed across servers in multiple jurisdictions, engaging questions of territorial jurisdiction and the cooperation of foreign or multinational service providers. Mobile forensics involves the extraction of call logs, messages, application data and location history from handsets, frequently complicated by device encryption, proprietary operating-system restrictions and the practice of remote wiping. Computer forensics remains the most established sub-field, encompassing disk imaging, file-system analysis, recovery of deleted data and examination of system logs. Network forensics is concerned with the analysis of traffic logs, intrusion-detection records and server access logs to reconstruct the path of an intrusion or the origin of a communication.

Email evidence raises authentication questions distinct from other categories because headers can be forged, though header analysis — examining routing information such as the Received and Message-ID fields — can itself furnish forensic corroboration. CCTV evidence is now ubiquitous in cybercrime-adjacent prosecutions (for example, in establishing physical access to a device or premises) and raises its own chain-of-custody questions concerning the retrieval of footage from a digital video

4. See generally the discussion of hash-based authentication in the schedule to the Bharatiya Sakshya Adhiniyam, 2023, and the National Institute of Standards and Technology's endorsement of the SHA-256 algorithm, referenced in Bureau of Police Research and Development training material on the BSA, 2023.

recorder before automatic overwriting occurs. Social media evidence — posts, direct messages, profile data — is acquired either through platform-assisted preservation requests or through forensic capture tools that record metadata and cryptographic hashes at the point of collection; a simple screenshot, without such safeguards, carries comparatively weak evidentiary value because the underlying content can be edited before capture.

Blockchain evidence, comprising records maintained on a distributed and cryptographically linked ledger, is increasingly relevant in offences involving cryptocurrency, and its evidentiary value derives from the tamper-evident structure of the ledger itself, though establishing the identity of the person controlling a given wallet address remains a distinct and often more difficult inferential task. AI-generated digital evidence — including deepfake audio, video and synthetic text — inverts the ordinary evidentiary presumption: where conventional digital evidence is presumed genuine until shown to be altered, AI-generated content increasingly requires the proponent to affirmatively demonstrate authenticity through provenance metadata, detection tools or corroborating human testimony, a challenge examined further in Section 8.

Across all these categories, forensic integrity depends on four recurring safeguards: write-blocking hardware or software that prevents alteration of source media during acquisition; contemporaneous documentation of every step in the acquisition and analysis process; independent verification of hash values at each transfer; and the qualification of the examiner, whose competence and impartiality bear directly on the weight a court is entitled to give the resulting certificate or testimony.

Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023

Section 63 of the BSA is the direct successor to Section 65B of the Indian Evidence Act, 1872, and retains its foundational structure: information contained in an electronic record, whether printed on paper or stored, recorded or copied in optical, magnetic or semiconductor media, is deemed to be a document and is admissible without proof or production of the original, provided the conditions specified in the section are satisfied. [5] Section 63(2) sets out the conditions of admissibility, requiring, in substance, that the computer output was produced by a device used regularly for the relevant activity, that information of the relevant kind was regularly fed into the device in the ordinary course of that activity, that the device was operating properly throughout, and that the information reproduced is derived from information fed into the device in the ordinary course of the activity.

The most significant legislative refinement introduced by the BSA lies in Section 63(4) and the accompanying Schedule, which now require a dual-part certificate: Part A, completed by the person responsible for the device or the management of the relevant activity, identifying the electronic record and describing the manner of its production; and Part B, completed by an expert, addressing the technical particulars of the device and the hash value of the record together with the algorithm used. [6] Where the former Section 65B required certification only by a person occupying a responsible official position in relation to the device, the BSA superimposes a requirement of independent technical validation, drawing conceptually on the notified 'Examiner of Electronic Evidence' mechanism under Section 79A of the IT Act.

This dual-certification design reflects a legislative judgment that a device operator's certificate, standing alone, addresses only the operational regularity of the system but says nothing about whether the specific record tendered in court is a bit-for-bit, unaltered copy of what the device produced. The expert's hash-value certification is intended to close that gap. Whether this innovation will meaningfully improve reliability in practice depends on the availability of qualified examiners — a matter addressed in Section 8 below — since a statutory requirement that cannot, as a practical matter, be satisfied risks reproducing exactly the exclusionary rigidity that the Supreme Court sought to soften in *Arjun Panditrao Khotkar*.

Legislative changes from the Indian Evidence Act, 1872

Beyond Section 63, the BSA makes two further changes of note. First, Section 61 expressly provides

5. Bharatiya Sakshya Adhiniyam 2023, s 63(1). See also the analysis of the transition from s 65B to s 63 in K.S. & K. Legal Insights, 'Section 63 Bharatiya Sakshya Adhiniyam 2023' (ksandk.com, 2024–25).

6. Bharatiya Sakshya Adhiniyam 2023, s 63(4) and Schedule (Parts A and B); see Bhatt & Joshi Associates, 'Electronic Evidence Under BSA 2023: Section 63 Certificate Requirements and Supreme Court Interpretation' (2025–26).

that electronic or digital records shall have the same legal effect, validity and enforceability as paper records, [7] a general equivalence provision that had no direct counterpart in the 1872 Act and that operates as an interpretative backdrop to Section 63. Second, the definition of 'document' and 'evidence' in Section 2 of the BSA has been widened to expressly encompass electronic records, removing an ambiguity that had earlier required courts to reason by analogy from the definition of 'document' under Section 3 of the 1872 Act. Illustrations appended to Section 2 clarify, by way of example, that emails, server logs, documents stored on computers, laptops or smartphones, messages, websites and voicemail messages are documents for evidentiary purposes. [8]

Legislative intent, admissibility and judicial discretion

The legislative intent behind retaining a certification-based regime, rather than moving wholesale to a system of unconditional admissibility subject to weight, appears to be a continued distrust of unauthenticated electronic material, calibrated against the practical recognition — introduced by amendment relative to the 1872-era Section 65B — that certification should not become an insurmountable barrier where it cannot, in the circumstances, be obtained. The BSA continues to permit a certificate to be dispensed with, or its absence excused, in defined circumstances of genuine impossibility, echoing the mechanism the Supreme Court itself constructed in *Arjun Panditrao Khotkar* by permitting an applicant to seek a judicial direction compelling production of a certificate from the person or authority in control of the relevant device. Read together, Section 63 preserves judicial discretion at the margins — in assessing whether the statutory conditions are cumulatively satisfied, and in determining whether non-compliance is excusable — while retaining the certificate as the ordinary gateway to admissibility for secondary electronic evidence.

On reliability and authenticity, Section 63 does not itself create a presumption of truth for the contents of a certified record; it deems the record admissible as a document and directs that the certificate is evidence of the matters stated in it, but the weight to be attached to the record, and the truth of the facts it purports to record, remain questions for trial on the ordinary principles of appreciation of evidence. This distinction — between authentication as a threshold for admission and appreciation as a matter for the trier of fact at the conclusion of trial — is doctrinally significant and is frequently elided in practice, where courts and counsel alike sometimes treat the mere production of a Section 63 certificate as if it settled the substantive reliability of the record's contents.

Relationship between the Bharatiya Sakshya Adhiniyam, the Information Technology Act, 2000 and the Bharatiya Nagarik Suraksha Sanhita, 2023

Electronic evidence in a cybercrime trial is rarely governed by a single statute. The BSA supplies the rule of admissibility; the IT Act supplies the substantive offences, the mechanism for digital signatures and intermediary liability, and the notified-examiner infrastructure; and the BNSS supplies the procedural framework by which such evidence is gathered, recorded and brought before the court. A coherent account of digital forensic evidence in Indian cybercrime trials therefore requires reading all three together rather than treating each as a self-contained code.

The Information Technology Act, 2000

The IT Act remains the principal statute defining cyber offences — including unauthorised access and data theft under section 43 and section 66, offences of hacking and identity theft, obscenity offences under section 67, and offences arising from failure to comply with the government's powers of interception, monitoring and decryption under section 69. Section 65 of the IT Act separately criminalises tampering with computer source documents, a provision of direct relevance to the integrity of the forensic chain itself, since an accused who alters source code or logs after seizure, or an investigator who does so, is potentially exposed to liability under this provision independent of the underlying cybercrime charge.

Section 79A of the IT Act empowers the Central Government to notify an agency as an Examiner of Electronic Evidence, competent to

7. Bharatiya Sakshya Adhiniyam 2023, s 61; see Nyaaya, 'Electronic recording of search and seizure processes is mandatory now' (2025), noting the complementary relationship between BSA s 61 and BNSS ss 105 and 185.

8. See the paper presented at the Bureau of Police Research and Development session on electronic evidence, referring to Illustration (vi) to s 2(d) of the Bharatiya Sakshya Adhiniyam, 2023.

provide expert opinion on electronic evidence before any court or authority. [9] This mechanism now supplies the institutional backbone for the expert-certification limb of the BSA's Section 63(4) Schedule: the 'expert' contemplated by Part B of the certificate is, in practice, expected to be drawn from or accredited in line with the notified examiner framework, so that the IT Act's institutional design and the BSA's evidentiary design operate as two halves of a single mechanism rather than as parallel, unconnected requirements.

Sections 43A and 72A of the IT Act, dealing respectively with compensation for failure to protect sensitive personal data and punishment for disclosure of information in breach of a lawful contract, bear indirectly on forensic practice by constraining how intermediaries and service providers may lawfully share user data with investigating agencies, a constraint that interacts with the BNSS provisions on production of documents discussed below.

The Bharatiya Nagarik Suraksha Sanhita, 2023

The BNSS, which replaced the Code of Criminal Procedure, 1973, introduces mandatory audio-video recording of search and seizure proceedings. Section 105 governs search and seizure in respect of cognizable offences and Section 185 the corresponding procedure for non-cognizable offences; both provisions require that the process of search, the preparation of the seizure list and the signatures of witnesses be recorded, preferably by mobile phone, and that the recording be forwarded to the jurisdictional Magistrate. [10] This requirement is intended to deter fabrication or planting of evidence during the seizure of digital devices, a persistent concern in cybercrime investigations where the seized item (a laptop, a mobile handset, a pen drive) is itself the principal evidentiary object.

Section 176 of the BNSS requires that a forensic team visit the scene of the crime and collect samples, with the process recorded through videography, in respect of offences punishable with imprisonment of seven years or more — a threshold that captures the more serious cybercrime offences, including those involving large-scale data theft or child sexual abuse material. The BNSS also introduces a general provision, Section 530, enabling trials, inquiries and proceedings to be conducted in electronic mode, by use of electronic communication or audio-video electronic means, a provision the Kerala High Court has read as reflecting a deliberate, system-wide emphasis on the use of technology across the criminal process rather than a narrow, isolated reform. [11]

Statutory harmonisation and interpretative tension

Judicial Trends in Cybercrime Trials

The jurisprudence on electronic evidence in India has developed less through sustained doctrinal design than through a sequence of corrective judgments, each responding to a perceived overcorrection in the one before. That sequence — from *State (NCT of Delhi) v Navjot Sandhu* through *Anvar P.V.*, *Tomaso Bruno* and *Shafhi Mohammad* to *Arjun Panditrao Khotkar* — remains the interpretative inheritance against which Section 63 of the BSA will be read, because Parliament has substantially re-enacted rather than replaced the underlying statutory text that these judgments construed.

The starting point: State (NCT of Delhi) v Navjot Sandhu

In its 2005 decision arising from the prosecution relating to the attack on Parliament House, the Supreme Court took the view that Section 65B of the Evidence Act was not the sole gateway for the admission of electronic records and that such records could, in the alternative, be proved through the general provisions on secondary evidence together with expert opinion, without the certificate contemplated by Section 65B(4). [12] The practical effect of *Navjot Sandhu* was to treat Section 65B as directory rather than as a complete and exclusive code,

9. Information Technology Act 2000, s 79A. The Central Forensic Science Laboratory and select State forensic science laboratories have been notified as Examiners of Electronic Evidence under this provision.

10. Bharatiya Nagarik Suraksha Sanhita 2023, ss 105 and 185; see P39A Criminal Law Blog, 'Criminal Law Bills 2023 Decoded #12: Audio-Video Recordings during Investigation' (2023), and Nyaaya, 'Electronic recording of search and seizure processes is mandatory now' (2025).

11. See the discussion of Rollymol v State of Kerala in Livelaw, 'Recording of Search and Seizure Through Audio-Video Electronic Means Under Section 105 Of The BNSS' (2025), noting the Kerala High Court's observations on the BNSS's emphasis on modern technology in criminal investigation.

13. State (NCT of Delhi) v Navjot Sandhu (2005) 11 SCC 600. The correctness of this position was later expressly overruled by a three-judge bench in Anvar P.V. v P.K. Basheer (2014) 10 SCC 473.

permitting courts latitude to receive electronic material on the strength of oral testimony alone. Critically evaluated, this approach was administrable and flexible, but it sat uneasily with the specific, non-obstante drafting of Section 65B, which had been inserted precisely to create a special regime for electronic records distinct from the ordinary rules of secondary evidence, and it left courts without a reliable, self-executing safeguard against the unilateral assertion of authenticity by whichever party tendered the record.

Tomaso Bruno v State of Uttar Pradesh

In *Tomaso Bruno*, decided in 2015, the Supreme Court considered the significance of CCTV footage that the prosecution had failed to produce or preserve, in a case concerning the death of a foreign tourist. [13] The Court proceeded on the footing that secondary evidence of the contents of the missing footage could, in principle, be led under the general provisions on documentary evidence, without addressing the specific requirements of Section 65B or the holding in *Anvar P.V.* which had been decided the previous year. This omission was subsequently characterised, in *Arjun Panditrao Khotkar*, as a decision rendered *per incuriam* on the electronic-evidence point, precisely because it failed to engage with the binding three-judge authority in *Anvar P.V.* The episode illustrates a recurring difficulty in this field: even the Supreme Court has, on occasion, decided cases involving electronic material without expressly working through the specialised evidentiary provisions, generating precedent that later required correction and creating a period of doctrinal uncertainty for trial courts attempting to apply consistent principles in the interim.

Anvar P.V. v P.K. Basheer

A three-judge bench in *Anvar P.V.* (2014) confronted directly the question left ambiguous by *Navjot Sandhu*: whether Section 65B constituted the exclusive mode of proving electronic records tendered as secondary evidence. [14] The Court held that Sections 65A and 65B formed a complete and self-contained code governing the admissibility of electronic records, and that the certificate under Section 65B(4) was a mandatory precondition where the electronic record was tendered as secondary evidence rather than produced in original form. In reaching this conclusion, the Court expressly overruled the contrary position taken in *Navjot Sandhu*, holding that oral evidence or expert opinion under the general provisions of the Evidence Act could not substitute for the specific certificate that Section 65B(4) required.

The reasoning in *Anvar P.V.* reflects a coherent interpretative choice: because Section 65B begins with a non-obstante clause ('Notwithstanding anything contained in this Act'), the provision was drafted to operate as a special and exclusive regime rather than as one optional route among several, and giving effect to that legislative choice required treating the certificate as indispensable rather than as merely one way of proving authenticity among others. The practical consequence, however, was that litigants who had gathered electronic evidence in good faith, but without anticipating or being able to secure a formal certificate — a document custodian who had left service, a foreign service provider unwilling to certify, a device whose responsible officer could not be traced — found their evidence excluded regardless of its underlying reliability. This rigidity became the impetus for the next stage of the jurisprudence.

Shafhi Mohammad v State of Himachal Pradesh

In *Shafhi Mohammad*, a two-judge bench in 2018 sought to soften the rigour of *Anvar P.V.* by holding that the requirement of a certificate under Section 65B(4) was procedural and could be relaxed where a party was unable, despite best efforts, to procure the certificate — for instance, because the device was not in that party's possession — and that in such circumstances the interests of justice permitted the electronic record to be proved by other means, including an application to the court for a direction to the person in possession of the device to produce the requisite certificate. [15]

Considered on its own terms, *Shafhi Mohammad* responded to a genuine practical problem, but it did so by a two-judge bench purporting to depart from a three-judge decision, a course inconsistent with the ordinary rules of precedent within the Supreme Court itself, and it introduced fresh uncertainty as to when, precisely, a certificate could be dispensed with and on what standard 'best efforts' or impossibility was to be assessed. Trial courts were left to apply a discretionary and unevenly articulated impossibility exception without clear

14. Tomaso Bruno v State of Uttar Pradesh (2015) 7 SCC 178.
15. Anvar P.V. v P.K. Basheer (2014) 10 SCC 473.
16. Shafhi Mohammad v State of Himachal Pradesh (2018) 2 SCC 801.

guidance on its boundaries, an unsatisfactory position that persisted until the reference to a three-judge bench that produced *Arjun Panditrao Khotkar*.

Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal

The facts of *Arjun Panditrao Khotkar* arose from an election petition rather than a criminal prosecution, but the Supreme Court's ruling on electronic evidence has governed criminal and cybercrime adjudication ever since. The appellant, a successful candidate for the Maharashtra Legislative Assembly, prevailed by a narrow margin of 296 votes; the respondents challenged the acceptance of his nomination papers, relying on CCTV footage from the Returning Officer's office to establish that the papers had been filed after the prescribed cut-off time. [16] The certificate contemplated by Section 65B(4) had not been furnished by the Election Commission despite repeated requests, and the Bombay High Court had accepted the footage on the footing of 'substantial compliance', treating the Returning Officer's oral testimony in cross-examination as functionally equivalent to the missing certificate.

A three-judge bench, referred the matter precisely because of the conflict between *Anvar P.V.* and *Shafhi Mohammad*, reaffirmed that the certificate under Section 65B(4) is mandatory for secondary electronic evidence and cannot be substituted by oral testimony asserting 'substantial compliance', thereby overruling *Shafhi Mohammad* to the extent it suggested otherwise, and disapproving *Tomaso Bruno* on the electronic-evidence point as having been decided *per incuriam*. [17] At the same time, the Court clarified two important qualifications: first, that where the original document itself — rather than a secondary, computer-generated output of it — is produced for inspection, no Section 65B certificate is required at all, because the provision governs only secondary evidence; and second, that a party unable to obtain a certificate is not without remedy, since an application may be made to the court for a direction to the person or authority in control of the relevant device to furnish it, with the further clarification that in criminal proceedings involving the liberty of the accused, courts retain a residual power to ensure that the ends of justice are not defeated by a mechanical insistence on production at an inconvenient stage. [18]

The ratio of *Arjun Panditrao Khotkar* has two dimensions of continuing significance for the interpretation of Section 63 of the BSA. The first is substantive: because Section 63(4) re-enacts the certification requirement in materially the same form as Section 65B(4), the holding that the certificate is a condition precedent to admissibility (not merely a matter of weight) should be treated as carrying forward under the BSA, absent a clear legislative signal to the contrary; nothing in the text of Section 63 indicates an intention to abandon that principle, and the introduction of a more demanding dual-signature certificate is, if anything, consistent with treating certification as a serious and non-negotiable threshold requirement rather than a mere formality. The second is procedural: the Court's clarification that the certificate need not accompany the electronic record at the stage of filing, but must exist by the time the record is formally tendered for exhibition, continues to answer a question on which Section 63 itself is silent, and this timing rule should likewise be treated as carrying forward, since it addresses a gap in the statutory text rather than a feature of the repealed provision that the new text has displaced.

Critical assessment of the line of authority

Viewed as a whole, the sequence from *Navjot Sandhu* to *Arjun Panditrao Khotkar* reflects the Supreme Court oscillating between two legitimate but competing values: evidentiary rigour, which treats certification as indispensable to guard against the ease with which digital material can be fabricated, and access to justice, which resists excluding genuinely reliable evidence merely because a formal certificate could not be procured through no fault of the party tendering it. *Arjun Panditrao Khotkar* represents a considered attempt to reconcile these values by retaining the certificate as the ordinary rule while creating a judicially supervised mechanism for its compulsion in cases of genuine difficulty.

What the line of authority does not resolve, and what the BSA itself does not squarely address, is the practical burden the dual-certificate requirement places on prosecuting agencies in cybercrime matters

17. Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1, paras 1–6.
18. Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1; see also the summary in Lexology, 'Supreme Court clarifies on the requirement of a certificate under Section 65B of the Evidence Act, 1872' (2020).
19. Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1, paras 56–61, addressing the mechanism by which a certificate may be compelled through court application.

specifically, where the volume of electronic exhibits in a single case — chat logs, transaction records, IP address logs, device images — can run into hundreds of discrete items, each in principle requiring its own certificate under the Section 63(4) Schedule. Whether courts will develop, as they did under Section 65B, a body of practice permitting composite or omnibus certification for functionally related exhibits, and whether such practice would be consistent with the individualised, item-by-item language of Section 63(4) ('at each instance where it is being submitted for admission'), [19] remains an open question that the reported case law under the BSA has not yet definitively answered, and on which this article accordingly offers no more than a reasoned expectation rather than a settled conclusion.

It should also be recorded, in the interests of methodological candour, that at the time of writing no reported Supreme Court or High Court decision squarely construing Section 63 of the BSA on a contested point of first impression has yet emerged in a form permitting the same depth of critical analysis as the Section 65B line of authority; the discussion above accordingly proceeds by way of reasoned extrapolation from the pre-2024 jurisprudence, applied to the materially similar text of Section 63, rather than by reference to a distinct and fully developed body of BSA-specific case law.

Challenges in Digital Forensic Investigation

The statutory refinements introduced by the BSA and BNSS address certification and procedural recording, but a number of practical and constitutional challenges persist independently of the text of any single statute.

Data integrity, chain of custody and delay

The central technical challenge remains ensuring that data presented at trial is identical to data seized at the point of investigation. Delay between seizure and forensic examination — attributable to laboratory backlog rather than any deficiency in the statutory framework — increases the risk of medium degradation, accidental alteration during storage, and challenge to the chain-of-custody narrative on cross-examination. Current published data on average examination turnaround times across State forensic science laboratories is not, so far as this review has been able to establish, available in a form permitting reliable national comparison, and no such figure is asserted here.

Cloud jurisdiction, encryption and the dark web

Where relevant data resides on servers outside India, Indian investigating agencies must rely on mutual legal assistance treaties or, increasingly, direct requests to multinational platforms, both of which involve delay and depend on the receiving jurisdiction's own disclosure standards. Device and application-level encryption presents a related difficulty: an investigating agency may lawfully seize a handset yet be technically unable to extract its contents without the cooperation of the accused or the manufacturer, raising the further constitutional question, discussed below, of whether an accused can be compelled to furnish a password or biometric unlock. Offences facilitated through the dark web compound these difficulties because anonymising technology is specifically designed to defeat the kind of IP-address and metadata tracing on which conventional network forensics depends.

Metadata manipulation, deepfakes and AI-generated evidence

Because courts have historically approached electronic records on a presumption that they are what they purport to be once duly certified, the emergence of convincingly falsified audio, video and image content generated by artificial intelligence unsettles that presumption. Neither the BSA nor the BNSS contains provisions specifically addressed to the detection or authentication of synthetic media, leaving courts to rely on general expert-evidence provisions and on forensic detection tools whose reliability is itself the subject of ongoing technical development. This is an area in which the legislative framework has, to date, lagged behind the underlying technology, and in which the absence of a specific statutory response is itself a finding of this article, discussed further below.

Forensic laboratory capacity and expert-witness credibility

The dual-certificate mechanism under Section 63(4) presupposes ready access to a qualified expert for Part B of the certificate. The notified-examiner mechanism under Section 79A of the IT Act, while an important institutional resource, is concentrated in a limited number of central and state

20. Bharatiya Sakshya Adhiniyam 2023, s 63(4), opening words.

forensic laboratories, and the geographic and case-load distribution of that capacity relative to the volume of cybercrime investigations nationally is not, on the basis of publicly available material, something this article is able to quantify with confidence; it is noted here as a structural constraint rather than asserted as a measured deficit. Where expert capacity is genuinely scarce, the credibility and consistency of expert testimony across different courts and laboratories becomes a live concern, particularly where the expert's opinion is contested by an equally qualified defence expert, an occurrence that remains comparatively rare in Indian cybercrime trials relative to jurisdictions with a more developed defence-side forensic bar.

Privacy, constitutional rights and judicial appreciation of technical evidence

The constitutional right to privacy, recognised by a nine-judge bench of the Supreme Court as an intrinsic part of the right to life and personal liberty under Article 21, [20] bears directly on the permissible scope of digital search, seizure and surveillance, requiring that intrusions into digital privacy satisfy the tripartite test of legality, legitimate aim and proportionality that the Court articulated in that decision. The BNSS's search-and-seizure provisions and the IT Act's interception powers under Section 69 must accordingly be read and applied consistently with this constitutional standard, a discipline that is more easily stated than consistently achieved at the level of routine investigative practice.

A related and persistent difficulty is the capacity of trial-court judges, prosecutors and, in jury-free Indian practice, the judge alone, to meaningfully appraise technically dense expert testimony on matters such as hash-value comparison, metadata interpretation or network-log reconstruction. Judicial training programmes conducted through State judicial academies and the National Judicial Academy have begun to address digital evidence appreciation, but the depth and consistency of such training across the trial-court cadre nationally is not systematically documented in the public domain, and this article accordingly identifies training deficiency as a structural risk rather than a measured shortfall.

Cross-border investigation and infrastructure

Cybercrime frequently spans multiple national jurisdictions, and India's cooperation mechanisms — principally mutual legal assistance treaties and, for a narrower set of purposes, informal law-enforcement channels — operate on timelines poorly matched to the volatility of digital evidence, which service providers may retain only for limited periods absent a timely preservation request. India is not a party to the Council of Europe's Budapest Convention on Cybercrime, [21] which supplies a widely used framework for expedited preservation and mutual assistance among its parties, a fact that materially affects the speed with which Indian investigators can secure foreign-held evidence relative to investigators in states that are party to the Convention.

Comparative Analysis

A comparative review of five jurisdictions illustrates the range of design choices available for authenticating electronic evidence, and situates the BSA's certification model within that range.

United Kingdom

English law abandoned a formal statutory authentication regime for electronic business records with the repeal of section 69 of the Police and Criminal Evidence Act 1984, moving instead to a general presumption that a mechanical or electronic device has operated correctly, rebuttable on evidence to the contrary, supplemented by the ordinary hearsay and best-evidence principles of the Civil Evidence Act 1995 and the Criminal Justice Act 2003. It is notable, as earlier Indian commentary on Section 65B itself records, that the original Indian provision drew conceptually on section 5 of the UK's Civil Evidence Act 1968 as it stood prior to the Law Commission's subsequent reform proposals, [22] so that English law has, since that borrowing, moved toward a more permissive presumption-based model precisely at a time when Indian law, through *Anvar P.V.* and *Arjun Panditrao Khotkar*, moved toward stricter mandatory certification.

United States

United States federal practice authenticates electronic evidence principally under Federal Rule of Evidence 901, which requires proof sufficient to

21. Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

22. Council of Europe, Convention on Cybercrime (Budapest, 23 November 2001) ETS No 185. India has not acceded to the Convention.

23. See the account in Ratanpriya, 'A Detailed Analysis of Section 65B of the Indian Evidence Act' (2023), noting that s 65B has its genesis in s 5 of the UK Civil Evidence Act as amended following a Law Commission proposal in 2000.

support a finding that the item is what its proponent claims, and, since a 2017 amendment, under Rule 902(13) and 902(14), which permit self-authentication of records generated by an electronic process or system and of data copied from an electronic device respectively, upon written certification by a qualified person, without the need for that person's live testimony at trial. [23] The American model resembles the Indian certification model in its reliance on hash-value comparison as the technical mechanism of authentication, but differs in that certification under Rule 902 renders the evidence self-authenticating for admissibility purposes only, leaving hearsay, relevance and, in criminal cases, Confrontation Clause objections to be separately addressed — a structural separation between authentication and admissibility that is less sharply drawn in Indian practice, where a Section 63 certificate is sometimes treated, in practice if not in principle, as disposing of the evidentiary inquiry altogether.

European Union

The European Union's eIDAS Regulation establishes a harmonised framework for electronic identification, electronic signatures, seals and time-stamps across member states, according qualified electronic signatures and qualified timestamps a presumption of integrity and of the accuracy of the date and time they indicate. [24] This model achieves, through ex ante technical certification embedded in the record itself at the point of creation, much of what the Indian Section 63 certificate seeks to achieve ex post at the point of tender in evidence, and illustrates a design choice — building authentication into the technical infrastructure rather than relying exclusively on a subsequently prepared litigation document — that Indian policy has not yet systematically pursued outside limited contexts such as digital signatures under the IT Act.

Lessons for India

Three lessons emerge from this comparison. First, jurisdictions that have moved toward presumption-based or burden-shifting models (Singapore, Australia) have done so on the premise that automated systems are, absent contrary evidence, more likely than not to operate correctly, a premise the Indian judiciary has been reluctant to adopt given persistent, well-founded concerns about tampering and fabrication in the Indian evidentiary environment; any move in that direction would require confidence-building measures, such as accredited forensic laboratories and standardised acquisition protocols, that are not yet uniformly in place. Second, the American separation between authentication (a threshold question) and the substantive weight or admissibility of the record's contents offers a clarifying discipline that Indian courts could usefully adopt in construing Section 63, treating certification as answering only the question 'is this what it purports to be' and reserving the question of what the record proves for ordinary appreciation of evidence at trial. Third, the European Union's ex ante model suggests that continued institutional investment in standardised, tamper-evident acquisition tools and accredited timestamping infrastructure for Indian investigating agencies could reduce reliance on the ex post certification process and thereby ease the practical burden that Section 63(4)'s dual-certificate requirement currently places on prosecuting agencies.

Findings

Section 63 of the BSA substantially re-enacts the structure of Section 65B of the former Evidence Act, and the interpretative principles established in Anvar P.V. and Arjun Panditrao Khotkar — that certification is a mandatory condition precedent for secondary electronic evidence, and that the certificate need not accompany the record at filing but must exist by the stage of exhibition — should, on ordinary principles of statutory continuity, carry forward under the new provision.

The BSA's principal doctrinal innovation is the dual-signature certificate under Section 63(4), requiring both a device-operator's affirmation and an independent expert's technical certification, a change that raises the evidentiary standard but correspondingly increases dependence on the availability of qualified examiners.

The BSA's expert-certification requirement is conceptually and institutionally linked to the notified Examiner of Electronic Evidence mechanism under Section 79A of the IT Act, meaning the practical efficacy of Section 63(4) depends on the

24. Federal Rules of Evidence, rr 901, 902(13)–(14) (as amended, effective 1 December 2017); see G Joseph, 'Self-Authentication of Electronic Evidence: New Rules 902(13)-(14)' (Moore's Federal Practice, 3rd edn).

26. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation).

continued expansion of that notified-examiner infrastructure.

The BNSS's mandatory audio-video recording of search and seizure under Sections 105 and 185 supplies an additional, procedurally distinct safeguard against evidence-planting, but is not expressly cross-referenced with the BSA's certification regime, leaving their evidentiary interaction to be worked out by practice rather than by statutory design.

A textual gap exists in Section 105 of the BNSS concerning whether its audio-video recording requirement extends to the search of a person as opposed to a place, a gap of particular significance in cybercrime investigation given that mobile handsets are frequently seized from an accused's person.

No BSA-specific reported judgment of the Supreme Court squarely construing Section 63 on a contested point of first impression was identified in the course of this research; analysis of the new provision therefore necessarily proceeds by reasoned extrapolation from the Section 65B line of authority.

The certification model adopted by the BSA is more exacting than the presumption-based models operating in Singapore and under the Australian Uniform Evidence Acts, reflecting a continued legislative and judicial preference in India for affirmative, party-driven authentication over system-level presumptions of reliability.

The American separation between authentication as a threshold question and hearsay, relevance or confrontation objections as distinct downstream questions is not as sharply maintained in Indian practice, where production of a Section 63 certificate is sometimes treated as resolving the evidentiary inquiry in its entirety.

Neither the BSA nor the BNSS contains provisions specifically directed at the authentication or detection of AI-generated or deepfake digital content, leaving this emerging category of evidentiary risk to be addressed through general expert-evidence principles that were not designed with synthetic media in mind.

India's absence from the Budapest Convention on Cybercrime constrains the speed of cross-border evidence preservation and mutual legal assistance relative to jurisdictions that are parties to that Convention, a structural limitation independent of any domestic statutory reform.

Reliable, nationally comparable empirical data on forensic laboratory turnaround times, notified-examiner caseloads, and judicial training coverage on digital evidence appreciation is not available in the public domain in a form that would permit confident quantification of the scale of these practical challenges.

The constitutional right to privacy recognised in Justice K.S. Puttaswamy (Retd) v Union of India imposes a proportionality discipline on digital search, seizure and interception powers under the BNSS and the IT Act, a discipline whose consistent application in routine investigative practice cannot be verified from the available secondary literature.

The interaction between encryption and the privilege against self-incrimination under Article 20(3) of the Constitution — specifically, whether an accused can be compelled to furnish a password or biometric unlock — remains an unsettled question not directly addressed by the BSA, the BNSS or the IT Act.

Suggestions

Parliament, or the concerned rule-making authority, should consider clarifying by amendment or clarificatory rule whether a single, omnibus Section 63(4) certificate may cover a functionally related set of electronic exhibits (for example, a complete forensic image and its constituent extracted files) rather than requiring an item-by-item certificate for each discrete piece of output, to ease the practical burden in cybercrime matters involving voluminous digital exhibits.

The Ministry of Home Affairs and State Governments should expand the network of laboratories and personnel notified as Examiners of Electronic Evidence under Section 79A of the IT Act, with transparent, published criteria for accreditation, so that the dual-certificate requirement under Section 63(4) does not become a practical barrier to admissibility in areas presently underserved by notified experts.

The gap in Section 105 of the BNSS concerning audio-video recording of the search of a person, as distinct from a place, should be addressed by amendment or by an authoritative judicial or executive clarification, given its particular relevance to the seizure of mobile devices in cybercrime investigation.

The National Judicial Academy and State judicial academies should develop and standardise a structured curriculum on digital evidence appreciation, covering hash-value verification, metadata interpretation and network-log analysis, so

that trial judges are better equipped to evaluate the technical substance of certified electronic records rather than treating certification as dispositive.

Forensic science laboratories should adopt and publish standardised, nationally uniform protocols for forensic imaging, hash generation and chain-of-custody documentation, to reduce inter-laboratory variance in acquisition practice that can otherwise be exploited on cross-examination.

A dedicated statutory or regulatory framework for the authentication and detection of AI-generated and deepfake digital content should be developed, potentially incorporating provenance-metadata standards and accredited detection-tool certification, rather than leaving this emerging risk to be addressed solely through general expert-evidence principles.

Investigating agencies should be directed, through binding standing orders rather than mere administrative guidance, to record the hash value of a seized digital medium contemporaneously with the audio-video recording of the seizure mandated by Sections 105 and 185 of the BNSS, so that the chain-of-custody narrative and the Section 63 certification process are evidentially linked from the outset.

Consideration should be given to statutory clarification of the still-unsettled question whether an accused may be compelled to furnish a password or biometric credential to unlock a seized device, harmonising the position with the privilege against self-incrimination under Article 20(3) of the Constitution.

The Bureau of Police Research and Development should coordinate periodic, published data collection on forensic laboratory turnaround times and notified-examiner caseloads, to enable evidence-based policy review of the practical operation of Section 63 of the BSA, an area in which current empirical data is presently insufficient for confident assessment.

Capacity-building programmes for public prosecutors specifically on cybercrime evidentiary practice should be expanded, given the distinct technical and procedural demands of cyber-offence prosecutions relative to conventional criminal trials.

Courts should be encouraged, through practice directions, to expressly distinguish in their reasoning between the authentication of an electronic record (a threshold, admissibility-stage inquiry under Section 63) and the appreciation of its evidentiary weight (a trial-stage inquiry), so as to avoid the elision between these two distinct questions observed in some existing practice.

International cooperation frameworks between Indian and foreign forensic laboratories, including reciprocal recognition of forensic certification standards, should be explored to reduce delay in cases requiring cross-border technical verification of digital evidence.

Conclusion

The Bharatiya Sakshya Adhiniyam, 2023 does not represent a rupture with the pre-existing law of electronic evidence so much as a consolidation and modest refinement of it. By re-enacting the substance of Section 65B in Section 63, while superimposing a dual-signature certificate requirement, Parliament has signalled continued reliance on affirmative, party-driven certification as the gateway to admissibility, and has left largely undisturbed the interpretative scaffolding painstakingly constructed by the Supreme Court across *Navjot Sandhu*, *Anvar P.V.*, *Tomaso Bruno*, *Shafhi Mohammad* and *Arjun Panditrao Khotkar*.

Assessed against the two objectives set out at the beginning of this article, the analysis suggests that the statutory framework governing digital forensics and electronic evidence is coherent in its allocation of function across the BSA, the IT Act and the BNSS — admissibility, substantive offence and institutional certification infrastructure, and investigative procedure, respectively — but that this coherence is more evident on the page than it is likely to be in the day-to-day administration of cybercrime trials, where forensic capacity, judicial technical literacy and cross-border cooperation mechanisms remain the binding constraints rather than the drafting of the statutes themselves. The judicial trend, so far as it can be projected from the pre-2024 case law onto the new statutory text, favours continued strictness on certification balanced by a judicially supervised safety valve for cases of genuine impossibility, a balance that is defensible in principle but whose practical fairness depends entirely on whether the safety valve remains genuinely accessible to under-resourced litigants and investigating agencies rather than becoming, in practice, as difficult to invoke as the certificate requirement it is meant to soften.

Looking forward, the effectiveness of the BSA in the specific domain of cybercrime adjudication will likely turn less on further legislative amendment than on institutional investment: in the expansion of notified forensic examiners under Section 79A of the

IT Act, in standardised acquisition protocols across State forensic laboratories, in structured judicial training on the technical appreciation of digital evidence, and in a considered policy decision on India's participation in cross-border cybercrime cooperation frameworks. The most significant unaddressed frontier is the authentication of AI-generated content, an area in which neither the BSA nor the BNSS yet offers a tailored evidentiary response, and which is likely to dominate the next phase of judicial and legislative attention to electronic evidence in India. Future research employing empirical methods — systematic review of trial-court records, structured interviews with forensic examiners and prosecutors, and time-series analysis of forensic laboratory throughput — would usefully supplement the doctrinal account offered here, particularly given the recurring gaps in publicly available quantitative data that this article has been careful to flag rather than to fill with invented figures.

Bibliography

Cases

Anvar P.V. v P.K. Basheer (2014) 10 SCC 473

Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1

Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1

K. Ramajyam v Inspector of Police (2016) Crl LJ 1542 (Mad)

Shafhi Mohammad v State of Himachal Pradesh (2018) 2 SCC 801

State (NCT of Delhi) v Navjot Sandhu (2005) 11 SCC 600

Tomaso Bruno v State of Uttar Pradesh (2015) 7 SCC 178

Legislation

Bharatiya Nagarik Suraksha Sanhita 2023

Bharatiya Nyaya Sanhita 2023

Bharatiya Sakshya Adhiniyam 2023

Code of Criminal Procedure 1973 (repealed)

Constitution of India, arts 20(3), 21

Indian Evidence Act 1872 (repealed)

Information Technology Act 2000

Civil Evidence Act 1968 (UK)

Civil Evidence Act 1995 (UK)

Criminal Justice Act 2003 (UK)

Police and Criminal Evidence Act 1984 (UK)

Federal Rules of Evidence (US), rr 901, 902

Evidence Act (Singapore, Cap 97, 1997 rev edn, as amended)

Uniform Evidence Acts (Australia)

Regulation (EU) No 910/2014 (eIDAS Regulation)

Council of Europe, Convention on Cybercrime (Budapest, 23 November 2001) ETS No 185

Journal Articles

Aradhya Sethia, 'Rethinking Admissibility of Electronic Evidence' (2016) 24(3) International Journal of Law and Information Technology 229

Prachi Ratanpriya, 'A Detailed Analysis of Section 65B of the Indian Evidence Act' (2023) 2(3) [student law review]

SCC Online Blog, 'The decision in Arjun Panditrao: Admissibility of electronic evidence in India continues to face hurdles' (SCC Times, 7 June 2021)

Government and Official Reports

Bureau of Police Research and Development, Handbook for Police Officers on Bharatiya Nagarik Suraksha Sanhita, 2023 (Punjab Police Academy, Phillaur, 2024)

Bureau of Police Research and Development, session paper on Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023

Ministry of Home Affairs, Notification bringing into force the Bharatiya Sakshya Adhiniyam 2023, the Bharatiya Nyaya Sanhita 2023 and the Bharatiya Nagarik Suraksha Sanhita 2023 (effective 1 July 2024)

National Crime Records Bureau, Crime in India (annual series, Government of India)

PRS Legislative Research, The Bharatiya Nagarik Suraksha Sanhita, 2023: Bill text and legislative brief

Official Websites and Other Authoritative Sources

Bhatt & Joshi Associates, 'Electronic Evidence Under BSA 2023: Section 63 Certificate Requirements & Supreme Court Interpretation' (bhattandjoshiassociates.com)

K.S. & K. Legal Insights, 'Section 63 Bharatiya Sakshya Adhiniyam 2023' (ksandk.com)

Livelaw, 'Recording Of Search And Seizure Through Audio-Video Electronic Means Under Section 105 Of The BNSS' (livelaw.in, 2025)

Nyaaya, 'Electronic recording of search and seizure processes is mandatory now' (nyaaya.org, 2025)

Obhan & Associates, 'Introduction of the Bharatiya Nagarik Suraksha Sanhita, 2023: A Step Towards Digital India' (obhanandassociates.com)

P39A Criminal Law Blog, 'Criminal Law Bills 2023 Decoded #12: Audio-Video Recordings during Investigation' (p39ablog.com, 2023)

Cornell Law School Legal Information Institute, Federal Rules of Evidence, r 902 (law.cornell.edu)

American Bar Association, 'New Rules for Self-Authenticating Electronic Evidence' (americanbar.org)