IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, April 2026
Impact Factor: 8.2

Cybercrime Investigation and Digital Evidence Under the Bharatiya Sakshya Adhiniyam, 2023: A Critical Appraisal

Panchalingam. B
SRM School of Law, SRM University, Chennai

Abstract: *The enactment of the Bharatiya Sakshya Adhiniyam, 2023 (hereinafter "BSA") marks a watershed moment in India's jurisprudential landscape with respect to electronic evidence and cybercrime adjudication. Replacing the archaic Indian Evidence Act, 1872, the BSA introduces a sophisticated framework that acknowledges the primacy of digital records in contemporary criminal investigations. This paper examines the key statutory provisions of the BSA pertaining to cybercrime investigation and digital evidence, evaluating their interface with the Bharatiya Nagarik Suraksha Sanhita, 2023 (hereinafter "BNSS") and the Information Technology Act, 2000 (hereinafter "IT Act"). Through a critical analysis of legislative text and judicial precedents — including the landmark judgements in Anvar P.V. v. P.K. Basheer, Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, and Shreya Singhal v. Union of India — this article argues that while the BSA represent a commendable modernisation effort, it leaves certain structural lacunae that demands urgent legislative attention. The paper also examines challenges like forensic infrastructure deficits, chain of custody controversies, and the tension between state surveillance powers and the constitutionally guaranteed right to privacy.*

Keywords: *Bharatiya Sakshya Adhiniyam*

I. INTRODUCTION

India's criminal justice system underwent a fundamental transformation on July 1, 2024, when three new legislations simultaneously came into force: the Bharatiya Nyaya Sanhita, 2023[1] (hereinafter "BNS"), the BNSS,[2] and the BSA.[3] These legislations replaced colonial-era statutes that had governed India's criminal law for over a century. Among the three, the BSA occupies a particularly critical position in the context of cybercrime investigation, as it deals with the admissibility, relevance, and probative value of electronic and digital records — the very currency of modern crime.

The rapid proliferation of digital technology in India — marked by the surge in internet penetration, digital financial transactions, and social media usage — has given rise to a parallel expansion in cybercrime. The National Crime Records Bureau (NCRB) has consistently documented a sharp rise in cybercrime cases across the country. In this environment, the legal framework governing the collection, preservation, and presentation of digital evidence becomes not merely a procedural concern, but a fundamental guarantee of justice. The erstwhile Indian Evidence Act, 1872, though amended in 2000 to accomodate electronic records through the insertion of Sections 65A and 65B,[4] was widely acknowledged to be inadequate for the realities of twenty-first century digital crime.

The BSA makes several significant departures from the old framework. It reconceptualises electronic records as primary evidence, introduces a mandatory dual-certificate format for admissibility of computer outputs, and expands

[1]Bharatiya Nagarik Suraksha Sanhita, Act No. 46 of 2023 (India).
[2]Information Technology Act, Act No. 21 of 2000 (India).
[3]Bharatiya Sakshya Adhiniyam, Act No. 47 of 2023 (India), pmbl.

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, April 2026 Impact Factor: 8.2

the definition of "document" to include a wide range of digital storage and communication devices.[5] Read alongside the BNSS's mandate for audio-video recording of search and seizure,[6] mandatory forensic investigation at crime scenes,[7] and chain of custody documentation for electronic devices,[8] the new legal regime presents a coherent attempt to bring India's evidence law into the digital age.

This article proceeds in six parts. After this introduction, Part II surveys the statutory framework for digital evidence under the BSA, with particular attention to Sections 61, 62, and 63. Part III analyses the investigative framework under the BNSS as it pertains to cybercrime. Part IV undertakes a detailed discussion of judicial precedents that have shaped the admissibility of electronic records. Part V critically examines the lacunae in the current framework. Part VI offer concluding observations and recommendations.

II. DIGITAL EVIDENCE UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

A. Reconceptualising the "Document": Section 2(1)(d)

The definitional architecture of the BSA reveals its most foundational departure from the old Evidence Act. Section 2(1)(d) of the BSA expansively defines "document" to include electronic and digital records.[9] Illustration (vi) specifically includes e-mails, server logs, documents on computers, laptops, or smartphones, messages, websites, and voicemail messages stored on digital devices within the ambit of "document." This is a significant upgrading from the pre-BSA position, where electronic records were treated as secondary evidence requiring certification under Section 65B of the IEA.

The practical consequence of this definitional shift is enormous. Under the old regime, electronic evidence occupied a somewhat precarious evidentiary position — valuable in fact but procedurally fragile. Under the BSA, the legal character of digital records is unambiguously affirmed, providing investigators and prosecutors with a more stable foundation for building cases that rest heavily on digital evidence.

B. Section 61: The Non-Discrimination Principle

Section 61 of the BSA is a provision of landmark importance. It categorically states that nothing in the Act shall be used to deny the admissibility of an electronic or digital record as evidence on the basis that it is an electronic or digital record.[10] Such records, subject to the certification requirement in Section 63, shall have the same legal effect, validity, and enforceability as other documents. This provision essentially codifies a principle of non-discrimination against digital evidence, aligning India's evidentiary law with the global trend towards technological neutrality in evidence law.

C. Electronic Records as Primary Evidence: Section 57

Under the BSA, electronic and digital records are treated as primary evidence in a number of scenarios. Section 57, read with its explanations, makes clear that where an electronic or digital record is created or stored simultaneously or sequentially in multiple files, each such file constitutes primary evidence.[11] Explanation 5 provides that where an electronic or digital record is produced from proper custody and is not disputed, it is likewise treated as primary evidence.[12] Explanation 6 similarly confers primary evidence status on each stored recording where a video is

[5]Bharatiya Sakshya Adhiniyam, Act No. 47 of 2023, § 2(1)(d) (India).
[6]Bharatiya Nagarik Suraksha Sanhita, Act No. 46 of 2023, § 105 (India).
[7]Bharatiya Nagarik Suraksha Sanhita, Act No. 46 of 2023, § 176(3) (India).
[8]Bharatiya Nagarik Suraksha Sanhita, Act No. 46 of 2023, § 193(2)(i) (India).

[10]Bharatiya Sakshya Adhiniyam, Act No. 47 of 2023, § 61 (India).
[11]Bharatiya Sakshya Adhiniyam, Act No. 47 of 2023, § 57, Explanation 4 (India).
[12]Bharatiya Sakshya Adhiniyam, Act No. 47 of 2023, § 57, Explanation 5 (India).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, April 2026 Impact Factor: 8.2

simultaneously transmitted, broadcast, or stored in electronic form.[13] Explanation 7 further extends this treatment to records stored in multiple storage spaces within a computer resource, including temporary files.[14]

This is a dramatic shift from the previous legal position under the IEA, where electronic records were uniformly classified as secondary evidence, requiring compliance with the stringent certification requirements of Section 65B. The reclassification of electronic records as primary evidence under the BSA has significant implications for how cybercrime cases are built and presented before courts.

D. Section 62 and Section 63: Admissibility of Electronic Records

Section 62 of the BSA serves as a gateway provision, stipulating that the contents of electronic records may be proved in accordance with the provisions of Section 63.[15] Section 63 then sets out the detailed conditions for admissibility of electronic records — specifically computer outputs — as evidence.

Section 63(1) provides that any information contained in an electronic record that is printed on paper, stored in optical or magnetic media, or semiconductor memory, produced by a computer or any communication device, shall be deemed to be a document admissible in evidence.[16] Critically, Section 63(3) broadens the definition of "computer" or "communication device" to encompass networks of computers and communication devices, as well as any combination thereof.[17]

The most significant innovation of Section 63 is the dual-certificate requirement in sub-section (4).[18] Unlike the old Section 65B(4) of the IEA, which required only a single certificate signed by a competent person in charge of the device, Section 63(4) mandates a certificate signed by both (a) the person responsible for the device, and (b) an expert. This certificate must follow the prescribed format set out in the Schedule to the BSA,[19] which divides the certificate into Part A (to be completed by the person in charge of the device) and Part B (to be completed by the expert).

Part B requires the expert to state the hash value of the electronic/digital record and the algorithm through which the hash was obtained. A hash value is a unique numeric value representing the contents of a file or dataset — the SHA-256 algorithm being the National Institute of Standards and Technology's recommended standard. By requiring hash verification in the expert's certificate, the BSA introduces a scientific standard for the authentication of digital records that was entirely absent under the old framework. Section 63(5) further specifies that information shall be taken to be supplied to a computer if it is supplied to a combination of any such devices or computer systems.[20]

III. THE INVESTIGATIVE FRAMEWORK UNDER THE BNSS, 2023

A. Mandatory Audio-Video Recording: Section 105

Section 105 of the BNSS is a landmark provision that directly addresses one of the most persistent criticisms of police investigation in India — the lack of transparency and accountability in the conduct of searches and seizures. Under this provision, the entire process of conducting a search or seizing property, including the preparation of the seizure list and the signing of such list by witnesses, must be recorded through audio-video electronic means, preferably by mobile phone.[21] The police officer is required to forward such recording without delay to the District Magistrate, Sub-Divisional Magistrate, or the Judicial Magistrate of the First Class.

---

[13]Bharatiya Sakshya Adhiniyam, Act No. 47 of 2023, § 57, Explanation 6 (India).
[14]Bharatiya Sakshya Adhiniyam, Act No. 47 of 2023, §§ 57, 63, Explanation 7 (India).
[15]Bharatiya Sakshya Adhiniyam, Act No. 47 of 2023, § 62 (India).
[16]Bharatiya Sakshya Adhiniyam, Act No. 47 of 2023, § 63(1) (India).
[17]Bharatiya Sakshya Adhiniyam, Act No. 47 of 2023, § 63(3) (India).
[18]Bharatiya Sakshya Adhiniyam, Act No. 47 of 2023, § 63(4) (India).
[19]Bharatiya Sakshya Adhiniyam, Act No. 47 of 2023, Schedule, Parts A & B (India).
[20]Bharatiya Sakshya Adhiniyam, Act No. 47 of 2023, § 63(5) (India).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, April 2026 Impact Factor: 8.2

The significance of Section 105 for cybercrime investigation can scarcely be overstated. In cybercrime cases, electronic devices — smartphones, laptops, hard drives, servers — are frequently the primary loci of evidence. The seizure of these devices is often the most critical step in the investigation. By making audio-video recording of this process mandatory, Section 105 creates an independent evidentiary record that can corroborate or contradict claims about how and when devices were seized, by whom, and in what condition — directly bearing on the chain of custody of the digital evidence subsequently extracted from those devices.

Similarly, Section 185 of the BNSS mandates that copies of any audio-video recordings from searches must be sent within forty-eight hours to the Magistrate empowered to take cognisance of the offence.[22] The Madhya Pradesh High Court has specifically observed that the BNSS has the potential to revolutionise the collection and presentation of evidence during criminal trials, particularly through the integration of information and communication technology in investigation.

B. Mandatory Forensic Investigation: Section 176(3)

Section 176(3) of the BNSS introduces a provision of considerable importance for serious cybercrime cases. It mandates the visit of a forensic expert to the crime scene for the collection of forensic evidence in cases of offences punishable with seven years of imprisonment or more, and further requires that the process of forensic evidence collection be video-recorded on a mobile phone or other electronic device.[23] This provision represents a decisive shift from the previously confession-driven model of investigation to a modern, evidence-based one.

Additionally, Section 176(1) of the BNSS provides an option for audio-video recording of statements made during police investigation.[24] While this is not mandatory in the same way as Section 176(3), it represents an important safeguard against torture and coercion during custodial interrogations — concerns which have been repeatedly flagged in the context of cybercrime investigations where technical complexity can lead to prolonged interrogations.

C. Chain of Custody Documentation: Section 193(2)(i)

Section 193(2)(i) of the BNSS mandates that a police report must include the chronology of custody in cases involving electronic devices.[25] This is a critically important provision from the perspective of cybercrime prosecution. The "chain of custody" — a documented record of who handled a piece of evidence, at what time, and in what manner — is fundamental to the admissibility and probative value of digital evidence. Any break in the chain of custody can raise doubts about the integrity of the evidence and potentially render it inadmissible.

In cybercrime cases, the digital evidence — whether it is a hard drive image, a seized smartphone, or network log files — can be corrupted or altered with relative ease compared to physical evidence. The statutory mandate of chain of custody documentation under the BNSS thus fills a critical procedural gap that previously existed in the investigation of cybercrimes.

D. Enhanced Powers of Search and Seizure: Section 94

Section 94 of the BNSS grants the police broader powers to seize electronic devices and records.[26] This is a significant expansion of the investigative toolkit in cybercrime cases. The provision must, however, be read in light of the constitutional guarantee of the right to privacy recognised by the Supreme Court in *K.S. Puttaswamy v. Union of India*,[27] which held that the right to privacy is a fundamental right under Article 21 of the Constitution. The extraction of data from electronic devices necessarily implicates this right, and any exercise of the power under Section 94 must satisfy the constitutional test of proportionality.

---

[22] Bharatiya Nagarik Suraksha Sanhita, Act No. 46 of 2023, § 185 (India).

[24] Bharatiya Nagarik Suraksha Sanhita, Act No. 46 of 2023, § 176(1) (India).

[26] Bharatiya Nagarik Suraksha Sanhita, Act No. 46 of 2023, § 94 (India).

[27] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, April 2026 Impact Factor: 8.2

IV. JUDICIAL PRECEDENTS: SHAPING THE ADMISSIBILITY OF DIGITAL EVIDENCE

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

The first significant Supreme Court pronouncement on electronic evidence arose in *State (NCT of Delhi) v. Navjot Sandhu*,[28] also known as the Parliament Attack Case. The Court held that electronic records could be admitted as evidence even without a certificate under Section 65B(4), allowing oral secondary evidence in certain circumstances. While this judgement represented an early and pragmatic approach to digital evidence, it was subsequently criticised for conflating the standards applicable to primary and secondary electronic evidence, and was eventually overruled.

B. Anvar P.V. v. P.K. Basheer (2014): The Certificate Mandate

The landmark three-judge bench judgment in *Anvar P.V. v. P.K. Basheer*,[29] overruled *Navjot Sandhu* and established that Section 65B(4) of the IEA is a mandatory procedural requirement for the admissibility of secondary electronic evidence. The Court held that Sections 65A and 65B constitute a "complete code" with respect to electronic records, and that oral evidence cannot substitute for the mandatory certificate. This judgement fundamentally shaped the landscape of cybercrime prosecution, establishing the certificate as a sine qua non for the admissibility of computer outputs.

The Court in *Anvar P.V.* further clarified that "source and authenticity are the two key factors for an electronic evidence." This formulation remains central to the evidentiary philosophy of the BSA, which doubles down on certification requirements by adding the expert certificate under Section 63(4). The judgment in *Sanjaysinh Ramrao Chavan v. Dattatray Gulabrao Phalke*,[30] reaffirmed this principle, holding that compliance with Section 65B is mandatory for the use of electronic evidence in judicial proceedings.

C. Shafhi Mohammad v. State of Himachal Pradesh (2018): Brief Relaxation

The two-judge bench decision in *Shafhi Mohammad v. State of Himachal Pradesh*,[31] introduced a degree of flexibility by holding that the certificate requirement under Section 65B(4) could be relaxed in the interest of justice, particularly in cases where the party adducing the evidence did not have possession or control over the device. However, this decision was delivered by a bench of lesser strength and was therefore in tension with the three-judge bench ruling in *Anvar P.V.* The resulting confusion necessitated a reference to a larger bench.

D. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020): Restoring Certainty

The three-judge bench judgment in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*,[32] delivered by Justices R.F. Nariman, S. Ravindra Bhat, and V. Ramasubramanian, conclusively resolved the conflict between *Anvar P.V.* and *Shafhi Mohammad*. The Court reaffirmed that the certificate requirement under Section 65B(4) is a mandatory condition precedent to the admissibility of electronic evidence as secondary evidence. *Shafhi Mohammad* was expressly overruled as being contrary to the law laid down in the three-judge bench decision in *Anvar P.V.*

The Court, however, introduced an important clarification: where the original electronic device itself is produced before the court as primary evidence — for instance, where the owner of a laptop or mobile phone steps into the witness box and testifies about the information stored therein — no Section 65B(4) certificate is required. This distinction between primary and secondary electronic evidence, now codified in the BSA, is a cardinal feature of the current legal framework. Additionally, the Court directed that where a party is unable to obtain the requisite certificate, an application may be made to the court for compelling the production of such certificate from the person in possession of the device.

[28] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600 (India).
[29] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).
[30] Sanjaysinh Ramrao Chavan v. Dattatray Gulabrao Phalke, (2015) 3 SCC 123 (India).
[31] Shafhi Mohammad v. State of Himachal Pradesh, (2018) 5 SCC 311 (India).
[32] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, April 2026 Impact Factor: 8.2

E. Shreya Singhal v. Union of India (2015): Balancing Cybercrime Law with Free Speech

Although not directly concerned with the admissibility of electronic evidence, the two-judge bench judgment in *Shreya Singhal v. Union of India*,[33] is foundational to any discussion of India's cybercrime legal framework. The Supreme Court struck down Section 66A of the IT Act, which criminalised the sending of "offensive" messages through communication devices, declaring it to be "open-ended and unconstitutionally vague," and in violation of Article 19(1)(a) of the Constitution. The Court held that the provision failed to qualify as a "reasonable restriction" under Article 19(2) and was thus void *ab initio*.

The *Shreya Singhal* judgment raises critical questions about the BNS's successor provisions addressing cybercrimes. Section 111 of the BNS, which deals with organised crime including cybercrimes,[34] has been criticised for its definitional ambiguity with respect to what constitutes a "cybercrime." If similarly vague penal provisions are enacted and used by the state to target legitimate digital speech, the spectre of *Shreya Singhal* will loom large over any prosecution premised on such provisions.

F. K.S. Puttaswamy v. Union of India (2017): Privacy as a Fundamental Right

The nine-judge bench constitution in *K.S. Puttaswamy v. Union of India*,[35] unanimously held that the right to privacy is a fundamental right forming part of the right to life and personal liberty under Article 21 of the Constitution. The judgment has profound implications for cybercrime investigation. Every exercise of state power to seize electronic devices, intercept communications, or extract personal data from devices must satisfy the constitutional test of proportionality — the state must demonstrate a legitimate aim, and the means employed must be both necessary and proportionate to that aim.

In the context of digital evidence, this means that the broad powers granted to the police under Section 94 of the BNSS[36] and Section 69 of the IT Act[37] to seize devices and intercept communications must be exercised with a degree of precision and restraint that the law currently does not mandatorily prescribe. As noted by legal scholars, regulations to be issued under the Digital Personal Data Protection Act, 2023[38] may in the future offer guidance to authorities extracting data from electronic devices, ensuring that such extractions are proportionate as mandated by *Puttaswamy*.

V. CRITICAL ANALYSIS: LACUNAE AND CHALLENGES

A. The "Expert" Conundrum under Section 63(4)

The most significant structural lacuna in the BSA is the failure to define who qualifies as an "expert" for the purposes of signing Part B of the certificate under Section 63(4).[39] The Act is conspicuously silent on the qualifications, accreditation, or institutional affiliation required of such experts. This creates a dual problem: on the one hand, it invites challenges to the admissibility of electronic evidence on the grounds that the signing expert is not adequately qualified; on the other, it risks the proliferation of inadequately credentialed individuals certifying the authenticity of complex digital records.

The infrastructure problem is equally acute. A 2023 study revealed that there are only fifteen notified forensic labs under Section 79A of the IT Act,[40] causing significant delays — digital evidence analysis in Maharashtra, for instance, reportedly takes eight to twelve months. The mandatory involvement of experts in the certification process under Section 63(4) will only intensify the pressure on this already stretched forensic infrastructure. As one commentator has

[33]Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
[34]Bharatiya Nyaya Sanhita, Act No. 45 of 2023, § 111 (India).

[36]Information Technology Act, Act No. 21 of 2000, § 69 (India).
[37]Digital Personal Data Protection Act, Act No. 22 of 2023 (India).

[39]Information Technology Act, Act No. 21 of 2000, § 79A (India).
[40]State of Rajasthan v. Kashi Ram, (2006) 12 SCC 254 (India).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, April 2026 Impact Factor: 8.2

aptly observed, the BSA's expert certification model "presumes access to both institutional capacity and qualified experts — an assumption that falters due to insufficiency of Indian Forensic Science Laboratories."

B. Chain of Custody: Practical Implementation Gaps

While the BNSS's mandate of chain of custody documentation under Section 193(2)(i) is commendable in principle, its practical implementation faces serious challenges. Indian law enforcement agencies, particularly at the state level, often lack the training, equipment, and institutional protocols necessary to maintain a forensically sound chain of custody for digital evidence.

Hash verification — the gold standard for demonstrating the integrity of digital evidence — requires specialised software tools like FTK Imager, Cellebrite, or EnCase, which may not be available at the scene of seizure or in all cybercrime police stations. The Supreme Court in *State of Rajasthan v. Kashi Ram*,[41] had emphasised the necessity of preserving the chain of custody for all forms of evidence. However, in the context of digital evidence, compliance with this mandate requires technical capacity that is still unevenly distributed across India's law enforcement apparatus.

C. Transitional Challenges and Pending Cases

The repeal savings clause of the BSA provides that any pending application, trial, inquiry, investigation, or appeal shall be dealt with under the Indian Evidence Act, 1872 as if the BSA had not come into force.[42] This transitional provision, while legally necessary, creates a bifurcated evidence regime — cases under the IEA standard (with its single Section 65B certificate) continuing alongside new cases under the BSA (with its dual-certificate requirement). Courts and practitioners must navigate both frameworks simultaneously, increasing the risk of procedural confusion.

Furthermore, any retroactive alignment of old electronic evidence with the new BSA standards risks raising suspicions of tampering or rehashing of data. The Supreme Court in *Arjun Panditrao* had emphasised the sanctity of the certification process; the transitional period demands particular care to ensure that the evidentiary integrity of digital records collected under the old framework is not compromised by attempts to shoe-horn them into the new certification format.

D. Privacy, Surveillance, and the Right to Digital Due Process

The expanded powers of seizure under Section 94 of the BNSS,[43] combined with the interception and decryption powers under Sections 69 and 69A of the IT Act,[44] create a formidable apparatus of state surveillance in the cybercrime context. While these powers are necessary for effective cybercrime investigation, they must be exercised within the constitutional framework established by *Puttaswamy*. At present, there is no mandatory judicial warrant requirement before the police can seize an electronic device under Section 94 of the BNSS in cognisable offence cases, raising significant concerns about the potential for overreach.

The *Arnesh Kumar v. State of Bihar*,[45] guidelines mandating that law enforcement must substantiate the need for arrest rather then treating it as a routine measure, are applicable to cybercrime cases as well. These guidelines must be read alongside the *Puttaswamy* proportionality framework to ensure that the investigation of cybercrime does not become a vehicle for disproportionate intrusions into the privacy of citizens.

E. The Question of Deepfakes and Synthetic Digital Evidence

The BSA does not address the admissibility or authentication standards for AI-generated or synthetic digital evidence — a significant oversight given the rapid proliferation of deepfake technology. Courts in India have issued takedown orders for deepfakes in personality rights cases, but no clear statutory standard exists for the authentication of such evidence in criminal proceedings. The hash-value certification mechanism under Section 63(4) was designed for conventional digital records and may be inadequate for synthetic media whose provenance is inherently contested.

---

[41] Pawan Kumar v. State of Haryana, (2017) 10 SCC 261 (India).

[44] Arnesh Kumar v. State of Bihar, (2014) 8 SCC 273 (India).

[45] Bharatiya Sakshya Adhiniyam, Act No. 47 of 2023, §§ 61–63 r/w Schedule (India).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, April 2026 Impact Factor: 8.2

This challenge is compounded by the fact that Section 330 of the BNSS provides that an expert witness is required to appear in court only if their report is formally contested by the opposite party. This means that expert certificates under Section 63(4) that go unchallenged escape adversarial scrutiny — a potentially serious gap in cases involving synthetic or manipulated digital evidence where the very authenticity of the expert's certification may be in question.

VI. CONCLUSION AND RECOMMENDATIONS

The Bharatiya Sakshya Adhiniyam, 2023 represents a significant and overdue modernisation of India's law of evidence, particularly with respect to digital and electronic records. By reconceptualising electronic records as primary evidence,[46] introducing a dual-certificate format anchored in hash verification,[47] and affirming the principle of non-discrimination against digital evidence under Section 61,[48] the BSA lays a more solid evidentiary foundation for cybercrime prosecution than its predecessor. Complemented by the BNSS's provisions for mandatory audio-video recording of search and seizure under Section 105,[49] compulsory forensic investigation under Section 176(3),[50] and chain of custody documentation under Section 193(2)(i),[51] the new legal framework is a commendable, if imperfect, achievement.

However, the paper has identified several structural lacunae that warrant immediate legislative and administrative attention. The failure to define the qualifications of the "expert" under Section 63(4) is a critical drafting omission that must be remedied, ideally through subsidiary legislation prescribing minimum qualifications and accreditation requirements. The capacity deficits in forensic infrastructure must be urgently addressed through sustained investment in Forensic Science Laboratories and the training of forensic personnel. The chain of custody protocols for digital evidence must be standardised through uniform guidelines issued by the Ministry of Home Affairs.

More fundamentally, the framework for cybercrime investigation must be anchored in a robust commitment to the constitutional right to privacy recognised in *Puttaswamy*. The powerful investigative tools available to law enforcement under the IT Act and the BNSS must be exercised proportionately, with adequate judicial oversight at the pre-seizure stage. In this regard, India may benefit from studying comparative models such as the United Kingdom's Extraction of Information from Electronic Devices: Code of Practice (2022), which provides structured procedural safeguards for state extraction of data from devices.

The BSA is a beginning, not an endpoint. As India's digital economy deepens and cybercrime becomes increasingly sophisticated — incorporating AI-generated evidence, blockchain transactions, and deepfake technology — the legal framework governing digital evidence will require continual recalibration. The courts, legislature, and the legal community must work in concert to ensure that the promise of the BSA translates into effective, rights-respecting justice in India's digital era.