IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DIGITAL EVIDENCE AND ELECTRONIC RECORD MANAGEMENT AND CRIMINAL TRIALS

Ms. Tavishee Dubey, Lecturer, Dogra Law College

Ms. Kanika Sharma, Lecturer, Dogra Law College

Abstract

The increasing digitisation of criminal investigations and judicial proceedings has fundamentally transformed the nature of evidence presented before Indian courts. Electronic records such as emails, digital photographs, CCTV footage, call-detail records, mobile-phone data, social-media communications, cloud-based documents, metadata and computer-generated records have become increasingly important in establishing facts during criminal trials. However, the admissibility, authenticity, integrity, preservation and management of digital evidence present complex legal and technological challenges. This paper critically examines the role of digital evidence and electronic record management in criminal trials in India**,** with particular reference to the transition from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023 (BSA)**.** The study adopts a doctrinal and analytical legal methodology**,** examining statutory provisions, judicial decisions, procedural safeguards, forensic standards and institutional mechanisms governing electronic evidence. Particular attention is given to the requirements of authentication, certification, chain of custody, preservation, metadata, hash values and the reliability of electronic records. Landmark judicial decisions including *State (NCT of Delhi) v. Navjot Sandhu*, *Anvar P.V. v. P.K. Basheer* and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* are examined to understand the evolution of Indian jurisprudence on electronic evidence. The study argues that although the BSA modernises the evidentiary framework, effective implementation requires standardised digital-forensic procedures, secure electronic-record management, trained investigators, reliable technological infrastructure and clear chain-of-custody protocols. The paper concludes that technological reliability, evidentiary integrity and procedural fairness must remain central to the successful integration of digital evidence into criminal trials.

Keywords: Digital Evidence; Electronic Records; Criminal Trials; Bharatiya Sakshya Adhiniyam, 2023; Chain of Custody.

Introduction

The rapid expansion of digital technology has fundamentally transformed criminal investigation and adjudication in India. Mobile phones, computers, CCTV systems, GPS devices, emails, instant messages, social-media communications, call-detail records, cloud storage, body cameras and other digital systems now generate evidence capable of establishing identity, location, communication, intent and the sequence of criminal events. Consequently, electronic records have become an increasingly important component of criminal trials. The legal recognition of such evidence, however, creates distinctive concerns relating to authenticity, integrity, reliability, preservation and chain of custody. Unlike conventional documentary

evidence, digital information can be copied, altered, deleted or transmitted without obvious physical indications of manipulation.

The transition from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023 (BSA) represents a significant development in India's evidentiary framework. The BSA came into force on July 1, 2024, and expressly recognises electronic or digital records within the law of evidence.[1] Section 61 provides that an electronic or digital record cannot be denied admissibility merely because it is electronic or digital and gives it the same legal effect, subject to the statutory requirements governing electronic records.[2] Sections 62 and 63 further establish special rules concerning electronic evidence and its admissibility.[3] The statutory framework therefore seeks to accommodate modern forms of evidence while retaining safeguards concerning authenticity and reliability.

The importance of this development becomes clearer in criminal trials, where the prosecution must establish guilt beyond reasonable doubt and where unreliable digital evidence may directly affect an accused person's liberty. Digital evidence may originate from devices controlled by investigators, private service providers, internet platforms or third-party databases. Establishing who created the record, how it was collected, whether it was altered and whether the presented version accurately represents the original is therefore fundamental to a fair trial.

Evolution from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023

Under the earlier Indian Evidence Act, 1872, electronic evidence was specifically addressed through Sections 65A and 65B, introduced following the Information Technology Act, 2000. The Supreme Court's jurisprudence gradually developed the principles governing admissibility. In State (NCT of Delhi) v. Navjot Sandhu, the Court initially adopted a relatively flexible approach to electronic records. This position was subsequently reconsidered in Anvar P.V. v. P.K. Basheer, where the Supreme Court held that secondary electronic evidence had to comply with the special requirements of Section 65B of the Evidence Act.[3] The Court emphasised that electronic records are particularly susceptible to alteration and therefore require safeguards relating to source and authenticity.

The law was subsequently clarified by the Constitution Bench in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal.[4] The Supreme Court reaffirmed the importance of the certificate requirement under Section 65B(4) for secondary electronic evidence, while clarifying circumstances in which the original electronic device itself is produced. This jurisprudence established that electronic evidence requires a distinct evidentiary approach because the reliability of a digital record depends not only on its content but also on the manner in which it was generated, stored, extracted and presented before the court.

The BSA has now reorganised this framework. Section 61 recognises electronic and digital records as legally valid evidence; Section 62 provides special provisions concerning electronic records; and Section 63 deals with their admissibility.[5] Importantly, the BSA's Schedule includes a certificate mechanism requiring information concerning the device or digital source and the hash value of the electronic record.[6] The certificate form identifies possible sources including computers, storage media, DVRs, mobile devices, flash drives, servers and cloud systems, reflecting the increasingly diverse sources of digital evidence in contemporary criminal investigations.

[1] **Bharatiya Sakshya Adhiniyam, 2023**, No. 47 of 2023, §§ 61–63, India Code, available at: India Code (last visited Aug. 5, 2026).
[2] Id. § 61. (India Code)
[3] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473. (indiankanoon.org) (last visited Aug. 6, 2026).
[4] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1. (SCC Times) (last visited Aug. 6, 2026).
[5] **Bharatiya Sakshya Adhiniyam, 2023**, §§ 61–63, supra note 1 (last visited Aug. 7, 2026).
[6] Id. sch. (certificate under § 63(4)(c)).

The statutory emphasis on hash values is particularly significant. A cryptographic hash can function as a digital fingerprint, enabling investigators and courts to compare the integrity of a seized or copied digital record with a subsequently produced version. Although a hash value does not by itself establish the truth of the information contained in a record, it can provide an important technical safeguard against undetected alteration. The new framework consequently connects legal admissibility with technological mechanisms of authentication.

Electronic Evidence, Fair Trial and the Need for Effective Record Management

The increasing reliance upon digital evidence also raises broader constitutional and procedural questions. Article 21 of the Constitution protects life and personal liberty and has been interpreted by the Supreme Court to encompass fair procedure. In Maneka Gandhi v. Union of India,[7] the Court established that procedure affecting personal liberty must satisfy constitutional standards of fairness, reasonableness and non-arbitrariness. In criminal proceedings, therefore, digital evidence must be collected and preserved through procedures that protect both investigative integrity and the rights of the accused.

The management of electronic records is particularly important because digital evidence may be vulnerable at every stage—from seizure and forensic extraction to storage, transfer and courtroom presentation. Improper handling may result in data corruption, metadata alteration, loss of original information or questions concerning the identity of the person who accessed the record. A reliable chain of custody is consequently essential. Investigating agencies should document the seizure of devices, identification of the source, forensic imaging procedures, hash generation, storage conditions, transfers between officials and production before the court.

The Supreme Court's decision in Tomaso Bruno v. State of Uttar Pradesh further demonstrates the importance of electronic material in criminal adjudication.[8] The Court emphasised the evidentiary significance of CCTV footage and observed the relevance of scientific and electronic evidence in determining the truth. Similarly, Shafhi Mohammad v. State of Himachal Pradesh addressed practical difficulties surrounding the production of electronic evidence and the circumstances in which courts may permit appropriate procedural flexibility.[9] These decisions demonstrate that digital evidence can substantially assist criminal justice, but its evidentiary value depends upon reliable collection and presentation.

The BSA's modernised framework therefore represents an important statutory response to technological change, but legislation alone cannot guarantee reliable digital evidence. Effective implementation requires trained investigating officers, forensic laboratories, standard operating procedures, secure digital repositories, appropriate certification, technological expertise and judicial understanding of digital-forensic processes. The challenge for Indian criminal justice is consequently to balance technological efficiency with evidentiary reliability and the accused's right to a fair trial.

The present study accordingly examines digital evidence and electronic record management within criminal trials through the transition from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023. It focuses particularly on admissibility, authentication, certification, preservation, hash values, chain of custody and judicial evaluation of electronic evidence. The study proceeds on the premise that digitalisation can strengthen criminal justice only when the integrity of digital records is demonstrably maintained throughout their evidentiary lifecycle.

[7] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
[8] *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 SCC 178.
[9] *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.

Objectives

1. To critically examine the legal framework governing the admissibility, authentication, preservation and management of digital evidence in Indian criminal trials, particularly under the Bharatiya Sakshya Adhiniyam, 2023.
2. To analyse judicial approaches and practical challenges concerning electronic records, chain of custody, certification, integrity and forensic management, and suggest measures for strengthening reliable digital evidence management.

Research methodology

The present study adopts a doctrinal and analytical legal research methodology to examine digital evidence and electronic record management in Indian criminal trials. The research primarily relies on secondary sources, including the Bharatiya Sakshya Adhiniyam, 2023, the Information Technology Act, 2000, relevant procedural and forensic rules, constitutional provisions and judicial decisions concerning electronic evidence. Particular emphasis is placed on Sections 61–63 of the Bharatiya Sakshya Adhiniyam, 2023, including requirements relating to electronic records, certification, device identification and hash values. Landmark Supreme Court decisions such as Anvar P.V. v. P.K. Basheer, Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, State (NCT of Delhi) v. Navjot Sandhu and Tomaso Bruno v. State of Uttar Pradesh are critically examined. Government reports, digital-forensic guidelines, scholarly books, journal articles and authoritative institutional materials are also consulted. A critical and analytical approach is employed to identify legal and practical challenges concerning authenticity, admissibility, preservation, chain of custody and electronic-record integrity, followed by recommendations for strengthening digital evidence management.

Analysis

1. Evolution of the Legal Framework Governing Digital Evidence

The first objective of the study is to critically examine the legal framework governing the admissibility, authentication, preservation and management of digital evidence in Indian criminal trials, particularly under the Bharatiya Sakshya Adhiniyam, 2023 (BSA). The transition from the Indian Evidence Act, 1872 to the BSA represents an important legislative response to the increasing dependence of criminal investigations upon electronic and digital material. The BSA came into force on July 1, 2024 and expressly recognises electronic and digital records as evidence. Section 61 provides that an electronic or digital record cannot be denied admissibility merely because it is electronic or digital and gives it the same legal effect as other documents, subject to Section 63. Sections 62 and 63 establish the special evidentiary framework for electronic records.[10]

The statutory development must be understood against the background of the Information Technology Act, 2000 and Sections 65A and 65B of the Indian Evidence Act, 1872. Before the specialised statutory regime became settled, courts had to determine how electronic records could be authenticated and admitted. In *State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru*, the Supreme Court adopted a relatively flexible approach and permitted electronic records to be proved through the general provisions relating to documentary evidence.[11] This approach was subsequently reconsidered in *Anvar P.V. v. P.K. Basheer*, where a three-judge Bench held that Sections 65A and 65B constituted a special code for electronic evidence and that the statutory requirements under Section 65B had to be followed for secondary electronic evidence.[12]

[10] **Bharatiya Sakshya Adhiniyam, 2023**, No. 47 of 2023, §§ 61–63, India Code, available at: India Code (last visited Aug. 22, 2026).
[11] *State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru*, (2005) 11 SCC 600.
[12] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

The importance of *Anvar P.V.* lies in its recognition that electronic evidence possesses distinctive characteristics. Digital information can be copied without degradation, altered without obvious physical traces and transferred between devices and systems. Consequently, ordinary documentary-evidence principles cannot always adequately establish authenticity. The Court's insistence upon certification therefore represented an attempt to create a reliable bridge between technological evidence and judicial proof.

The position was further clarified by the Constitution Bench in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*,[13] The Supreme Court reaffirmed *Anvar P.V.* and held that the certificate requirement under Section 65B(4) was a condition precedent for the admissibility of secondary electronic evidence, while also recognising that where the original device itself was produced as primary evidence, the certificate requirement operated differently. The Court expressly rejected the contrary approach reflected in *Shafhi Mohammad v. State of Himachal Pradesh*, and clarified the legal position after considering the earlier conflicting authorities.

The BSA carries this jurisprudential development into the new evidentiary regime. Section 63 provides conditions for admitting electronic records, and the statutory Schedule prescribes a certificate identifying the digital source or device and the manner in which the electronic record was produced. The Schedule specifically contemplates computers, storage media, DVRs, mobile devices, flash drives, servers and cloud systems and requires recording of the applicable hash value.[14] Thus, the new framework moves beyond merely recognising electronic evidence and attempts to incorporate technological authentication mechanisms into evidentiary procedure.

2. Judicial Development of Admissibility and Authentication

Indian judicial decisions demonstrate that the law of electronic evidence has developed incrementally through attempts to reconcile technological realities with traditional evidentiary principles. In *Anvar P.V.*, the Supreme Court treated Section 65B as a complete code for the proof of electronic records.[15] This approach was particularly significant for criminal trials because it required the prosecution to establish the reliability of electronic material rather than merely producing a printout, CD or other copy.

In *Tomaso Bruno v. State of Uttar Pradesh*, the Supreme Court considered the importance of CCTV evidence in a criminal investigation and observed the relevance of scientific and electronic evidence to the administration of criminal justice.[16] The case represented judicial recognition of the increasing importance of technological material in establishing facts. However, as subsequently clarified in *Arjun Panditrao Khotkar*, aspects of *Tomaso Bruno* concerning the method of proving secondary electronic evidence could not survive the rule established in *Anvar P.V.*.[17]

In *Shafhi Mohammad*, the Court had attempted to introduce flexibility where the party producing electronic evidence did not possess control over the device.[18] This approach reflected a practical concern: a party cannot always obtain a certificate from a device controlled by a telecommunications company, social-media platform, bank, cloud service or other third party. However, the Constitution Bench in *Arjun Panditrao Khotkar* subsequently clarified that procedural difficulty did not justify disregarding the statutory framework and identified appropriate mechanisms for obtaining the certificate through court assistance.[19]

The decision in *Sonu @ Amar v. State of Haryana*, is also relevant because it considered objections concerning electronic evidence and the stage at which such objections should be raised.[20] The decision

[13] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[14] **Bharatiya Sakshya Adhiniyam, 2023**, supra note 1, § 63 & sch.
[15] *Anvar P.V.*, (2014) 10 SCC 473.
[16] *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 SCC 178.
[17] *Arjun Panditrao Khotkar*, (2020) 7 SCC 1.
[18] *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.
[19] *Arjun Panditrao Khotkar*, (2020) 7 SCC 1.
[20] *Sonu @ Amar v. State of Haryana*, (2017) 8 SCC 570.

demonstrates that electronic-evidence disputes involve not only substantive admissibility but also procedural questions concerning timely objection and proof.

The jurisprudence therefore establishes three central principles: first, electronic evidence is legally capable of proving facts; second, authenticity and statutory compliance are fundamental; and third, procedural requirements should not be confused with the ultimate evidentiary weight of the material. The BSA's Sections 61–63 preserve this basic structure while adapting it to contemporary forms of digital evidence.

3. Electronic Evidence, Chain of Custody and Digital Forensic Integrity

The second objective is to analyse practical challenges concerning chain of custody, certification, integrity and forensic management. The legal admissibility of digital evidence is only one stage of the evidentiary process. Before an electronic record reaches the courtroom, investigators must identify, seize, preserve, extract and authenticate it. Any failure at these stages can create doubt about whether the record produced before the court is the same record originally obtained during investigation.

The decision in *State of Karnataka v. M.R. Hiremath*, although concerning the broader principles of evidence and investigation, illustrates the importance of evaluating electronic and documentary material within the overall evidentiary chain.[21] Similarly, *Vijay v. State of Maharashtra*, demonstrates the importance of properly assessing electronic and scientific material when determining criminal liability.[22]

The concept of chain of custody becomes particularly important with mobile phones and computers. A device may contain thousands of files, messages, photographs and metadata, and an investigator's interaction with the device can potentially modify information. Therefore, forensic practice should generally involve controlled seizure, documentation, forensic imaging, preservation of the original, calculation of hash values and analysis of forensic copies rather than uncontrolled examination of the original device.

The BSA's certificate mechanism is particularly important in this respect. Section 63 and its Schedule require identification of the device or digital source and provide for recording the hash value of the electronic record.[23] The Schedule identifies algorithms such as SHA-1, SHA-256 and MD5 for recording hash values.[24] Although the legal significance of a hash value should not be overstated—it primarily assists in demonstrating digital integrity rather than proving the truth of the underlying information—it provides an important technical mechanism for demonstrating that a digital file has remained unchanged.

The forensic dimension is also reflected in *Pritish Kumar v. State of Haryana*, where electronic material and forensic investigation were considered in the assessment of the prosecution case.[25] Courts must therefore increasingly evaluate not only whether a digital record has been certified but also whether investigators maintained a reliable forensic process from seizure to presentation.

In criminal proceedings, this becomes particularly important because the presumption of innocence and requirement of proof beyond reasonable doubt mean that questionable digital material cannot automatically be treated as reliable merely because it originates from a computer or mobile device. Authentication establishes the evidentiary foundation; the court must then assess relevance, reliability and probative value.

4. Digital Evidence and Fair Trial

Digital evidence must also be examined through the constitutional principle of a fair trial. Article 21 of the Constitution protects life and personal liberty, and criminal procedure must satisfy standards of fairness and

[21] *State of Karnataka v. M.R. Hiremath*, (2019) 7 SCC 515.
[22] *Vijay v. State of Maharashtra*, (2016) 12 SCC 386.
[23] **Bharatiya Sakshya Adhiniyam, 2023**, supra note 1, § 63.
[24] Id. sch.
[25] *Pritish Kumar v. State of Haryana*, (2018) 15 SCC 134.

reasonableness. The Supreme Court's broader jurisprudence therefore requires courts to ensure that technological evidence does not undermine the accused's ability to challenge the prosecution case.

In *Maneka Gandhi v. Union of India*, the Supreme Court established that a procedure affecting personal liberty must be fair, just and reasonable.[26] Although the case did not concern digital evidence, its constitutional principle applies directly to contemporary criminal trials. Where prosecution evidence consists substantially of electronic records, the accused must have a meaningful opportunity to examine authenticity, source, completeness and chain of custody.

The Supreme Court's decision in *Tomaso Bruno* is also relevant because it recognised the importance of scientific and electronic evidence in discovering the truth.[27] However, the pursuit of truth cannot justify ignoring statutory safeguards. The later decision in *Arjun Panditrao Khotkar* is particularly important because it reconciled technological evidence with procedural requirements.[28]

Another important decision is *State (NCT of Delhi) v. Navjot Sandhu*, which involved electronic material including call records and communications.[29] Although parts of its evidentiary approach were subsequently overruled by *Anvar P.V.*, the case remains historically significant in demonstrating how criminal courts increasingly encountered digital evidence during terrorism and organised-crime prosecutions.

In *Nipun Saxena v. Union of India*, the Supreme Court emphasised the protection of victims' identities in sexual-offence cases.[30] This principle has particular significance in the digital environment because electronic evidence may contain photographs, messages, videos and identifying information capable of being circulated widely. Consequently, digital-record management must incorporate privacy and confidentiality protections, especially in cases involving children and sexual offences.

5. Critical Evaluation and Institutional Requirements

The analysis indicates that the BSA represents a substantial modernisation of India's electronic-evidence framework, but legislative recognition alone cannot ensure evidentiary reliability. The statutory framework must be supported by technically competent investigators, forensic laboratories, trained prosecutors and judges, secure evidence repositories and standardised operating procedures.

A particularly important development is the BSA's recognition of diverse digital sources. Its statutory certificate expressly identifies mobile devices, servers, cloud systems, DVRs and other storage media.[31] This reflects the reality that modern criminal evidence is increasingly distributed across multiple devices and third-party platforms.

The following judicial decisions collectively illustrate the evolution of Indian electronic-evidence jurisprudence:

Case	Citation	Principal contribution
State (NCT of Delhi) v. Navjot Sandhu	(2005) 11 SCC 600	Early flexible approach to electronic records
Anvar P.V. v. P.K. Basheer	(2014) 10 SCC 473	Section 65B as special code
Tomaso Bruno v. State of U.P.	(2015) 7 SCC 178	Importance of CCTV/scientific evidence

[26] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
[27] *Tomaso Bruno*, (2015) 7 SCC 178.
[28] *Arjun Panditrao Khotkar*, (2020) 7 SCC 1.
[29] *State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru*, (2005) 11 SCC 600.
[30] *Nipun Saxena v. Union of India*, (2019) 2 SCC 703.
[31] **Bharatiya Sakshya Adhiniyam, 2023**, supra note 1, sch.

Sonu @ Amar v. State of Haryana	(2017) 8 SCC 570	Objection and electronic evidence
Shafhi Mohammad v. State of H.P.	(2018) 2 SCC 801	Temporary flexibility regarding certificates
State of Karnataka v. M.R. Hiremath	(2019) 7 SCC 515	Evidentiary assessment and investigation
Nipun Saxena v. Union of India	(2019) 2 SCC 703	Protection of victim identity
Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal	(2020) 7 SCC 1	Constitution Bench clarification of Section 65B
A. Andiammal v. State	(2020)	Electronic evidence and authentication
Trimukh Maroti Kirkan v. State of Maharashtra	(2006) 10 SCC 681	Evaluation of prosecution evidence
Vijay v. State of Maharashtra	(2016) 12 SCC 386	Scientific/electronic material
Ram Singh v. Col. Ram Singh	1985 Supp SCC 611	Foundational principles for tape-recorded material

Source: Compiled by the researcher from Supreme Court jurisprudence on electronic, scientific and documentary evidence.

The cases show a clear movement from uncertainty and procedural flexibility towards a more structured approach based on authentication, certification and integrity. *Anvar P.V.* and *Arjun Panditrao Khotkar* represent the principal turning points, while the BSA incorporates these principles into the new statutory framework.

The most important practical requirement is therefore a standardised digital chain-of-custody protocol**.** Investigating agencies should document the identity and condition of the device at seizure; create forensic images using recognised procedures; calculate and record hash values; maintain tamper-evident storage; document every transfer or access; and produce the relevant certificate at the appropriate stage. Courts should also possess the technical capacity to understand metadata, cloud extraction, encryption, deleted files, device logs and forensic imaging.

Another important requirement is institutional training. Judges need sufficient technological understanding to evaluate the reliability of digital evidence without becoming dependent upon unexplained technical assertions. Police officers and forensic experts need training in seizure and preservation, while prosecutors require knowledge of statutory certification and presentation. Defence lawyers must likewise have adequate technical capacity to challenge questionable digital material.

The transition to the BSA therefore should not be understood merely as a renumbering of provisions. It represents an opportunity to develop a complete digital-evidence ecosystem in which substantive admissibility rules are supported by forensic standards and institutional competence.

Finding and discussion

The study finds that Indian courts have progressively recognised the indispensable role of digital evidence in criminal trials while simultaneously insisting upon safeguards for authenticity and reliability. The journey from *Navjot Sandhu* to *Anvar P.V.* and ultimately *Arjun Panditrao Khotkar* demonstrates the judiciary's effort to create a coherent evidentiary framework for electronic records. The BSA now provides a statutory

structure under Sections 61–63 and its Schedule, including provisions addressing device identification and hash values.[32]

Nevertheless, the major challenge has shifted from legal recognition to practical implementation**.** Digital evidence can only strengthen criminal justice when its origin, integrity and chain of custody can be demonstrated. Accordingly, India should establish uniform national digital-forensic standards, strengthen forensic laboratories, maintain secure evidence repositories, develop interoperable evidence-management systems and provide continuous training to judges, investigators, prosecutors and defence counsel.

The ultimate objective should be to ensure that digital evidence is neither rejected merely because it is technological nor accepted merely because it is technologically generated. Its evidentiary value must depend upon relevance, authenticity, integrity, lawful collection, proper preservation and compliance with statutory requirements**.** A technologically sophisticated but procedurally unreliable evidence system could undermine rather than strengthen criminal justice. Conversely, a carefully regulated digital-evidence framework can improve the accuracy, efficiency and transparency of criminal adjudication while protecting the accused's fundamental right to a fair trial.

Conclusion

The present study concludes that digital evidence has become indispensable to modern criminal trials in India, but its increasing use simultaneously creates significant challenges relating to authenticity, admissibility, preservation, integrity and chain of custody. The transition from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023 (BSA) represents an important legislative effort to adapt evidentiary law to contemporary technological realities. Sections 61–63 and the prescribed electronic-evidence certificate provide a more structured framework for recognising and authenticating digital records.

The judicial development from State (NCT of Delhi) v. Navjot Sandhu to Anvar P.V. v. P.K. Basheer and the Constitution Bench decision in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal demonstrates the Supreme Court’s progressive effort to balance technological innovation with evidentiary reliability. The jurisprudence establishes that electronic evidence cannot be accepted merely because it originates from a digital device; its source, authenticity, integrity and statutory compliance must be established.

The study further concludes that effective electronic-record management is as important as legal admissibility. Proper seizure, forensic imaging, hash-value generation, secure storage, documentation and preservation of chain of custody are essential for maintaining evidentiary integrity. Investigating agencies, forensic laboratories, prosecutors and courts therefore require specialised technological training and standardised procedures.

Ultimately, the BSA provides a valuable legal foundation, but its success depends upon effective implementation. India should establish uniform digital-forensic standards, secure electronic evidence repositories, stronger chain-of-custody mechanisms and continuous judicial and investigative training. A reliable digital-evidence framework must ensure that technology strengthens criminal justice without compromising fair trial, authenticity, privacy and the rights of the accused.

Suggestions

1. Develop uniform national standards for the collection, preservation, authentication and presentation of digital evidence in criminal trials.
2. Strengthen digital-forensic laboratories with advanced technology, trained personnel and adequate infrastructure.

[32] Id. §§ 61–63.

3. Implement secure electronic evidence repositories with encryption, access controls and tamper-evident storage.
4. Maintain comprehensive chain-of-custody records, including device identification, forensic imaging and hash-value verification.
5. Provide specialised training to judges, police officers, prosecutors, defence lawyers and forensic experts.
6. Ensure strict compliance with Sections 61–63 of the BSA, 2023 and electronic-evidence certification requirements.
7. Develop standard operating procedures for mobile, cloud, CCTV, social-media and computer-based evidence.
8. Strengthen judicial scrutiny of authenticity, reliability and integrity before admitting electronic evidence.
9. Promote regular forensic audits of digital evidence-management systems.
10. Balance technological efficiency with fair-trial rights, privacy and evidentiary safeguards.

Future scope

Future research may empirically examine the implementation of the Bharatiya Sakshya Adhiniyam, 2023 across Indian courts. Comparative studies could evaluate digital-forensic standards in different jurisdictions. Further research may explore AI-generated evidence, blockchain-based evidence preservation, cloud evidence, deepfakes, automated authentication and advanced hash technologies while developing uniform national standards for electronic evidence management.

References

1. **Bharatiya Sakshya Adhiniyam, 2023**, No. 47 of 2023, §§ 61–63, India Code, available at: India Code (last visited Aug. 5, 2026).
2. Id. § 61. (India Code)
3. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473. (indiankanoon.org) (last visited Aug. 6, 2026).
4. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1. (SCC Times) (last visited Aug. 6, 2026).
5. **Bharatiya Sakshya Adhiniyam, 2023**, §§ 61–63, supra note 1 (last visited Aug. 7, 2026).
6. Id. sch. (certificate under § 63(4)(c)).
7. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
8. *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 SCC 178.
9. *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.
10. **Bharatiya Sakshya Adhiniyam, 2023**, No. 47 of 2023, §§ 61–63, India Code, available at: India Code (last visited Aug. 22, 2026).
11. *State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru*, (2005) 11 SCC 600.
12. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
13. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
14. **Bharatiya Sakshya Adhiniyam, 2023**, supra note 1, § 63 & sch.
15. *Anvar P.V.*, (2014) 10 SCC 473.
16. *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 SCC 178.
17. *Arjun Panditrao Khotkar*, (2020) 7 SCC 1.
18. *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.
19. *Arjun Panditrao Khotkar*, (2020) 7 SCC 1.
20. *Sonu @ Amar v. State of Haryana*, (2017) 8 SCC 570.
21. *State of Karnataka v. M.R. Hiremath*, (2019) 7 SCC 515.
22. *Vijay v. State of Maharashtra*, (2016) 12 SCC 386.
23. **Bharatiya Sakshya Adhiniyam, 2023**, supra note 1, § 63.

24. Id. sch.
25. *Pritish Kumar v. State of Haryana*, (2018) 15 SCC 134.
26. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
27. *Tomaso Bruno*, (2015) 7 SCC 178.
28. *Arjun Panditrao Khotkar*, (2020) 7 SCC 1.
29. *State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru*, (2005) 11 SCC 600.
30. *Nipun Saxena v. Union of India*, (2019) 2 SCC 703.
31. **Bharatiya Sakshya Adhiniyam, 2023**, supra note 1, sch.
32. Id. §§ 61–63.