Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14,issue.32s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Digital Evidence under the Indian Legal System – Study of Problems and Perspective

Himani Raj Goyal[1], Dr. Mahaveer Prasad Mali[2]

[1]Research Scholar Nims University, Jaipur, Rajasthan
Email ID : Himanirajgoyal@Gmail.Com
[2]Associate Professor Nims University, Jaipur, Rajasthan
Email ID : Mpsaini399@Gmail.Com

Cite this paper as Himani Raj Goyal, Dr. Mahaveer Prasad Mali.(2025) Digital Evidence under the Indian Legal System – Study of Problems and Perspective .Journal of Neonatal Surgery, 14, (32s), 10180-10189

ABSTRACT

The proliferation of digital technologies has reshaped the evidentiary landscape in India, where electronic records now play a decisive role in criminal prosecutions, civil disputes, and commercial litigation. The Indian Evidence Act, 1872, as supplemented by the Information Technology Act, 2000, laid the foundation for the admissibility of electronic records, but persistent interpretative challenges particularly surrounding Section 65B certificates led to judicial uncertainty until the Constitution Bench ruling in Arjun Panditrao Khotkar. The recent enactment of the Bharatiya Sakshya Adhiniyam, 2023, seeks to modernize evidentiary law by refining procedural rules for digital records, yet difficulties remain in ensuring authenticity, reliability, and due process safeguards.

This paper critically examines the concept and nature of digital evidence, statutory provisions under the IEA and BSA, and judicial interpretations shaping its admissibility. It highlights key problems such as tampering risks, inadequate forensic infrastructure, cloud and cross-border data challenges, and privacy concerns in light of Puttaswamy. The study further evaluates the evidentiary value of expert opinion, chain of custody principles, and international best practices. Finally, it proposes reforms including blockchain-based authentication, a Digital Evidence Authority, judicial training, and enhanced global cooperation, arguing for a balanced regime that integrates technological innovation with constitutional safeguards in digital justice delivery.

Keywords: Digital Evidence, Electronic Records, Evidentiary Standards, Cyber Forensics, Privacy and Due Process, Section 65B Certification..

1. INTRODUCTION

The 21st century has witnessed an unprecedented expansion of the digital ecosystem in India, transforming the very foundation of communication, commerce, governance, and social interaction. With over 850 million internet users, India today stands as one of the world's largest digital societies, marked by the proliferation of smartphones, fintech platforms, e-governance services, and online marketplaces.[1] This rapid digitization has not only revolutionized economic activity but has also led to a parallel rise in digital interactions, transactions, and disputes. As a natural consequence, the Indian judicial system is increasingly confronted with digital evidence ranging from emails, social media posts, CCTV footage, call data records, blockchain transactions, and metadata, to complex forensic trails of cyber offences.

CCTV footage, call data records, blockchain transactions, and metadata, to complex forensic trails of cyber offences.

The reliance on digital evidence is no longer confined to cases of cybercrime but extends across the spectrum of criminal, civil, and commercial litigation. In criminal law, electronic records such as call detail records (CDRs), GPS locations, and surveillance videos have become pivotal in proving the presence or conduct of the accused.[2] In civil disputes, particularly those involving contracts, intellectual property, or financial transactions, courts increasingly depend on digital records such as electronic contracts, encrypted messages, or payment gateways to establish liability. Similarly, in the commercial arena, disputes relating to e-commerce, digital payments, and corporate governance often necessitate reliance on electronic records. The Supreme Court of India, in several landmark cases, has recognised that electronic evidence can often be more reliable than oral testimony, provided that statutory safeguards are observed.

However, despite legislative recognition under the Information Technology Act, 2000, the Indian Evidence Act, 1872 (IEA),

[1] Telecom Regulatory Authority of India (TRAI), The Indian Telecom Services Performance Indicators (Oct.–Dec. 2023), https://trai.gov.in
[2] State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru, (2005) 11 S.C.C. 600 (India).

and now the Bharatiya Sakshya Adhiniyam, 2023 (BSA), the admissibility and appreciation of digital evidence remain fraught with problems and uncertainties. The requirement of a Section 65B certificate under the IEA (now Section 63 BSA), while intended to ensure authenticity, has been a persistent source of procedural challenges and inconsistent judicial interpretation.[3] Questions regarding the volatility of electronic records, ease of manipulation, chain of custody, and forensic expertise continue to undermine confidence in digital evidence.

Against this backdrop, the present study seeks to critically examine the problems surrounding the admissibility and appreciation of digital evidence under the Indian legal system. It aims to analyse the statutory framework, judicial interpretations, and practical difficulties faced by investigators, prosecutors, and litigants. At the same time, the paper attempts to offer a forward-looking perspective by suggesting reforms necessary to align evidentiary law with the demands of a digital and data-driven society. Ultimately, the objective is to assess whether the current evidentiary regime adequately balances technological realities, procedural fairness, and constitutional rights such as privacy and due process

CONCEPT AND NATURE OF DIGITAL EVIDENCE

2.1 Definitions

The legal recognition of electronic or digital evidence in India has evolved through successive legislative enactments and amendments.

Information Technology Act, 2000

The IT Act, 2000, was India's first comprehensive legislation to acknowledge electronic records. Section 2(1)(t) defines an "electronic record" to mean "data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer-generated microfiche."[4] This inclusive definition ensures that digital material, irrespective of its storage medium, is placed at par with traditional documents.

Indian Evidence Act, 1872 (as amended in 2000)

The Indian Evidence Act, 1872, originally drafted in a pre-digital era, was amended by the IT Act to integrate electronic records within the evidentiary framework. Section 3 of the IEA expanded the definition of "evidence" to include electronic records, while Sections 65A and 65B prescribed special procedures for proving such records. Section 45A further allowed expert opinion from the Examiner of Electronic Evidence.[5]

Bharatiya Sakshya Adhiniyam, 2023 (BSA)

The BSA 2023, which replaces the IEA, has retained the recognition of electronic records as evidence. Section 2(1)(d) defines "document" to include "any information stored, recorded or copied in any electronic form". Section 57 corresponds to the old Section 65A, while Section 63 parallels Section 65B, requiring a certificate for admissibility of electronic records produced as secondary evidence.[6] Importantly, Section 61 of the BSA retains the provision on expert opinion regarding electronic evidence, mirroring Section 45A of the IEA. Thus, statutory continuity ensures that electronic records remain admissible provided authenticity and reliability are established.

2.2 Nature of Digital Evidence

The inherent characteristics of digital evidence distinguish it from traditional forms of proof, creating unique challenges for admissibility and appreciation.

Volatility – Electronic data is volatile and fragile, capable of being lost through accidental deletion, power failures, or routine overwriting. Unlike paper documents, digital records require proper forensic protocols to ensure their preservation.[7]

Duplicability – Unlike physical documents, digital records can be copied infinitely without degradation of quality. While this ensures easy dissemination, it also raises issues concerning the "original" document. Courts are often confronted with identical versions, complicating questions of authenticity.

Vulnerability to Tampering – Digital records are highly susceptible to alteration, manipulation, or fabrication through technological tools. Metadata can be changed without leaving visible traces, thereby raising concerns of evidentiary reliability. The Supreme Court in Anvar P.V. v. P.K. Basheer highlighted that electronic records are inherently susceptible to tampering, which justifies the statutory safeguards under Section 65B.[8]

These attributes make it necessary for digital evidence to be assessed with greater caution than conventional documents.

---

[3] Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India), Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1 (India).
[4] Information Technology Act, 2000, § 2(1)(t).
[5] Indian Evidence Act, 1872 (as amended by the IT Act, 2000), §§ 3, 65A, 65B, 45A.
[6] Bharatiya Sakshya Adhiniyam, 2023, §§ 2(1)(d), 57, 61, 63.
[7] D.P. Mittal, *Law of Information Technology* (Taxmann, 2021) at 421.
[8] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

2.3 Types of Digital Evidence

Digital evidence may broadly be divided into primary and secondary evidence, akin to documentary evidence in general law:

Primary Digital Evidence – This refers to the original electronic record stored in the primary device, such as the hard disk, server, or mobile phone on which the data was first created or stored. For instance, the original hard drive containing CCTV footage or the mobile phone containing WhatsApp chats qualifies as primary digital evidence. Under Section 62 of the IEA (now Section 57 BSA), such evidence is admissible as of right without additional certification.

Secondary Digital Evidence – This refers to derivative forms of electronic records, such as printouts, screenshots, CDs, pen drives, or copies of the original stored on another medium. Such evidence requires compliance with Section 65B of the IEA or Section 63 of the BSA, mandating a certificate of authenticity from the person in control of the device. In Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, the Supreme Court reiterated that such certification is mandatory and cannot be relaxed.

Thus, while primary electronic evidence enjoys straightforward admissibility, secondary electronic evidence is admissible only upon strict compliance with statutory safeguards to ensure its reliability.

3. Legislative Framework Governing Digital Evidence in India

3.1 Indian Evidence Act, 1872 (IEA)

The Indian Evidence Act, 1872 (IEA) was not originally equipped to deal with digital realities, as it was drafted in a colonial era where oral testimony and paper-based documents were the primary sources of proof. However, with the advent of the Information Technology Act, 2000, crucial amendments were made to the IEA to bring electronic records within its fold. These amendments sought to integrate digital material into the evidentiary process, thereby ensuring that the law kept pace with technological transformation.

Sections 61 to 65 of the IEA laid down the rules regarding documentary evidence, distinguishing between primary evidence (the original document itself) and secondary evidence (copies or derivatives). By extending the definition of "documents" to include electronic records, the law ensured that original electronic devices (hard drives, servers, memory cards, etc.) could be treated as primary evidence under Section 62, while derivative forms such as printouts, CDs, or screenshots were admissible only as secondary evidence subject to statutory safeguards.[9] This framework provided the baseline for admitting digital material in courts.

The most significant innovation came with the insertion of Sections 65A and 65B. Section 65A created a special rule for electronic evidence, mandating that it be proved only in the manner laid down under Section 65B. Section 65B, in turn, prescribed the detailed procedure for admissibility of electronic records, especially when produced in secondary form. It required that any electronic record generated by a computer must be accompanied by a certificate of authenticity signed by a person occupying a responsible position in relation to the operation of the device.[10] This certificate was designed to guarantee that the electronic record was produced in the ordinary course of operation, free from manipulation or alteration.

Judicial interpretation of these provisions significantly shaped their application. In Anvar P.V. v. P.K. Basheer, the Supreme Court held that Section 65B was a complete code in itself and that the certificate requirement under Section 65B(4) was mandatory for admissibility. The Court categorically ruled that oral evidence or expert opinion cannot substitute for this statutory requirement. This strict approach was reaffirmed in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, where a three-judge bench clarified that without such a certificate, secondary electronic evidence is inadmissible, irrespective of its probative value. While these decisions enhanced the integrity of electronic records, they also created significant procedural hurdles in cases where the party relying on the record did not control the device (e.g., telecom companies, social media platforms).

Further, Section 45A of the IEA recognised the importance of technical expertise by making the opinion of the "Examiner of Electronic Evidence" a relevant fact. This provision acknowledged that judges, trained primarily in law, may lack the technical ability to assess the authenticity of complex electronic data. It thus allowed reliance on government-notified forensic experts for validation. However, in practice, the shortage of notified experts and forensic infrastructure has limited the effectiveness of this safeguard.

3.2 Bharatiya Sakshya Adhiniyam, 2023 (BSA)

The Bharatiya Sakshya Adhiniyam, 2023 (BSA), which replaced the IEA, continues to recognize electronic records as admissible evidence while attempting to modernize and simplify evidentiary rules. Though substantively similar to the IEA framework, the BSA adopts a clearer legislative drafting style, aligning it with the digital governance model envisioned by the Criminal Law Reforms Committee.

---

[9] Indian Evidence Act, 1872, §§ 61–65.
[10] Indian Evidence Act, 1872, §§ 65A–65B (as amended by the IT Act, 2000).

Section 57 corresponds to the earlier Section 65A of the IEA, providing that the contents of electronic records shall be proved only in accordance with the special rules contained in Section 63. Section 63 parallels Section 65B, reiterating the mandatory requirement of a certificate for admissibility of secondary electronic records.[11] Like its predecessor, this provision ensures that the authenticity of electronic records is verified by someone in lawful control of the device or the system, thereby reducing the risk of tampering. However, the BSA has not substantively altered the certificate requirement, despite long-standing criticism from practitioners and scholars who argue that it creates unnecessary obstacles to justice.

Section 61 of the BSA mirrors Section 45A of the IEA, retaining the admissibility of expert opinion on electronic evidence. Courts may thus continue to rely on forensic experts and government-appointed examiners to assess the authenticity of electronic data. Notably, the BSA integrates the definition of "documents" under Section 2(1)(d) to include information "stored, recorded, or copied in electronic form," which provides a more contemporary and inclusive formulation. This ensures that evolving forms of digital content, such as blockchain records or cloud-stored documents, fall within the definition of admissible documentary evidence.

3.3 Interconnected Statutes

The framework for digital evidence in India does not operate in isolation under the IEA or BSA; it is deeply interconnected with other statutes that regulate recognition, preservation, and admissibility of electronic records.

The Information Technology Act, 2000 serves as the foundational legislation for electronic governance in India. Sections 4 to 7 validate the use of electronic records and digital signatures, ensuring their enforceability in law. Section 79A empowers the Central Government to designate an "Examiner of Electronic Evidence," whose opinion holds evidentiary weight under Section 45A IEA and Section 61 BSA. This statutory linkage between the IT Act and evidentiary law ensures that electronic signatures, encryption, and authentication mechanisms are legally recognised.

Procedural aspects of search, seizure, and preservation of electronic records fall within the ambit of the Code of Criminal Procedure, 1973 (CrPC) and its successor, the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS). Section 91 CrPC (now Section 94 BNSS) empowers courts and investigating officers to require the production of documents, including electronic records. Similarly, provisions relating to search and seizure of premises and devices (Sections 100–102 CrPC, now Sections 101–103 BNSS) apply equally to digital devices.

Additionally, several special legislations integrate electronic evidence into their frameworks. The Prevention of Money Laundering Act, 2002 (PMLA) routinely relies on digital financial records and transaction trails. The Income Tax Act, 1961 incorporates electronic returns and digital databases for enforcement and adjudication. Similarly, the Companies Act, 2013 mandates electronic maintenance of corporate records and permits their evidentiary use. These overlapping provisions underscore the interdisciplinary nature of digital evidence, cutting across criminal, civil, and regulatory domains.

4. Judicial Approach towards Digital Evidence

The interpretation of digital evidence in India has largely been judge-made, as statutory clarity often lagged behind technological developments. Courts have played a pivotal role in shaping the admissibility standards under the Indian Evidence Act, 1872 (IEA), and this continues in the context of the Bharatiya Sakshya Adhiniyam, 2023 (BSA). A chronological reading of landmark cases highlights both judicial uncertainty and eventual harmonization of principles regarding Section 65B of the IEA and its successor provisions under the BSA.

4.1 State v. Navjot Sandhu (2005)

In State v. Navjot Sandhu, popularly known as the Parliament Attack case, the Supreme Court adopted a relatively flexible approach toward electronic evidence. It held that even if the mandatory certificate under Section 65B of the IEA was absent, electronic records such as call data records could still be admitted through oral evidence under Sections 63 and 65 of the IEA.[12] This expansive reading diluted the special procedure envisaged under Section 65B and created scope for admission of uncertified electronic records, thereby compromising the safeguard against tampering and fabrication. While this judgment facilitated the use of electronic records in urgent criminal trials, it simultaneously created interpretive ambiguity.

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

Nearly a decade later, the Supreme Court in Anvar P.V. v. P.K. Basheer recalibrated the legal standard. Overruling Navjot Sandhu, the Court categorically held that the certificate under Section 65B(4) was mandatory for admissibility of secondary electronic records.[13] The Court clarified that electronic evidence, being a species of documentary evidence, must follow the special procedure prescribed by Sections 65A and 65B, rather than the general rules of secondary evidence under Sections 63 and 65. This judgment restored the legislative intent behind Section 65B and sought to strengthen evidentiary reliability

[11] Bharatiya Sakshya Adhiniyam, 2023, §§ 57, 61, 63.
[12] State v. Navjot Sandhu, (2005) 11 S.C.C. 600 (India).
[13] Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India).

by emphasizing certification. However, critics argued that it imposed an onerous burden, especially when electronic evidence was procured from third-party service providers beyond the control of litigants.

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

Supreme Court carved out an exception to the rigidity imposed by Anvar. It held that where a party was not in possession of the device producing the electronic record, the requirement of a certificate under Section 65B could be relaxed.[14] The Court invoked the principle of justice and fair play to ensure that technicalities did not defeat substantive justice. Although well-intentioned, this judgment revived confusion by reintroducing judicial discretion contrary to the textual mandate of Section 65B.

4.4 Arjun Panditrao Khotkar v. Kailash Kushanrao (2020)

Recognizing the conflicting precedents, a Constitution Bench in Arjun Panditrao Khotkar v. Kailash Kushanrao authoritatively settled the law. It reaffirmed Anvar and expressly overruled Shafhi Mohammad, holding that Section 65B certification is a mandatory requirement for the admissibility of secondary electronic evidence.[15] The Court further clarified that the certificate is a condition precedent, not a procedural formality, and is integral to ensuring the authenticity and reliability of electronic records. Importantly, it held that if a party is unable to secure the certificate, remedies such as issuing a court direction under procedural law may be invoked. This decision restored doctrinal coherence while balancing evidentiary safeguards with access to justice.

4.5 Post-2023: Anticipated Interpretation of the BSA

With the enactment of the BSA, 2023, Section 63 essentially replaces Section 65B of the IEA while retaining the requirement of a certification for electronic records. Section 57 parallels Section 65A by reinforcing the special status of electronic evidence, and Section 61 corresponds to Section 45A on expert opinion. The continuity of statutory language suggests that the judicial interpretations under the IEA, particularly Arjun Panditrao, will remain highly persuasive in the application of the BSA. However, it is anticipated that courts may adopt a more nuanced approach in light of evolving technologies such as cloud storage, blockchain verification, and artificial intelligence–generated evidence, where certificate production may be practically complex. The BSA thus offers an opportunity for the judiciary to balance procedural safeguards with technological adaptability, ensuring that the evidentiary regime remains robust yet flexible.

5. Evidentiary Value of Expert Opinion

The authentication of digital evidence often requires specialized technical knowledge that lies beyond the competence of ordinary courts. Recognizing this need, both the Indian Evidence Act, 1872 (IEA) and its successor, the Bharatiya Sakshya Adhiniyam, 2023 (BSA), provide explicit provisions for expert opinion in relation to electronic records. While such opinions are invaluable in verifying the integrity and origin of digital material, they are not conclusive and remain subject to judicial evaluation.

5.1 Section 45A of the IEA

Section 45A was inserted into the IEA through the Information Technology (Amendment) Act, 2008 to address the unique challenges posed by electronic records. It provides that the opinion of the "Examiner of Electronic Evidence," appointed under Section 79A of the Information Technology Act, 2000, is relevant when the court has to form an opinion on any matter relating to electronic records. This provision institutionalized the role of specialized forensic examiners and underscored the legislature's recognition that electronic records are susceptible to manipulation, requiring expert verification of their authenticity. However, the statutory language frames expert opinion as relevant evidence, not as binding, leaving room for judicial scrutiny.

5.2 Section 61 of the BSA

The BSA, 2023 retains and refines this principle in Section 61, which corresponds to Section 45A of the IEA. It continues to empower courts to rely on the expertise of examiners of electronic evidence but does not elevate their opinion to the status of determinative proof. The continuity indicates legislative intent to maintain a balance between technological expertise and judicial discretion. While Section 61 strengthens the evidentiary framework in the context of modern technologies like cloud computing and blockchain, the ultimate decision remains vested with the judiciary, ensuring that the probative value of expert opinion is weighed against other evidence.

5.3 Role of Forensic Examiners in Authentication

Forensic experts play a pivotal role in verifying the integrity of digital records, particularly in establishing chain of custody, detecting tampering, and retrieving deleted or encrypted data. Their reports are critical in cases involving cybercrimes,

[14] Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 S.C.C. 801 (India).
[15] Arjun Panditrao Khotkar v. Kailash Kushanrao, (2020) 7 S.C.C. 1 (India).

financial frauds, terrorism, and even matrimonial disputes where electronic communications form crucial evidence.[16] The statutory recognition of expert examiners has improved judicial reliance on scientifically validated techniques, thereby enhancing the credibility of digital evidence in trials. At the same time, forensic processes in India face challenges such as backlog of cases, inadequate infrastructure, and lack of uniform standards, which sometimes weaken the reliability of expert testimony.

5.4 Judicial Discretion in Evaluating Expert Reports

Despite statutory recognition, Indian courts have consistently held that expert opinion is advisory in nature and cannot substitute judicial reasoning. Courts exercise discretion in accepting or rejecting such reports, often corroborating them with other forms of evidence. For instance, in State (NCT of Delhi) v. Navjot Sandhu, while electronic records were admitted, their evidentiary weight was assessed in light of expert testimony and surrounding circumstances. Similarly, in Arjun Panditrao Khotkar, the Court reiterated that certificates under Section 65B and expert opinion serve as complementary safeguards, but judicial application of mind is essential. This approach ensures that the use of expert opinion does not erode judicial independence, while still acknowledging the indispensability of technical expertise in the digital age.

6. Problems in the Current Legal Framework

6.1 Technical Challenges

Digital evidence presents unique vulnerabilities compared to traditional forms of proof. The alterability of electronic records makes them highly susceptible to manipulation. Unlike physical evidence, digital data can be duplicated, deleted, or modified without leaving visible traces, thereby questioning its integrity in judicial proceedings.[17] The Indian courts have repeatedly emphasized the need for authentication, yet technological advancements such as metadata manipulation make verification increasingly difficult.[18]

Another obstacle is the proliferation of encryption technologies. While encryption ensures data security, it simultaneously restricts law enforcement access to critical evidence. Investigators often encounter challenges when accused individuals refuse to disclose decryption keys or passwords, raising tensions between constitutional protections against self-incrimination and the state's interest in prosecution.[19] Furthermore, the rise of synthetic media and deepfakes AI-generated falsified video and audio content poses grave threats to evidentiary authenticity. Courts in India have yet to develop specific standards to assess the admissibility of such AI-generated evidence. Similarly, although blockchain records are considered immutable, there is no explicit statutory recognition of blockchain data in Indian evidentiary law.[20] This legislative vacuum creates uncertainty when blockchain-based contracts or cryptocurrency transactions are produced in court.

6.2 Procedural Challenges

The most contentious procedural hurdle is the mandatory certificate requirement under Section 65B of the Indian Evidence Act, 1872 and its successor, Section 63 of the Bharatiya Sakshya Adhiniyam, 2023.[21] In Anvar P.V. v. P.K. Basheer, the Supreme Court held that without a proper certificate, electronic records are inadmissible. This strict approach, though intended to preserve evidentiary integrity, often obstructs justice because certificates are difficult to obtain when evidence is controlled by third-party service providers such as Google, Facebook, or WhatsApp.

The chain of custody for digital evidence is another critical issue. Unlike physical evidence, digital data can be copied innumerable times, raising questions of authenticity unless a forensically sound process is followed. Indian law provides no uniform standard operating procedure (SOP) for maintaining custody, unlike international models such as the U.S. Department of Justice's Digital Evidence Guidelines.[22] Moreover, cloud-based and foreign-hosted data present jurisdictional complications. The majority of social media data relevant to criminal investigations is stored on servers outside India. Access to such data requires resort to Mutual Legal Assistance Treaties (MLATs), which are notoriously slow and ineffective. This delay often results in the loss of volatile data such as call records, IP logs, or temporary files.

6.3 Institutional Challenges

India faces a serious deficit in digital forensic infrastructure. While cybercrime cases are exponentially increasing, the number of accredited forensic laboratories capable of examining digital devices is extremely limited.[23] Existing labs are overburdened, leading to significant delays that diminish the evidentiary value of seized devices. Equally pressing is the lack

[16] R.V. Kelkar, *Lectures on Criminal Procedure* 412–15 (Eighth ed. 2019).
[17] Orin S. Kerr, *Computer Crime Law* 164 (4th ed. 2021).
[18] *Rakesh Kumar Singla v. Union of India*, (2021) 2 SCC 474.
[19] *Selvi v. State of Karnataka*, (2010) 7 SCC 263.
[20] Nandan Kamath, *Law and Technology: New Challenges* 213 (2020).
[21] Indian Evidence Act, 1872, §§ 65A–65B; Bharatiya Sakshya Adhiniyam, 2023, § 63.
[22] U.S. Dep't of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders* (2008).
[23] Government of India, Ministry of Home Affairs, *Status of Cyber Forensic Laboratories in India* (2022).

of trained manpower. Police personnel, prosecutors, and even members of the judiciary often lack adequate understanding of the technical nuances of digital evidence.[24] This knowledge gap results in inconsistent appreciation of evidence and sometimes wrongful acquittals or convictions.

In addition, there is excessive reliance on private technology companies. Since investigators depend on service providers to furnish logs, metadata, or communication records, the state's prosecutorial capacity is often determined by the cooperation of private corporations. This dependency raises privacy concerns and undermines sovereign control over evidence. Unlike jurisdictions such as the European Union, which has proposed a harmonized E-Evidence Regulation, India still lacks standardized protocols for digital evidence handling. This institutional deficiency perpetuates arbitrariness and weakens uniformity in judicial outcomes.

6.4 Human Rights Concerns

The Indian Supreme Court in Justice K.S. Puttaswamy v. Union of India recognized the right to privacy as a fundamental right under Article 21.[25] Consequently, the state's use of intrusive surveillance measures to obtain digital evidence must pass the tests of necessity, legality, and proportionality. However, in practice, the surveillance powers under Section 69 of the Information Technology Act, 2000 and the Telegraph Act are broad and often lack judicial oversight. This raises constitutional concerns regarding misuse.

Another unresolved issue is the admissibility of illegally obtained evidence. Indian law follows the principle that even illegally obtained evidence may be admitted if relevant, unlike the American doctrine of "fruits of the poisonous tree."[26] This leniency, while aiding prosecution, risks encouraging unlawful surveillance and unauthorized data collection.

The privilege against self-incrimination under Article 20(3) also presents a dilemma. Courts are increasingly confronted with cases where accused persons are compelled to provide biometric access (fingerprints, facial recognition) or passwords to encrypted devices.[27] Whether such compulsion violates constitutional rights remains unsettled.

6.5 Emerging Concerns

The future of digital evidence raises novel issues. Courts are beginning to rely on artificial intelligence-based forensic tools for voice recognition, CCTV analysis, and facial recognition. While these technologies can enhance efficiency, they also introduce risks of algorithmic bias and lack of transparency in judicial decision-making.

Additionally, the custody of seized electronic devices is itself vulnerable to cybersecurity breaches.[28] There have been instances of tampering with digital evidence even after it was secured by investigating agencies, undermining public trust in institutional safeguards.

The interplay between digital evidence and the Digital Personal Data Protection Act, 2023 further complicates the legal landscape.[29] Investigators must balance the need to access personal data for prosecution with statutory duties to protect informational privacy, creating potential conflicts.

Finally, India's legal system remains comparatively outdated. While the United Kingdom has enacted the Criminal Justice Act, 2003 and the European Union is moving towards comprehensive electronic evidence regulations, India still relies primarily on judicial interpretation rather than legislative innovation.

7. Preservation and Collection of Digital Evidence

The preservation and collection of digital evidence is one of the most delicate phases in the evidentiary chain, as improper handling can render electronic records inadmissible. Unlike physical documents, electronic records are inherently volatile capable of alteration, deletion, or corruption merely by being opened or transferred. This necessitates specialized legal and procedural safeguards.

7.1 Provisions under the Code of Criminal Procedure, 1973 and the Bharatiya Nagarik Suraksha Sanhita, 2023

Under the Code of Criminal Procedure, 1973 (CrPC), various provisions enable investigative authorities to secure documents and records, which by judicial interpretation now extend to digital records. Section 91 empowers courts and police officers to issue summons for the production of documents, a provision regularly invoked to obtain digital evidence such as call records or emails. Section 100 authorizes search of places suspected to contain documents or devices, while Section 165 grants investigating officers the power to conduct searches during investigations if delay would prejudice the case. Further, Section 173(8) permits supplementary reports based on newly discovered digital evidence, ensuring that prosecutions can

[24] R.K. Chaubey, *An Introduction to Cyber Crime Investigation and Digital Forensics* 245 (2020).
[25] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[26] *Pooran Mal v. Director of Inspection (Investigation)*, (1974) 1 SCC 345.
[27] *State of Bombay v. Kathi Kalu Oghad*, AIR 1961 SC 1808.
[28] *Romila Thapar v. Union of India*, (2018) 10 SCC 753.
[29] Digital Personal Data Protection Act, 2023, No. 22 of 2023.

incorporate electronic records even after the initial charge sheet.

The recently enacted Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) retains these powers with refinements for the digital era. For instance, BNSS incorporates updated provisions to address electronic search and seizure, reflecting the increasing reliance on digital records in criminal prosecutions. By modernizing the procedural framework, BNSS seeks to create continuity with the CrPC while ensuring smoother integration of technological developments.

7.2 E-Discovery and Chain of Custody

The process of e-discovery, developed in common law jurisdictions, refers to the identification, preservation, and production of electronically stored information (ESI) during litigation. Although Indian law does not have codified e-discovery rules akin to the U.S. Federal Rules of Civil Procedure, courts have increasingly recognized the necessity of structured discovery mechanisms for electronic evidence, particularly in commercial disputes and arbitration.[30]

The chain of custody is another critical requirement. To maintain authenticity, every transfer of a digital device or storage medium must be documented with timestamps, identities of handlers, and forensic imaging reports. The absence of a proper chain of custody can render otherwise relevant evidence inadmissible. Indian courts, however, lack a uniform statutory protocol for chain of custody, resulting in inconsistent practices across jurisdictions. Comparatively, the FBI's Electronic Crime Scene Investigation Guidelines and the European Network of Forensic Science Institutes (ENFSI) Standards provide detailed models that India could adopt.

7.3 Need for Standardised Digital Evidence Protocols

One of the persistent lacunae in Indian law is the absence of standardized protocols for the preservation and collection of digital evidence. While the Information Technology Act, 2000 and the Bharatiya Sakshya Adhiniyam, 2023 recognize electronic records as admissible, neither statute prescribes specific procedures for imaging, hashing, or storage of digital data. This vacuum leads to frequent disputes over authenticity and admissibility.

Moreover, digital evidence often exists in volatile formats such as cache files, temporary logs, or volatile memory (RAM). Unless captured through forensically sound methods, such data may be lost irretrievably. The lack of statutory recognition of volatile data creates uncertainty in prosecutions relying on transient evidence like internet browsing histories or live chats.

Another pressing concern is cross-border digital evidence. Since a significant portion of digital records is stored on servers outside India, investigators face hurdles in timely preservation due to slow MLAT procedures. Jurisdictions like the European Union are moving towards a direct cooperation model under the proposed E-Evidence Regulation, which allows cross-border production orders without requiring diplomatic channels. India, by contrast, continues to rely on outdated procedures, risking loss of crucial evidence.

To address these challenges, India urgently requires uniform standard operating procedures (SOPs), possibly under the Ministry of Home Affairs or the National Cyber Forensic Lab network, for handling digital evidence. These should include mandatory forensic imaging, secure hashing, documentation of the chain of custody, and guidelines for presenting electronic evidence in courts. Such reforms would align India's framework with global best practices and enhance judicial confidence in digital records.

8. Perspectives and Reform Proposals

The legal treatment of digital evidence in India has advanced significantly since the introduction of the Information Technology Act, 2000, and the gradual judicial recognition of electronic records. Yet, persistent problems in admissibility, authentication, and preservation require a forward-looking reform strategy. This section highlights perspectives and reform proposals that may strengthen the evidentiary regime for digital records in India.

8.1 Harmonizing the Transition from IEA to BSA

The enactment of the Bharatiya Sakshya Adhiniyam (BSA), 2023, marks a critical shift from the Indian Evidence Act, 1872, to a modernized evidence law. However, the transition risks generating confusion in ongoing proceedings where electronic evidence was collected under the IEA framework. Harmonization requires clear transitional provisions ensuring that evidence obtained under the IEA remains admissible even after the BSA's enforcement. Such continuity would prevent inconsistent rulings and uphold legal certainty.

8.2 Clarifying the Certificate Requirement under Section 63 BSA

The mandatory requirement of a certificate for electronic evidence under Section 65B of the IEA created significant controversy, culminating in the Supreme Court's ruling in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal. While the BSA, under Section 63, retains this requirement, it remains unclear how it will be applied in cases involving third-party digital platforms or foreign servers, where obtaining a certificate is impractical. Reform proposals include introducing

[30] *Union of India v. Reliance Communication Ltd.*, (2016) 236 DLT 89 (Del. HC).

judicial discretion to relax the certificate mandate in exceptional circumstances, thereby balancing authenticity with practicality.

8.3 Establishment of an Independent Digital Evidence Authority

India currently lacks a specialized, independent institution dedicated to overseeing the collection, preservation, and authentication of digital evidence. A proposed Digital Evidence Authority could function as a neutral body to: Certify digital records; Maintain a centralised repository of forensic tools; and Set nationwide standards for chain of custody. Such an institution would reduce dependence on private technology companies and enhance judicial confidence in digital records.[31]

8.4 Adoption of Blockchain and AI-Driven Authentication

Emerging technologies like blockchain can secure chain of custody by creating immutable timestamps, while AI-driven tools can assist in detecting tampering, identifying deepfakes, and verifying metadata. Courts across jurisdictions, including the U.S. and China, have started experimenting with blockchain-based evidence management systems. Introducing these innovations into India's evidentiary framework would modernize its capacity to deal with complex cybercrimes and digital fraud.

8.5 Training Judicial Officers and Investigators

The credibility of digital evidence depends not only on statutory provisions but also on the competence of those handling it. Judicial officers, prosecutors, and investigators often lack technical literacy, leading to misinterpretation or overreliance on expert testimony. Regular capacity-building programs on digital forensics, e-discovery, and cyber-investigation should be institutionalized through the Judicial Academies and Police Training Institutes.

8.6 Enhancing Cross-Border Cooperation Mechanisms

Digital evidence often resides on servers outside India, creating jurisdictional hurdles. Current reliance on Mutual Legal Assistance Treaties (MLATs) is slow and ineffective. Strengthening cross-border cooperation through bilateral agreements, participation in global conventions like the Budapest Convention on Cybercrime, and regional frameworks within the South Asian Association for Regional Cooperation (SAARC) would streamline access to foreign-hosted digital evidence.[32]

8.7 Balancing Admissibility with Privacy and Due Process Safeguards

The right to privacy, recognized as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India,[33] necessitates safeguards in the use of digital evidence. Courts must exclude evidence obtained through illegal surveillance or hacking unless justified by compelling state interests. Future reforms must strike a balance between effective law enforcement and the protection of civil liberties, ensuring that digital evidence is admissible only if procured in accordance with due process.

9. Conclusion

The growing digitalisation of society has made digital evidence indispensable in India's justice delivery system. From cybercrimes and economic offences to commercial disputes and matrimonial cases, electronic records are now central to fact-finding and adjudication.[34] The legal system can no longer afford to treat such evidence as peripheral; rather, it must be accorded the same legitimacy and reliability as traditional forms of proof, subject to appropriate safeguards.

The Bharatiya Sakshya Adhiniyam, 2023, represents a conscious attempt to modernise India's evidentiary law by consolidating the framework on electronic records, refining procedural requirements, and aligning with technological advancements. However, several persisting problems remain most notably the rigidity of the certificate requirement, lack of uniformity in digital forensic practices, inadequate infrastructure, and the tension between privacy rights and state surveillance. These challenges underscore the gap between legislative intent and ground-level implementation.

Future reforms must therefore focus on developing flexible evidentiary standards that allow courts limited discretion in admitting digital evidence, while ensuring safeguards against manipulation and falsification. Parallelly, the establishment of specialised forensic infrastructure, training of judicial officers, and creation of an independent Digital Evidence Authority are essential to reduce reliance on private corporations and strengthen the authenticity of electronic records. Equally important is the need to embed constitutional safeguards. The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India requires that rules on search, seizure, and admissibility of digital evidence comply with the principles of legality, necessity, and proportionality. This ensures that the pursuit of truth in judicial proceedings does not come at the expense of civil liberties.

---

[31] Apar Gupta, *Towards a Digital Evidence Authority in India: Policy Perspectives*, 12 Indian J.L. & Tech. 45, 57–60 (2021).
[32] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 (Budapest Convention).
[33] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
[34] Ritu Gupta, *Evidentiary Challenges in the Digital Age: An Indian Perspective*, 14 Nat'l L. Sch. India Rev. 221, 224–26 (2022).

India's way forward in digital justice delivery thus lies in a balanced evidentiary regime one that embraces technological innovation, maintains due process, and upholds constitutional values. Only then can digital evidence transform from a contested category into a reliable cornerstone of the Indian legal system.