INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

ADMISSIBILITY OF ELECTRONIC EVIDENCE IN CYBERCRIME: A COMPARATIVE AND DOCTRINAL ANALYSIS UNDER INDIAN LAW

AUTHOR – AALIYA AMEER.A, STUDENT AT TAMILNADU DR. AMBEDKAR LAW UNIVERSITY, CHENNAI

BEST CITATION – AALIYA AMEER.A, ADMISSIBILITY OF ELECTRONIC EVIDENCE IN CYBERCRIME: A COMPARATIVE AND DOCTRINAL ANALYSIS UNDER INDIAN LAW**,** *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (4) OF 2026, PG. 943-948, APIS – 3920 – 0001 & ISSN - 2583-2344

ABSTRACT

The exponential growth of cybercrime in the digital era has fundamentally transformed the nature of criminal evidence, compelling legal systems to evolve from traditional evidentiary frameworks to technologically adaptive regimes. In India, this transition is marked by the shift from the Indian Evidence Act, 1872 (IEA) to the Bharatiya Sakshya Adhiniyam, 2023 (BSA), alongside the continuing relevance of the Information Technology Act, 2000 (IT Act). This research paper undertakes a doctrinal and analytical examination of the admissibility of electronic evidence in cybercrime cases, focusing on statutory provisions, judicial precedents, procedural safeguards, and comparative international perspectives.

The study critically evaluates Sections 65A–65B of the IEA and Sections 61–63 of the BSA, highlighting the evolution from a restrictive certification-based model to a more technology-neutral admissibility regime. It further explores landmark judgments such as *Anvar P.V. v. P.K. Basheer* and *Arjun Panditrao Khotkar v. Kailash Gorantyal*, which shaped the jurisprudence on electronic evidence.

Despite legislative advancements, challenges such as cross-border data access, technical complexity, and data integrity persist. The study concludes by recommending institutional strengthening, forensic standardisation, and judicial capacity-building.

I. INTRODUCTION

The digital revolution has significantly altered the evidentiary landscape of criminal justice systems. Traditional reliance on physical documents has been replaced by electronic records such as emails, metadata, and cloud-based information.[1830] Cybercrime, in particular, leaves behind digital footprints that form the backbone of modern prosecutions.[1831]

In India, the Indian Evidence Act, 1872 initially lacked provisions addressing electronic evidence. Amendments through the IT Act introduced Sections 65A and 65B, which attempted to regulate admissibility.[1832] However, procedural rigidity and interpretational inconsistencies led to practical challenges.[1833]

The Bharatiya Sakshya Adhiniyam, 2023 marks a paradigm shift by recognising electronic evidence as primary evidence and adopting a technology-neutral approach.[1834] This reform reflects the need to align legal frameworks with technological realities.

II. LITERATURE REVIEW

Academic scholarship highlights the transformation of evidentiary law in response to digitalisation. Kishore argues that digital evidence requires re-evaluation of authenticity

[1830] P. Jain, Evidentiary Shifts in the Age of Digitalisation, 7 *Indian J. Legal Stud.* (2022).
[1831] Nat'l Crime Records Bureau, *Crime in India 2023* (2024).
[1832] Indian Evidence Act, 1872, §§ 65A–65B.
[1833] N. Basu, *Indian Evidence Act: Principles and Practice* (2021).
[1834] Bharatiya Sakshya Adhiniyam, 2023, § 61.

standards.[1835] Basu emphasises the limitations of traditional doctrines in handling electronic records.[1836]

Jain notes that digitalisation has shifted evidentiary paradigms from physical to data-centric models.[1837] Singh underscores the importance of integrity and authenticity due to risks of manipulation.[1838]

Recent scholarship on the BSA highlights its modern approach. Krishnan describes it as a technology-aware statute, while Deshmukh emphasises its focus on digital trust and admissibility.[1839]

III. INDIAN LEGAL FRAMEWORK GOVERNING ELECTRONIC EVIDENCE

A. Indian Evidence Act, 1872 (as Amended)

The Indian Evidence Act, 1872 forms the foundational framework for evidentiary law in India. The introduction of Sections 65A and 65B through the IT Act amendments marked a significant step towards recognising electronic records. Section 65B, in particular, establishes conditions for admissibility, including the requirement of a certificate verifying the authenticity of computer-generated outputs.[1840]

The Supreme Court in *Anvar P.V. v. P.K. Basheer* held that compliance with Section 65B(4) is mandatory for admissibility of electronic evidence unless the original device is produced.[1841] This judgment established a strict procedural regime, emphasising the importance of certification.

B. Information Technology Act, 2000

The IT Act provides the legal foundation for electronic records and digital signatures in India. Section 2(t) defines electronic records broadly, while Sections 3 and 5 recognise digital signatures as legally valid.[1842] The Act also facilitates authentication mechanisms and establishes certifying authorities, thereby supporting evidentiary frameworks under the IEA and BSA.

C. Bharatiya Sakshya Adhiniyam, 2023

The BSA represents a comprehensive overhaul of evidentiary law. Section 61 explicitly states that electronic records cannot be denied admissibility solely because they are electronic.[1843] Sections 62–63 provide conditions for admissibility, including certification requirements.

Unlike the IEA, the BSA treats electronic records as primary evidence rather than secondary evidence, thereby simplifying procedural requirements. This shift reflects a policy orientation towards integrating digital evidence into mainstream evidentiary practice.

V. TYPES OF ELECTRONIC EVIDENCE IN CYBERCRIME

Electronic evidence in cybercrime encompasses a wide range of digital artefacts, including:

- Communication evidence (emails, chats, social media)
- Network and system logs (IP addresses, server logs)
- Multimedia evidence (CCTV footage, audio/video files)
- Cloud-based data (remote servers, storage platforms)
- Digitally signed documents

Each category presents unique challenges in terms of authentication, preservation, and admissibility. Courts increasingly rely on forensic analysis and metadata to establish reliability.

[1835] R. Kishore, *Law of Evidence in the Digital Age* (2023).
[1836] N. Basu, *Indian Evidence Act: Principles and Practice* (2021).
[1837] P. Jain, supra note 6.
[1838] K. Singh, Authenticity and Integrity of Electronic Evidence (2021).
[1839] S. Krishnan (2024); A. Deshmukh (2024).
[1840] Indian Evidence Act, 1872, § 65B.
[1841] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[1842] information Technology Act, 2000, §§ 3, 5.
[1843] Bharatiya Sakshya Adhiniyam, 2023, § 61.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

V. PROCEDURAL ASPECTS OF ELECTRONIC EVIDENCE

The admissibility of electronic evidence depends significantly on procedural compliance. Key stages include:

1. **Collection and Seizure** – Must comply with CrPC provisions and forensic protocols.
2. **Preservation** – Requires maintaining integrity through hashing and secure storage.
3. **Chain of Custody** – Essential to establish authenticity and prevent tampering.
4. **Certification** – Mandatory under statutory provisions.
5. **Presentation in Court** – Includes digital displays, printouts, and expert testimony.

Failure to adhere to these procedures can result in exclusion of evidence.

VI. SUBSTANTIVE ADMISSIBILITY STANDARDS

Electronic evidence must satisfy the following criteria:

- **Authenticity** – Proof of origin
- **Integrity** – Absence of tampering
- **Relevance** – Connection to facts in issue
- **Reliability** – Trustworthiness of process

These standards ensure that digital evidence is both legally admissible and probatively valuable.

VI. SUBSTANTIVE ADMISSIBILITY STANDARDS

Electronic evidence must satisfy the following criteria:

- **Authenticity** – Proof of origin
- **Integrity** – Absence of tampering
- **Relevance** – Connection to facts in issue
- **Reliability** – Trustworthiness of process

These standards ensure that digital evidence is both legally admissible and probatively valuable.

VIII. COMPARATIVE AND INTERNATIONAL PERSPECTIVES

- **United States** – Federal Rules of Evidence adopt a flexible, authentication-based approach.
- **United Kingdom** – Electronic signatures recognised under ECA 2000.
- **European Union** – eIDAS Regulation ensures uniform digital trust framework.

India's BSA aligns with these global trends by adopting a technology-neutral approach.

VIII. COMPARATIVE AND INTERNATIONAL PERSPECTIVES

- **United States** – Federal Rules of Evidence adopt a flexible, authentication-based approach.
- **United Kingdom** – Electronic signatures recognised under ECA 2000.
- **European Union** – eIDAS Regulation ensures uniform digital trust framework.

India's BSA aligns with these global trends by adopting a technology-neutral approach.

IX. CHALLENGES

The admissibility and effective utilisation of electronic evidence in India continue to face significant structural, technical, and legal challenges despite progressive statutory reforms. One of the foremost challenges is the **technical complexity of digital evidence**. Unlike traditional forms of evidence, electronic records are inherently volatile, easily alterable, and dependent on sophisticated technological systems. The dynamic nature of digital data—such as real-time logs, encrypted communications, and cloud-based storage—makes preservation and authentication particularly difficult. Even minor lapses in handling can compromise evidentiary value.

Another major concern is the **lack of adequate forensic infrastructure and expertise**. While specialised cyber forensic laboratories exist, their availability is uneven across jurisdictions, and many law enforcement agencies lack the

technical capacity to handle complex digital evidence. This results in delays, improper evidence handling, and in some cases, rejection of evidence due to procedural non-compliance. Additionally, the shortage of trained digital forensic experts further exacerbates the problem, limiting the effectiveness of expert testimony under provisions such as Section 45A of the Indian Evidence Act.

The issue of **chain of custody and data integrity** presents another critical challenge. Digital evidence requires meticulous documentation at every stage—from seizure to presentation—to establish authenticity and prevent allegations of tampering. However, in practice, maintaining an unbroken and verifiable chain of custody is difficult due to inadequate training and lack of standardised protocols. Courts often scrutinise such lapses rigorously, which may lead to exclusion or reduced evidentiary weight.

A particularly complex issue is **cross-border data access and jurisdictional limitations**. Much of today's digital evidence is stored on servers located outside India, particularly in cloud infrastructures operated by multinational corporations.[1844] Accessing such data requires reliance on Mutual Legal Assistance Treaties (MLATs) or other international cooperation mechanisms, which are often time-consuming and inefficient. This delay can result in loss or alteration of critical evidence, thereby affecting the outcome of investigations and trials.

Further, the **intersection of electronic evidence with privacy and data protection laws** poses emerging challenges. With the enactment of the Digital Personal Data Protection Act, 2023, investigators must balance evidentiary requirements with privacy rights. The collection and use of personal data as evidence must comply with statutory safeguards, failing which it may be challenged on constitutional grounds.

Finally, **inconsistent judicial interpretation** has historically created uncertainty in the application of electronic evidence laws. While landmark judgments have clarified certain aspects, variations in lower court approaches persist, particularly regarding certification requirements and admissibility thresholds.

X. RECOMMENDATIONS

Addressing the challenges associated with electronic evidence requires a comprehensive and multi-dimensional approach involving legal, institutional, and technological reforms.

First, there is a pressing need for the **standardisation of forensic procedures and evidence-handling protocols**. Uniform guidelines should be developed and implemented across all investigative agencies to ensure consistency in the collection, preservation, and analysis of digital evidence. These standards must incorporate internationally accepted best practices, including forensic imaging, hashing techniques, and secure storage mechanisms.

Second, **capacity building within the judiciary and law enforcement agencies** is essential. Judges, prosecutors, and investigators must be trained in digital forensics, cyber law, and emerging technologies to effectively interpret and evaluate electronic evidence. Regular workshops, certification programmes, and collaboration with technical experts can significantly enhance institutional competence.

Third, the government should invest in **strengthening cyber forensic infrastructure**. This includes establishing well-equipped forensic laboratories in all states, upgrading existing facilities, and ensuring timely access to expert analysis. Public-private partnerships with technology firms and academic institutions can also play a vital role in bridging the infrastructure gap.

Fourth, there is a need to **simplify and rationalise certification requirements** under evidentiary laws. While certification ensures authenticity, overly rigid requirements can hinder justice, especially when evidence originates from third-party systems. The law

[1844] Nat'l Crime Records Bureau, *Crime in India 2023: Statistics on Cyber Offences* (Ministry of Home Affairs 2024).

should adopt a balanced approach that maintains evidentiary integrity while allowing reasonable flexibility in exceptional circumstances.

Fifth, enhancing **international cooperation mechanisms** is crucial for addressing cross-border evidence challenges. India should actively engage in bilateral and multilateral agreements to facilitate faster data sharing and streamline MLAT processes. Participation in global cybercrime frameworks can also improve coordination and evidence accessibility.

Sixth, the integration of **advanced technologies such as artificial intelligence (AI) and blockchain** can significantly improve evidence management. AI tools can assist in analysing large volumes of digital data, while blockchain can provide tamper-proof records, thereby strengthening the integrity of electronic evidence.

Finally, it is important to ensure that **legal reforms remain adaptive and future-oriented**. As technology evolves, evidentiary laws must be periodically reviewed and updated to address emerging challenges such as deepfakes, quantum encryption, and IoT-based evidence.

XI. CONCLUSION

The transformation of evidentiary law in response to the digital revolution represents one of the most significant developments in contemporary legal systems. In India, the shift from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023 marks a decisive move towards modernisation and technological alignment.[1845] By recognising electronic records as primary evidence and adopting a technology-neutral approach, the BSA addresses many of the limitations inherent in the earlier framework.

However, legislative reform alone is insufficient to ensure the effective admissibility and utilisation of electronic evidence. The practical challenges associated with digital evidence—ranging from technical complexity to procedural compliance—require robust institutional mechanisms and continuous capacity building. The judiciary must play a proactive role in interpreting and applying evidentiary standards in a manner that balances procedural rigour with substantive justice.

Furthermore, the increasing reliance on digital evidence necessitates a rethinking of traditional legal concepts such as authenticity, reliability, and chain of custody. Courts must adapt to new forms of proof while maintaining safeguards against misuse and manipulation. The integration of forensic science, technological expertise, and legal principles is essential to achieving this balance.

From a broader perspective, India's evolving framework reflects a global trend towards recognising the centrality of digital evidence in modern litigation. By aligning with international standards and adopting progressive reforms, India is well-positioned to address the challenges of cybercrime in the digital age.

In conclusion, the admissibility of electronic evidence is not merely a question of statutory compliance but a test of the legal system's ability to adapt to technological change. Ensuring the credibility and reliability of such evidence requires a holistic approach that combines legal reform, institutional strengthening, and technological innovation. Only then can the justice system effectively respond to the complexities of cybercrime and uphold the principles of fairness and due process.

XII. BIBLIOGRAPGY AND REFERENCES

1. R. Kishore, *Law of Evidence in the Digital Age* 12–15 (Eastern Law House 2023).
2. P. Jain, Evidentiary Shifts in the Age of Digitalisation, 7 *Indian J. Legal Stud.* 34, 36 (2022).
3. N. Basu, *Indian Evidence Act: Principles and Practice* 89 (LexisNexis 2021).

[1845] Policy recommendations derived from analysis of statutory framework and supra notes

4. K. Singh, Authenticity and Integrity of Electronic Evidence, 4 *Cyber L. Rev.* 45 (2021).
5. P. Sharma, *Cybercrime and Digital Forensics in Indian Jurisprudence* 74 (Universal Law Publ'g 2020).
6. A. R. Menon, Digital Footprints as Forensic Evidence, 8(2) *J. Info. Sec. L.* 59 (2022).
7. S. Chawla, The Legal Status of Digital Artefacts in Criminal Proceedings, 11 *Indian L. Rev.* 112 (2023).
8. S. Krishnan, *The Bharatiya Sakshya Adhiniyam: A Commentary* 22–27 (Thomson Reuters 2024).
9. A. Deshmukh, Digital Trust and Admissibility of E-Evidence under the BSA, 2 *Indian J. Tech. L.* 44 (2024).
10. Nat'l Crime Records Bureau, *Crime in India 2023: Statistics on Cyber Offences* (Ministry of Home Affairs 2024).
11. Ministry of Law & Justice, *Statement of Objects and Reasons: Bharatiya Sakshya Adhiniyam, 2023*, Gazette of India, Part II, Section 2.
12. *State of Tamil Nadu v. Suhas Katti*, 2004 Cri LJ 295 (Mad).
13. *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.
14. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
15. *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.
16. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
17. Indian Evidence Act, 1872, No. 1 of 1872, §§ 3, 65A–65B, 45A (India).
18. Information Technology Act, 2000, No. 21 of 2000, §§ 2(t), 3, 4, 5, 79A (India).
19. Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, §§ 2(1)(d), 2(1)(e), 61–63, 80 (India).
20. Code of Criminal Procedure, 1973, No. 2 of 1974, §§ 93, 165 (India).