International Journal of Advance and Innovative Research
Volume 12, Issue 2: April - June 2025
ISSN 2394 - 7780

ADMISSIBILITY OF DIGITAL EVIDENCE IN INDIAN COURTS: A CRITICAL REVIEW OF LEGAL STANDARDS AND JUDICIAL TRENDS

Dr. I. Nagmani
Assistant Professor of Law, MATS Law School, MATS University, C.G

ABSTRACT

The increasing reliance on digital evidence—ranging from emails and CCTV footage to mobile data—has significantly transformed the landscape of Indian litigation. However, this evolution has raised complex legal questions regarding the admissibility, authenticity, and procedural safeguards surrounding such evidence. This article offers a concise review of the legal framework governing digital evidence in India, focusing on key statutory provisions, judicial interpretations, and the recent introduction of the Bharatiya Sakshya Adhiniyam, 2023.

Under the earlier Indian Evidence Act, 1872, Sections 65A and 65B governed electronic records, requiring a certificate for admissibility. The new Bharatiya Sakshya Adhiniyam carries forward these provisions under Section 61, while clarifying admissibility of blockchain records and AI-generated content. Importantly, it allows relaxation of the certificate requirement when authenticity is not contested, thus addressing some rigidity in the earlier framework.

Judicial pronouncements have significantly influenced this domain. From the lenient stance in Navjot Sandhu (2005) to the stricter interpretation in Anvar P.V. (2014) and Arjun Panditrao (2020), courts have gradually moved towards greater evidentiary precision. Despite this, challenges remain—such as difficulty in procuring Section 61 certificates, inadequate forensic infrastructure, and lack of technical training for enforcement and judicial officers.

Comparative insights from jurisdictions like the UK and USA show more flexible approaches that focus on reliability over formal compliance. For India to match this, it must simplify procedures, enhance forensic capacity, and harmonise judicial practice.

In conclusion, while the Bharatiya Sakshya Adhiniyam is a progressive step, its success depends on institutional readiness, judicial consistency, and a nuanced understanding of technology in law.

***Keywords**: Digital Evidence, Bharatiya Sakshya Adhiniyam, Section 65B Certificate, Comparative Jurisprudence, Judicial Reforms.*

1. INTRODUCTION

In the digital era, the nature of evidence presented before courts has undergone a profound transformation. As society increasingly operates through screens and devices, so too have disputes and crimes begun to leave digital footprints—emails exchanged, messages sent on WhatsApp, CCTV footage from street corners, or metadata embedded in a photo or document. Whether in complex white-collar crimes, cyber frauds, marital disputes, or even violent offences, electronic records are now central to investigations and courtroom adjudication.[1]

This growing dependence on digital evidence has introduced new challenges for the Indian legal system. Unlike traditional documentary or oral evidence, digital records are intangible, volatile, and technically complex. A document stored on a server can be remotely altered; a message can be deleted or spoofed; a video clip can be edited in seconds.[2] In such a context, courts must be equipped not only to receive digital evidence but also to critically assess its authenticity, integrity, and reliability. The question is no longer whether digital evidence should be admitted, but how it should be admitted—and under what conditions.

At the heart of this challenge lies the legal framework governing admissibility. Indian law initially addressed digital evidence through the *Indian Evidence Act, 1872*, particularly after the amendments introduced by the *Information Technology Act, 2000*.[3] Sections 65A and 65B became the primary provisions for determining the

[1] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (discussing digital expression and legal response in India); see also Sapan Parekh, *Digital Evidence: The Future of Evidence in Indian Courts*, 4 NLUD J. Legal Stud. 77, 78 (2018).

[2] Pavan Duggal, *Cyberlaw: The Indian Perspective* 87–88 (5th ed. 2022).

[3] The Indian Evidence Act, No. 1 of 1872, §§ 65A–65B, India Code (as amended by the Information Technology Act, 2000); see also Information Technology Act, No. 21 of 2000, § 92.

ISSN 2394 - 7780

admissibility of electronic records. However, the enactment of the Bharatiya Sakshya Adhiniyam, 2023, which replaces the colonial-era law, marks a new phase—modernising evidentiary standards and addressing technological realities more comprehensively.[1] Yet, this transition has also reignited debates on procedural rigidity, judicial interpretation, and institutional preparedness.

This article undertakes a critical review of the legal standards that govern the admissibility of digital evidence in Indian courts. It examines the statutory evolution from the colonial framework to the newly enacted *Bharatiya Sakshya Adhiniyam*, analyses key judicial decisions that have shaped digital evidence jurisprudence, and reflects on the practical challenges faced by law enforcement and courts. Through a doctrinal and comparative lens, it seeks to assess whether India's evidentiary law is truly keeping pace with the digital realities of contemporary litigation—and what reforms are necessary to bridge the gap between legal form and technological function.

2. LEGAL FRAMEWORK GOVERNING DIGITAL EVIDENCE IN INDIA

The admissibility of digital evidence in Indian courts is primarily governed by a combination of three legal instruments: the *Indian Evidence Act, 1872* (now repealed), the *Information Technology Act, 2000,* and the recently enacted *Bharatiya Sakshya Adhiniyam, 2023*. Together, these statutes shape the legal standards for recognising, presenting, and admitting electronic records in judicial proceedings.

2.1 The Indian Evidence Act, 1872 (as amended)

The original *Indian Evidence Act, 1872*, though framed in a pre-digital era, was amended by the *Information Technology Act, 2000* to include provisions on electronic evidence. Section 3 of the Act was amended to expand the definition of "evidence" to include electronic records.[2] More substantively, Sections 65A and 65B were introduced as special provisions for the admissibility of electronic records. Section 65A acted as a general reference to special provisions for electronic evidence, while Section 65B laid down specific conditions for the admissibility of such records, including the requirement of a certificate under Section 65B (4).[3]

Additionally, Section 22A was inserted to clarify the limited admissibility of oral admissions regarding electronic records, and Section 45A authorised the use of expert opinion to explain or verify electronic evidence. These provisions collectively provided a framework, albeit with procedural rigidity and interpretational ambiguities that led to conflicting judicial rulings in later years.

2.2 The Information Technology Act, 2000

The *Information Technology Act, 2000* serves as the foundational law for digital infrastructure, electronic governance, and cybercrime. [3] It conferred legal recognition on electronic records and digital signatures through Sections 4 and 5, ensuring that electronic documentation could have the same legal status as their physical counterparts. The Act also authorised the use of secure digital signatures and mandated retention of electronic records for evidentiary purposes under various business and governmental regulations.

Importantly, the IT Act does not directly regulate the admissibility of digital evidence in court; instead, it functions in tandem with the *Evidence Act*—originally, and now with the *Bharatiya Sakshya Adhiniyam*. This symbiotic relationship ensures that while the IT Act defines and validates digital content, the rules for their judicial admissibility are located within the evidentiary statutes.

2.3 The Bharatiya Sakshya Adhiniyam, 2023

With the repeal of the *Indian Evidence Act, 1872*, the Bharatiya Sakshya Adhiniyam, 2023 has now become the governing law on evidence in India.[4] It retains most of the core concepts introduced in the earlier statute but rearticulates them with modernised language and clarity. Chapter IV of the Adhiniyam is dedicated to electronic records. Notably, Section 2(1)(d) includes "electronic record" in the definition of evidence, maintaining continuity with its predecessor.[5]

Section 61 of the new law corresponds to the repealed Section 65B, reiterating the requirement of a certificate for the admissibility of electronic records. However, the Adhiniyam improves upon the previous regime by introducing specific provisions relating to emerging technologies such as blockchain, digital signatures, and

[1] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, Gazette of India, Extraordinary, Part II, sec. 1 (Sep. 11, 2023).

[2] The Indian Evidence Act, No. 1 of 1872, § 3 (as amended by the Information Technology Act, 2000).

[3] Id. §§ 65A–65B; see Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (clarifying mandatory certificate requirement).

[4] Information Technology Act, No. 21 of 2000, §§ 4–10A, India Code (2000).

[5] Id. § 2(1)(d); see also id. § 61 (electronic records and certificate requirement).

ISSN 2394 - 7780

even AI-generated content.[1] Moreover, it allows courts discretion to waive the certificate requirement if the electronic record is not in dispute and can be otherwise authenticated, addressing one of the most pressing concerns raised in past judicial critiques.

Together, these legal developments signal a shift toward a more technologically responsive evidentiary regime—albeit one that must still overcome challenges in implementation and uniform interpretation.

3. JUDICIAL INTERPRETATION AND LANDMARK JUDGMENTS

The Indian judiciary has played a pivotal role in shaping the law around the admissibility of digital evidence. Over the past two decades, key rulings by the Supreme Court have significantly influenced how electronic records are understood within the evidentiary framework—especially in relation to Section 65B of the *Indian Evidence Act, 1872*, and now Section 61 of the *Bharatiya Sakshya Adhiniyam, 2023*.

In *State (NCT of Delhi) v. Navjot Sandhu* (2005), commonly known as the Parliament Attack case, the Supreme Court adopted a relatively flexible approach. It held that even in the absence of a certificate under Section 65B(4), electronic evidence could still be admitted under general provisions of the Evidence Act, provided it was otherwise relevant and not disputed.[2] This ruling gave significant leeway to prosecuting agencies and trial courts, but it also blurred the procedural safeguards meant to ensure authenticity.

Nearly a decade later, this approach was overruled in *Anvar P.V. v. P.K. Basheer* (2014). The Court held unequivocally that a certificate under Section 65B(4) is mandatory for the admissibility of any electronic record.[3] The judgment was a major shift—it aimed to ensure the integrity of digital evidence but simultaneously created hurdles in cases where such certification was difficult to obtain, such as with data from third-party servers or inaccessible devices.

To address these difficulties, the Court in *Shafhi Mohammad v. State of Himachal Pradesh* (2018) relaxed the mandatory certificate requirement, stating that it should not apply when the party seeking to produce the evidence is not in possession of the device or system from which the electronic record is generated.[4] However, this attempt at balancing procedural fairness with practical limitations was soon questioned for contradicting the earlier *Anvar* ruling.

The legal uncertainty was finally resolved by a Constitution Bench in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), which reaffirmed the mandatory nature of the Section 65B(4) certificate.[5] The Court clarified that the requirement is procedural but non-negotiable unless the genuineness of the electronic record is admitted by the opposite party or the original device is produced in court. This judgment brought much-needed doctrinal clarity but left intact the practical difficulties involved in procuring such certification.

Despite these authoritative rulings, High Courts across India have shown inconsistent application, especially in cases involving WhatsApp chats, CCTV footage, and call records. Some trial courts admit electronic evidence without a certificate citing urgency or presumed authenticity, while others reject it outright, leading to frequent appeals. The inconsistency not only delays justice but also undermines public confidence in the reliability of digital evidence in courts.

4. PRACTICAL CHALLENGES IN ADMITTING DIGITAL EVIDENCE

While the legal framework for digital evidence in India has developed substantially, its implementation remains fraught with practical difficulties. These issues stem not only from technological complexities but also from systemic inadequacies within the justice delivery system. The result is a disconnect between the formal legal requirements for admitting digital evidence and the practical capacity of stakeholders to comply with them.

A significant procedural hurdle lies in the complexity of obtaining the Section 65B certificate under the *Indian Evidence Act, 1872* and now Section 61 of the *Bharatiya Sakshya Adhiniyam, 2023*. This certificate must declare that the electronic record was produced from a reliable system and must specify the manner and conditions of its creation.[6] However, in many cases, especially when evidence originates from third-party

[1] Id. §§ 62–65 (on digital signature verification, blockchain admissibility, and expert testimony).

[2] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.

[3] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

[4] Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.

[5] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

[6] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1, ¶ 24 (India).

ISSN 2394 - 7780

platforms such as WhatsApp, Facebook, or cloud service providers like Google or Amazon Web Services, the party relying on the evidence has no control over the system or the ability to generate such a certificate.[1] Even when the content is accessible, service providers are often reluctant to issue certificates or delay compliance due to legal and jurisdictional complications.

Another issue is the difficulty in accessing metadata and device-level evidence, which is often essential for verifying the authenticity of a digital record.[2] Metadata can confirm whether a photo was taken at a particular location or if a document was edited after its purported submission. However, unless collected with forensic tools and preserved carefully, such information may be altered, lost, or rendered inadmissible.

Moreover, the chain of custody—the chronological documentation showing the seizure, custody, control, and transfer of electronic evidence—is frequently broken or inadequately recorded. Digital data is fragile: it can be altered by merely opening a file or copying it without proper safeguards.[3] In many criminal investigations, electronic records are collected without appropriate forensic imaging, and their origin or integrity becomes difficult to prove in court. This weakens the evidentiary value and opens the door to defence arguments regarding manipulation or fabrication.

Compounding the problem is the lack of digital forensic infrastructure and trained personnel across India.[4] Most district courts lack access to certified forensic laboratories or digital evidence handling units. Even at the police level, investigation officers often lack training in securing and documenting electronic records. While central agencies like CERT-In and state cybercrime units have some capacity, these are not uniformly accessible. The absence of standardised protocols exacerbates procedural lapses, particularly in remote or rural jurisdictions.

Further, the judicial approach to digital evidence remains inconsistent, especially at the trial court level. While the Supreme Court in *Arjun Panditrao Khotkar* reaffirmed the mandatory nature of the Section 65B certificate,[5] some trial courts continue to admit electronic records based on oral testimony or circumstantial relevance without insisting on compliance. Others reject otherwise reliable evidence solely due to technical non-fulfilment.[6] This divergence creates unpredictability and undermines legal certainty, especially for litigants unfamiliar with the technological and procedural nuances involved.

Together, these challenges demonstrate that the effectiveness of digital evidence is not merely a function of statutory language but depends on robust institutional capacity, consistent judicial

5. COMPARATIVE JURISPRUDENCE

India's legal approach to the admissibility of digital evidence, though evolving, still grapples with rigid procedural requirements and uneven implementation. In contrast, other common law jurisdictions such as the United Kingdom and the United States offer valuable models that emphasise functionality, reliability, and practical access to justice without undermining evidentiary integrity.

In the United Kingdom, the legal treatment of electronic evidence is guided primarily by the *Civil Evidence Act, 1995* and provisions under the *Criminal Justice Act, 2003*. These statutes adopt a relatively liberal approach toward admissibility, focusing more on the authenticity and reliability of digital records rather than formalistic preconditions.[7] For instance, while courts require parties to prove that a digital record is genuine, they do not demand a certificate analogous to India's Section 65B or Section 61. Instead, authenticity may be demonstrated

[1] Apar Gupta, *The Legal Labyrinth of WhatsApp Evidence*, The Wire (Oct. 18, 2020), https://thewire.in/law/legal-validity-whatsapp-evidence.

[2] Pavan Duggal, *Cyberlaw: The Indian Perspective* 118–20 (5th ed. 2022).

[3] Nandan Kamath, *Law Relating to Computers, Internet & E-commerce* 241–42 (5th ed. 2021).

[4] India Justice Report, *State of Forensics in India 2022*, at 14–18 (Tata Trusts), https://www.indiajusticereport.org.

[5] Arjun Panditrao, supra note 1, ¶¶ 56–59.

[6] See e.g., *Vikas v. State of Haryana*, 2022 SCC OnLine P&H 4978 (rejecting call data records for lack of proper certification despite reliability).

[7] Fed. R. Evid. 901(a) (U.S.) (requiring "evidence sufficient to support a finding that the item is what the proponent claims it is").

ISSN 2394 - 7780

through supporting documentation, expert testimony, or circumstantial evidence, allowing flexibility without compromising on evidentiary scrutiny.[1]

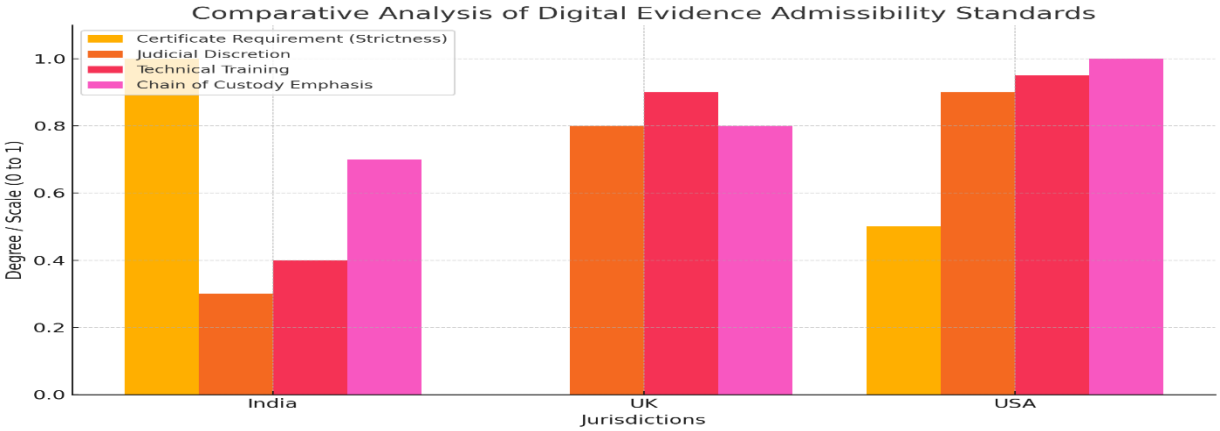
In the United States, the treatment of electronic evidence is governed by the Federal Rules of Evidence (FRE). Under Rules 901 and 902, electronic records are admissible if a party can establish that the item is what it claims to be.[2] Courts routinely examine the chain of custody, metadata, and expert forensic reports to assess the authenticity of digital evidence. Significantly, Rule 902(14), added in 2017, allows certain electronic records to be self-authenticating when accompanied by a certificate of a qualified person—akin to, but more flexible than, India's mandatory Section 65B certificate.[3]

What distinguishes these jurisdictions from India is not just the letter of the law, but also the institutional infrastructure and training that supports the handling of digital evidence. Judges, lawyers, and law enforcement personnel in both the UK and US are routinely trained in the technical and forensic dimensions of digital records. Moreover, courts in these countries adopt a purposive approach, focusing on the reliability and probative value of the evidence rather than excluding it for procedural lapses that do not compromise its integrity.

India stands to gain from these models. While the Bharatiya Sakshya Adhiniyam, 2023 retains the core structure of its predecessor regarding digital evidence, it could benefit from adopting international best practices that prioritise substance over form.[4] Incorporating principles such as judicial discretion, flexible authentication standards, and investment in forensic capacity could help Indian courts move from a compliance-heavy model to a justice-oriented framework.

Here is a comparative bar graph illustrating key differences in the admissibility of digital evidence across India, the UK, and the USA. It highlights how:

- *India enforces the most rigid certificate requirement.*
- *Judicial discretion and technical training are stronger in the UK and USA.*
- *Chain of custody practices are most robust in the USA.*



6. REFORM PROPOSALS AND RECOMMENDATIONS

Despite the evolving jurisprudence and the legislative shift from the *Indian Evidence Act, 1872* to the *Bharatiya Sakshya Adhiniyam, 2023*, the procedural and institutional ecosystem for handling digital evidence in India remains underdeveloped. A series of targeted reforms—both legal and structural—are necessary to bridge the gap between law and practice.

First, there is an urgent need to standardise procedures for the production, certification, and admissibility of electronic records. Investigating agencies, prosecutors, and litigants often struggle with varying formats, unclear protocols, and inconsistent judicial expectations regarding Section 65B (now Section 61) certification. A

[1] Fed. R. Evid. 902(14) (U.S.); see also Paul W. Grimm & Kevin F. Brady, *Authentication of Social Media Evidence*, 36 Am. J. Trial Advoc. 433, 444 (2013).

[2] Stephen Mason & Daniel Seng, *Electronic Evidence* 9–18 (5th ed. 2017).

[3] Civil Evidence Act 1995, c. 38, §§ 1–2 (UK); Criminal Justice Act 2003, c. 44, § 134 (UK).

[4] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 61, Gazette of India, Extraordinary, Part II, sec. 1 (Sep. 11, 2023).

ISSN 2394 - 7780

standard operating procedure (SOP) should be developed by a central authority, perhaps under the aegis of the Ministry of Home Affairs or the Supreme Court's e-Committee, to streamline how digital records are collected, certified, and presented in courts.

Second, capacity building and regular training programmes for judicial officers, prosecutors, defence lawyers, and police personnel must be institutionalised. Understanding how metadata, encryption, hash values, and digital signatures work is no longer optional for those involved in adjudication and investigation—it is essential. Collaborations with cyber forensic institutions and technical universities can help bridge the knowledge gap.

Third, the integration of digital forensics with legal proceedings must be systematised. Presently, the forensic analysis of digital evidence is often disconnected from the legal process, leading to delayed and fragmented understanding in court. Establishing dedicated cyber forensic units within district court systems, staffed with trained personnel, can help streamline this process.

Fourth, amendments to Section 61 of the Bharatiya Sakshya Adhiniyam (formerly Section 65B) should be considered. The law must evolve to allow exceptions where certification is impractical, particularly in cases involving third-party data or ephemeral communication. A presumption of authenticity—similar to Rule 902(14) of the U.S. Federal Rules of Evidence—could be introduced where reliable metadata or chain-of-custody documentation exists.

Finally, India urgently requires a comprehensive Code or set of Guidelines on Digital Evidence, issued by the Supreme Court or High Courts under their rule-making powers. Such a document should address admissibility standards, preservation practices, technical formats, expert roles, and rights of the accused. This would not only enhance consistency across jurisdictions but also restore confidence in the credibility of digital justice.

7. CONCLUSION

As technology redefines the way evidence is created, stored, and presented, Indian courts are being compelled to engage with increasingly complex digital records. The journey from *Navjot Sandhu* to *Arjun Panditrao Khotkar* reflects the judiciary's attempt to reconcile procedural safeguards with technological realities. The transition to the *Bharatiya Sakshya Adhiniyam, 2023* represents an important step in modernising Indian evidence law, particularly by reaffirming the role of digital evidence.

However, significant gaps remain. Procedural rigidity, infrastructural limitations, lack of standardisation, and uneven judicial practice continue to hinder the effective use of digital evidence. The challenge lies in striking a balance between ensuring the authenticity and integrity of electronic records and facilitating meaningful access to justice.

Moving forward, India must embrace a coherent techno-legal jurisprudence that is adaptive, inclusive, and consistent. Legal reforms must be accompanied by institutional strengthening, digital literacy, and policy-level coordination across law enforcement and the judiciary. Only then can the promise of digital justice become a practical reality—enhancing both the efficiency and credibility of the Indian legal system in the digital age.