Page 5033 - 5044 **DOI:** *https://doij.org/10.10000/IJLMH.119581*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

Digital Proof on Trial: An Analysis of Section 65B and Admissibility of Electronic Evidence in Trial Court

AKASH TRIPATHI[1]

ABSTRACT

The growing dependence on electronic technology in private and business life has generated a vast increase in the amount and importance of electronic documents. These comprise emails, electronic agreements, video recordings from monitoring, and mobile phone information, all of which can become vital pieces of evidence in court cases. But, as compared to conventional paper documents, electronic records pose distinct admissibility challenges because of authenticity, reliability, integrity, and tampering or manipulation issues.

This article discusses the legal provisions for the admissibility of electronic evidence, with an emphasis on the Indian legal system, particularly the Indian Evidence Act, 1872, as updated by the Information Technology Act, 2000. The core area of debate is Section 65B of the Evidence Act, which has prescribed special procedural and technical requirements for the admission of electronic evidence. The article discusses landmark judgments, such as Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, which had decided the jurisprudential approach to Section 65B certification as mandatory. In addition, the research compares United States and United Kingdom practices to see how common law jurisdictions are responding to equivalent challenges. It analyzes technological capabilities like hashing, digital signatures, and blockchain to establish their contribution towards making evidence more reliable. The paper concludes by proposing the creation of standardized protocols, judicial training in digital forensics, and legislative reform to bring legal processes into harmony with changing technological realities. Admissibility of electronic records remains a vital issue in securing justice being served and perceived to be served in the digital era.

Keywords*: Electronic Evidence, Admissibility, Section 65B, Digital Records, Indian Evidence Act, Information Technology Act, Digital Forensics, Legal Framework.*

[1] Author is a LL.M. student at Gautam Buddha University, Opposite Yamuna Expressway, Noida, Uttar Pradesh, India.

 [ISSN 2581-5369]

I. INTRODUCTION

The quick pace of information and communications technology (ICT) has completely revolutionized how people, corporations, and the government produce, store, and transmit information. The resulting electronic revolution has, in turn, contributed to a surge in increasing dependence on digital records—both emails and contracts to CCTV imagery and social networking data—as substantive forms of proof in civil as well as criminal proceedings. Subsequently, this has forced the judicial system to deal with problematic questions relating to the admissibility of digital records.

Compared to physical paper-based documents, electronic documents pose special problems concerning their authenticity, integrity, and reliability. Unlike physical documents, digital documents may readily be manipulated, erased, copied, or fabricated without leaving any trace. This creates serious questions about their evidentiary worthiness and the capacity of courts to accept them as authentic representations of fact.

Realizing these issues, legal frameworks of all the countries have started to modernize their evidentiary laws to include the admissibility of electronic records. In India, this process commenced with the passing of the Information Technology Act, 2000, by which the Indian Evidence Act, 1872 was amended to include certain provisions dealing with electronic records—most significantly Sections 65A and 65B. These provisions specify the technical requirements under which electronic evidence may be deemed admissible, centering on technical compliance and certification-based authentication.

Judicial rulings have been instrumental in defining the terrain of electronic evidence in India. Cases like Anvar P.V. v. P.K. Basheer (2014)[2] and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)[3] have established the compulsory nature of Section 65B certification and settled several practical issues concerning digital evidence.

In spite of such developments, serious gaps persist at the operational levels of applying the law. Several legal professionals don't have technical expertise to deal with or provide electronic evidence substantively, while courts struggle to cope with infrastructural and procedural constraints. Besides, newer technologies like blockchain, cloud storage, and artificial intelligence bring additional features that the available legal infrastructure does not completely embrace.

This article attempts to critically review the admissibility of electronic evidence from both legal

[2] *Justice Kurian Joseph, Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[3] *Justice R.F. Nariman, Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

 [ISSN 2581-5369]

and technological perspectives. It reviews statutory provisions, judicial decisions, and international best practices, as well as the technological tools and procedural measures required for guaranteeing the credibility and admissibility of digital evidence in contemporary legal systems.

II. DEFINITION AND SCOPE OF ELECTRONIC RECORDS

The definition of the term "electronic record" is meant to capture information or data that is generated, sent, received, or stored in a digital or electronic form, and not in traditional physical mediums like paper. In legal cases, the admissibility of such records will to a great extent depend on their legal definition, form, as well as the possibility of establishing their authenticity and integrity.

(A) Statutory Definition in Indian Law

In India, the definition of electronic records is based mainly on the Information Technology Act, 2000. As per Section 2(1)(t) of the Act:

"Electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer-generated microfiche.

This definition has been deliberately made broad to accommodate the variety of digital content. It encompasses textual documents (Word files, PDFs), audio and video files, images, emails, server logs, and even transactional data on digital platforms.

(B) Incorporation in the Indian Evidence Act, 1872

After the passing of the Information Technology Act, the Indian Evidence Act, 1872 was amended to incorporate electronic records into the traditional evidence framework. Section 3 of the Act, "definition of 'evidence'", was amended to include: "All documents including electronic records produced for the inspection of the Court…"This implies that digital records are now recognized as "documents" for legal purposes, hence subject to documentary evidence rules under the Act.

(C) Types of Electronic Records

Electronic records can be classified into different types depending on their nature and source: Communicative Records: Emails, SMS, chat transcripts, and social media posts. Transactional Records: Bank logs online, receipts online, digital invoices. Multimedia Evidence: CCTV images, photographs, audio and video recordings. Metadata and Logs: File creation timestamps, server access logs, GPS location information. Structured Databases: Relational database entries, spreadsheet entries, cloud-based records.

 [ISSN 2581-5369]

(D) International Approach

Under international legal systems, electronic records are also defined. For instance: The United Nations Commission on International Trade Law (UNCITRAL) defines an electronic record as information generated, communicated, received or stored by electronic means. Under the Federal Rules of Evidence (U.S.), Rule 1001(d) characterizes data stored in any medium as "writings" or "recordings," as long as they can be retrieved and utilized.

(E) Evidentiary Relevance

The application of electronic records in judicial proceedings is immense and on the rise. Courts increasingly use electronic documents in:

Civil cases: Contracts, letters, financial reports.

Criminal trials: Mobile data, surveillance records, online confessions.

Cybercrime cases: System logs, email headers, web activity.

Due to their significant role, it is crucial that the legal system makes them reliable and properly handled, particularly as they can easily be altered or deleted without physical traces.

III. LEGAL FRAMEWORK

The admissibility of electronic evidence in Indian courts is regulated by a mix of statutory law and judicial interpretations. The primary legal texts are the Indian Evidence Act, 1872, and the Information Technology Act, 2000. They collectively provide a framework to incorporate contemporary digital records into a legal system initially conceived for physical documents. The shift has created many interpretative and procedural issues, particularly regarding the authenticity and certification of electronic evidence.

(A) Indian Evidence Act, 1872

The Indian Evidence Act was, in 2000, amended by the Information Technology Act to include provisions for electronic records. Two important sections—Section 65A and Section 65B—were added to specifically address the admissibility of electronic evidence.

a. Section 65A – Special provisions as to evidence relating to electronic record

This section says that contents of electronic records can be established in accordance with the procedure to be followed under Section 65B. It is practically a gateway clause requiring the sole application of Section 65B in respect of electronic records.[4]

[4] Justice Kurian Joseph, in Anvar P.V. v. P.K. Basheer (2014), opined that Section 65B is a complete code and overrides general provisions pertaining to secondary evidence. This was a change from the previous opinion that

b. Section 65B – Admissibility of electronic records

Section 65B prescribes the procedural steps to be followed for admission of electronic records. Of note, it states that: Any information contained in an electronic record that is printed on paper, stored, recorded or copied in optical or magnetic media shall be deemed to be a document if certain conditions are satisfied and it is supported by a certificate under Section 65B(4).[5] The certificate should: Specify the electronic record. Provide a description of the mode of its production. Provide details of the device used. Be signed by an individual holding a responsible official position.

c. Section 22A – When oral admissions as to contents of electronic records are relevant Oral admissions are not applicable unless genuineness of the electronic record is doubtful. This makes oral evidence not able to substitute correct procedural compliance for admission of electronic documents.

d. Section 45A – Opinion of examiner of electronic evidence Inserted through the IT Act, the section provides the option for an opinion of a certified digital or forensic expert to be admitted and thus makes the professional expertise function stronger in judging electronic records.

(B) Information Technology Act, 2000

The IT Act is the supporting structure for Indian law recognizing electronic records.

Section 2(1)(t) defines "electronic record" comprehensively.

Section 3 and 3A gives legal authenticity to digital signatures and electronic signatures.

Section 4 gives effect to the equivalency of electronic records and paper-based records where information is available and usable for future reference.

Section 85B creates a presumption regarding the genuineness of electronic agreements where authenticated by secure electronic signatures. All these provisions together seek to give legal recognition, authentication, and enforceability to electronic communications and records.

(C) Presumptions Regarding Electronic Records

Section 85A: Presumption as to electronic agreements.

Section 85B: Presumption regarding secure digital signatures.

permitted oral testimony or other secondary evidence without strict compliance.

[5] In Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), Justice R.F. Nariman reaffirmed the same position, making it clear that Section 65B(4) certification is necessary except when the original device is led in court.

 [ISSN 2581-5369]

Section 85C: Presumption as to digital signature certificates.

Section 90A: Presumption as to electronic records older than five years.

These presumptions change the burden of proof and enable courts to accept some electronic records on face value, as long as they satisfy statutory requirements.

(D) Procedural and Practical Aspects

Although the law requires procedural protections for admissibility, practical issues remain: Who can give the certificate? Only an individual who is in charge of the computer system or device which created or stored the information, holding a responsible official position, may issue the certificate. What happens if the certificate is not obtainable? According to Arjun Panditrao, if the original device is created and tested in court, the certificate will not be required. Nonetheless, this is usually not practical. Is the certificate able to be filed subsequently? Yes. The court in Arjun Panditrao held that the certificate may be filed at any stage prior to the trial's conclusion.

IV. JUDICIAL PRECEDENTS

Judicial decisions have been the cornerstone of legal precedent regarding electronic evidence in India. The judiciary has undergone a transition from having a liberal approach to admissibility to having a more systematic and rigid approach over the past few years. Decisions of the Supreme Court have helped instill much-needed clarity, particularly under Section 65B of the Indian Evidence Act, 1872.[6]

1. Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473

This path-breaking judgment of Justice Kurian Joseph^1 was a watershed moment in the admissibility of electronic records. The Supreme Court reversed the earlier stand in State (NCT of Delhi) v. Navjot Sandhu (2005), and oral evidence was held to be acceptable for establishing electronic records. The Court held: "Evidence relating to electronic record, as discussed under Section 65B of the Evidence Act, is a code in itself." This judgment reiterated that secondary electronic evidence cannot be admitted unless there is satisfaction of Section 65B(4)—namely, a proper certificate given by a person competent to issue it.

2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1

Handed down by Justice R.F. Nariman^2, this judgment reaffirmed and clarified the Anvar ruling. The Court settled questions referred to a larger bench on the obligatory nature of Section

[6] Justice Kurian Joseph – *Anvar P.V. v. P.K. Basheer*

65B(4) certificates.[7]

Key takeaways: Section 65B certificate is obligatory for secondary electronic evidence.

It can be submitted at any stage of trial, including subsequent stages, provided it is in accordance with the statute. If the original device is manufactured in court, the certificate need not be produced. This case solidified the rule that electronic evidence lacking certification cannot be held valid regardless of how material it seems.

3. State (NCT of Delhi) v. Navjot Sandhu (2005) 11 SCC 600 (also referred to as the Parliament Attack case)

Before Anvar, this case by a bench comprising Justice P. Venkatarama Reddi^3 upheld the admissibility of electronic records without Section 65B certificates, if other evidence methods (e.g., oral evidence) proved them to be authentic.[8] This decision caused tremendous uncertainty and enabled a liberal approach, which was subsequently overruled in Anvar.

4. Tomaso Bruno v. State of Uttar Pradesh (2015) 7 SCC 178

Here, the Supreme Court emphasized the significance of electronic evidence, especially CCTV footage, in criminal investigations. The Court faulted the investigating agencies for failing to produce available electronic evidence and held that non-production of digital evidence can constitute withholding material evidence, affecting the trial's fairness.

5. Sonu @ Amar v. State of Haryana (2017) 8 SCC 570

In this decision, Justice R.K. Agrawal[9] reaffirmed the principle of strict compliance with Section 65B. He opined that un-certified electronic evidence is not admissible, even if there was no objection made at trial. The judgment made it clear that waiver cannot be made for admissibility by consent or default.

6. Shafhi Mohammad v. State of Himachal Pradesh (2018) 2 SCC 801

This decision of Justice A.K. Goel[10] attracted controversy by holding that Section 65B certificate is not required if the person availing proof does not possess the device. This stance was specifically overruled by the larger bench in Arjun Panditrao, which condemned Shafhi Mohammad for judicial overreach and for failing to discern the legislative mandate.

[7] Justice R.F. Nariman – *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*
[8] Justice P. Venkatarama Reddi – *State v. Navjot Sandhu*
[9] Justice R.K. Agrawal – *Sonu @ Amar v. State of Haryana*
[10] Justice A.K. Goel – *Shafhi Mohammad v. State of Himachal Pradesh*

 [ISSN 2581-5369]

V. CHALLENGES IN ADMISSIBILITY

Notwithstanding the increasing use of electronic records in the Indian evidentiary system, there remain important challenges to their unproblematic and equitable admissibility. These are both procedural and technical in nature, but commonly overlap in ways that influence the direction of litigation. Legal professionals, judges, and lawmakers need to appreciate these challenges.

(A) Procedural Challenges

a. Strict Compliance with Section 65B

The condition under Section 65B(4) of the Indian Evidence Act—that a certificate should be attached to any secondary electronic evidence—has caused a number of complications: In most instances, the individual creating or operating the device is unknown or unavailable, and certification becomes impossible. Delays in obtaining the certificate usually result in the exclusion of vital evidence at trial phases. Courts have been grappling with erratic practices: some accept late submission of certificates (as allowed in Arjun Panditrao[11]), whereas others outrightly reject them due to non-compliance.

b. Practitioner Lack of Awareness

Most lawyers and law enforcers lack technical expertise when it comes to handling digital evidence, e.g., extracting metadata, hash values, or obtaining logs securely.

This leads to: Mishandling of data, Inadequate storage and chain of custody, and Incomplete or deficient certification papers.

c. Lack of Clarity in Interpretation

Rulings such as Shafhi Mohammad v. State of Himachal Pradesh[12] caused temporary uncertainty by inferring that the certificate is not always required, particularly if the device is not in the custody of the party. While overturned in Arjun Panditrao, such conflicting judgments have caused disparity between courts.

(B) Technical Issues

a. Data Tampering and Alterations

Electronic data is susceptible to mutation and vulnerability. Electronic evidence can: Manipulated without any visible evidence, Copied or erased remotely, Edited with deepfakes, photo editing, or time stamp editors. This renders proof of authenticity and integrity highly

[11] Justice R.F. Nariman – *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*
[12] Justice R.F. Nariman – *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*

 [ISSN 2581-5369]

challenging without effective forensic evidence.

b. Metadata and Its Volatility

Metadata—data like time created, author, or device—is essential to verifying electronic records. However: Metadata may be changed or removed inadvertently (e.g., file transfer or printing). Lawyers typically produce electronic documents in hard form (screenshots or printouts), which delete essential metadata, degrading evidentiary quality.

c. Storage and Accessibility Challenges

Electronic documents saved on foreign servers or cloud platforms present jurisdictional and access challenges. It is challenging to: Procure foreign server or technology company certifications. Validate integrity when the storage platform is decentralized or resides in a foreign legal jurisdiction.

(C) Infrastructure and Capacity Limitations

a. Forensic Infrastructure Absence There are very few digital forensic labs in India, and the majority of courts lack technical experts or equipment to authenticate electronic records independently.

b. Delay in Investigation

Digital evidence tends not to be preserved over time, resulting in loss or corruption. For example, CCTV footage can be overwritten within a few days if not extracted and preserved right away. Police officers and investigating agencies tend to be ill-equipped to handle these timelines.

c. Privacy and Ethical Concerns

As the usage of electronic records such as social media posts, personal messages, and private emails grows, the right to privacy of individuals is compromised. Courts need to ensure: Electronic records are legally acquired (e.g., with proper warrants or consent). Sensitive personal data are handled confidentially and with care.

Not doing so can result in violations of Article 21 of the Constitution (right to privacy)[13], as held in the Puttaswamy v. Union of India judgment[14].

VI. TECHNOLOGICAL SOLUTIONS

To overcome the weaknesses and limitations of electronic records, courts and stakeholders have

[13] Constitution of India, Article 21 – Protection of life and personal liberty
[14] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1

to utilize an array of technological protocols and tools. These technologies can enhance the credibility, traceability, and admissibility of such records, if supported by legally accepted procedures and infrastructure.

(A) Digital Signatures and Hashing Algorithms

Digital signatures and hashing form the core of verifying electronic documents. A digital signature employs asymmetric cryptography to provide non-repudiation, whereas hashing functions such as SHA-256 produce a digital fingerprint of a file that is unique.

Indian courts recognize digital signatures by virtue of the Information Technology Act, 2000, Section 3(2)[15].

In State of Maharashtra v. Dr. Praful B. Desai, the Supreme Court permitted electronic records as reliable means of communication, observing the need to preserve the identity of sender and integrity of content[16]. Such technologies assist in authenticating the originality of emails, scanned documents, and transactional records in legal cases[17].

(B) Blockchain for Evidence Management

Blockchain provides an immutable, transparent bookkeeping system that is appropriate for keeping the chain of custody of digital evidence. Blockchain-kept records are cryptographically sealed and timestamped, which makes them tamper-resistant. A number of foreign jurisdictions, such as Estonia, employ blockchain to manage judicial records[18]. Blockchain has been piloted by law enforcement agencies of Gujarat and Maharashtra, although not yet mainstream in India[19].

(C) Tools for Metadata Extraction

Metadata like file creation date, GPS location, or device type provides a vital context regarding electronic records.

Software such as ExifTool, FTK, and EnCase are utilized by digital forensic teams to retrieve metadata[20].

Courts tend to analyze metadata to establish the chain of custody and to exclude tampering, as emphasized in Tomaso Bruno v. State of Uttar Pradesh (2015).

---

[15] Information Technology Act, 2000, Section 3(2) – Recognition of Digital Signatures
[16] *State of Maharashtra v. Dr. Praful B. Desai*, (2003) 4 SCC 601
[17] Solove, Daniel J., and Paul M. Schwartz, *Information Privacy Law*, Aspen Publishing, 2015
[18] Tapscott, Don and Alex Tapscott, *Blockchain Revolution*, Penguin, 2016
[19] Gujarat Police Adopts Blockchain to Track Cybercrime Evidence," *The Hindu*, 2022
[20] Casey, Eoghan, *Digital Evidence and Computer Crime*, Academic Press, 2011

 [ISSN 2581-5369]

(D) Digital Forensics and Cyber Labs

India is slowly increasing its network of Cyber Forensic Laboratories (CFLs). These labs assist in: Data recovery and verification,

Multimedia analysis, Tracking erased messages, call records, or modified photos. Expert witness testimony by certified digital forensic experts is frequently necessary under Section 45A of the Indian Evidence Act, 1872[21].

(E) E-Courts and Online Evidence Presentation

Indian courts are headed towards digitization under the e-Courts Mission Mode Project: Electronic evidence can now be filed online through e-filing portals. Video conferencing, remote examination, and screen sharing are now acceptable, particularly post-COVID-19, with procedural support from the Supreme Court[22].

(F) Safe Cloud-Based Evidence Vaults

Cloud-based evidence vaults provide: Access-restricted, encrypted stores for confidential digital files, Stamped logs for every upload and access point, Streamlined sharing with courts, lawyers, and police authorities. Singapore and Dubai courts already have safe cloud evidence portals; India's NIC Cloud (MeghRaj) is also being considered for digital court services.

(G) AI-Driven Evidence Validation

Artificial Intelligence software is increasingly being used for: Identification of deepfakes and manipulated media, Detection of anomalies in vast databases (such as money laundering), Voice identification and speaker recognition in computer audio files. AI-supported devices such as Amber Video (UK) and Serelay (UK) are already being adopted by investigators to authenticate videos. India is gradually shifting towards such integration^13.

VII. CONCLUSION

The admissibility of electronic records is a dynamic field at the intersection of law and technology. While significant legal developments have provided clarity, practical challenges remain. Ensuring the authenticity and integrity of electronic records is essential for justice delivery in the digital age. A holistic approach involving legislative reform, technological integration, and judicial education is imperative.

*****

[21] Indian Evidence Act, 1872, Section 45A – Opinion of Examiner of Electronic Evidence
[22] *In Re: Guidelines for Court Functioning through Video Conferencing*, Suo Motu Writ (Civil) No. 5/2020, Supreme Court

VIII. REFERENCES

- Indian Evidence Act, 1872
- Information Technology Act, 2000
- *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473
- *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1
- Federal Rules of Evidence (USA)
- Civil Evidence Act, 1995 (UK)
- Justice B.N. Srikrishna Committee Report on Data Protection (2018)
- Information Technology Act, 2000, Section 3(2) – Recognition of Digital Signatures
- *State of Maharashtra v. Dr. Praful B. Desai*, (2003) 4 SCC 601
- Solove, Daniel J., and Paul M. Schwartz, *Information Privacy Law*, Aspen Publishing, 2015
- Tapscott, Don and Alex Tapscott, *Blockchain Revolution*, Penguin, 2016
- "Gujarat Police Adopts Blockchain to Track Cybercrime Evidence," *The Hindu*, 2022
- Casey, Eoghan, *Digital Evidence and Computer Crime*, Academic Press, 2011
- *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 SCC 178
- Indian Evidence Act, 1872, Section 45A – Opinion of Examiner of Electronic Evidence
- National e-Governance Plan (NeGP) – e-Courts Mission Mode Project, Government of India
- *In Re: Guidelines for Court Functioning through Video Conferencing*, Suo Motu Writ (Civil) No. 5/2020, Supreme Court
- NIC Cloud Infrastructure – MeghRaj: https://cloud.gov.in
- Gaurav Jalan, "AI and Law Enforcement: Detecting Fake Evidence," *Bar and Bench*, July 2023
- "UK Police Using Deepfake Detection Tools," *The Guardian*, May 2022

*****

 [ISSN 2581-5369]