



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

SHORT ARTICLE: ELECTRONIC EVIDENCE IN COURT

-Kalyani Chaple

ABSTRACT

In today's digital era, electronic evidence has become one of the important part of the judicial system. Digital files- such as emails, text messages, photos, videos and GPS data, are frequently used as proof in both civil and criminal cases. To control how courts accepts admissibility of the electronic evidence, India first added rules to the Indian Evidence Act, which was later amended by the Information Technology Act of 2000. Today, updated rules for handling electronic proof are found in the Bharatiya Sakshya Adhiniyam, 2023. Various landmark judgments have justified the legal requirements for admitting electronic evidence.¹ Though, today also challenges such as data tampering, cybercrime, and authentication continues to exist. Thus, to ensure the reliability of electronic evidence, strong legal safeguards and technical expertise are essential.

KEYWORDS

Evidence, Electronic record, Admissibility, The Information Technology Act, 2000, The Indian Evidence Act, 1872, The Bharatiya Sakshya Adhiniyam, 2023

INTRODUCTION

Technology has evolved from how people communicate or work and even how to save our resources. In the modern world, proofs such as emails, WhatsApp messages and CCTV footage (basically any digital record) have provided themselves useful in civil and criminal cases to prove facts.

¹ *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

Parliament has given Recognition to these Electronic records and The Information Technology Act, 2000 inserted Sections 65A and 65B into the Indian Evidence Act, 1872². This provision is now replaced by Sections 61 to 63 currently in place as per the Bharatiya Sakshya Adhiniyam, 2023.³ They provided legal framework for the admissibility and proof of electronic records.

Electronic evidence is now used in cases which involves cybercrime, financial fraud, murder, and commercial litigation. However, since digital records can be altered or deleted, courts need proof of their authenticity and reliability before admitting them as an evidence. The Hon'ble Supreme Court, through various landmark decisions clarified these legal requirements. This article explains the concept, legal framework, admissibility, and challenges relating to the electronic evidence in court India.

MEANING OF ELECTRONIC EVIDENCE

Electronic evidence, or digital evidence — is a term for any information (usually but not limited to binary data) stored or transmitted in binary form that may be relied on as evidence either by producing it before the court to prove or disprove a fact of the case. It comprises of emails, WhatsApp chats, CCTV feeds as well as audio and video recordings in addition to digital photographs, geographic data or geolocation info GPS co-ordinates -- is an electronic document.

Electronic records are encompassed under the Information Technology Act, 2000⁴, while their admissible legal framework is guided by the Indian Evidence Act, 1872 and further bolstered under the new Bharatiya Sakshya Adhiniyam, 2023. Although electronic evidence is can be easily altered or manipulated as it is often accurate and reliable. Therefore, courts require strict compliance with legal procedures before allowing it as evidence.

TYPES OF ELECTRONIC EVIDENCE

Electronic evidence can be presented in many different forms, as these days the majority of information is generated, stored or communicated on electronic devices. Depending on the system type and information, we create different electronic evidence. Types of Electronic Evidence It is written as below in a common way.

² Information Technology Act, No. 21 of 2000, §§ 91–94 (India).

³ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63.

⁴ Information Technology Act, No. 21 of 2000.

- I. EMAILS:** The most used tool in business disputes, employment issues and criminal investigation to infer communication between parties.
- II. MESSAGES:** WhatsApp chats SMSs, Telegram messages and other types of communications can establish conversations, agreements the existence of an admission or a threat depending upon whether the legal requirements are met.
- III. CCTV FOOTAGE:** CCTV recordings provide direct visual evidence in criminal cases, thefts, road accidents for public safety matters.
- IV. RECORDINGS:** Audio recordings and videos can be used to prove conversations or events, if it is genuine and untampered.
- V. CALL DETAIL RECORDS:** CDRs relate details like the duration, numbers involved, and tower locations to assist a criminal investigation.
- VI. ELECTRONIC DOCUMENTS:** PDFs, spreadsheets, electronic contracts, bank records, and government databases are one of the important forms of a documentary evidence.

LEGAL FRAMEWORK GOVERNING ELECTRONIC EVIDENCE IN INDIA

The admissibility and proof of electronic evidence in India are governed by various statutes. The three most important laws are the Information Technology Act, 2000, the Indian Evidence Act, 1872, and the Bharatiya Sakshya Adhiniyam, 2023.

I. INFORMATION TECHNOLOGY ACT, 2000: The Information Technology Act, 2000 was enacted to provide legal recognition to electronic records and electronic transactions. Before this legislation, Indian law mainly recognized paper documents. The rapid growth of digital technology made it necessary to introduce a legal framework for electronic communication and digital evidence.

Some important provisions of the Information Technology Act include:

- 2(1)(t) Electronic record, which includes data, image or sound stored, received or sent in any electronic form.⁵
- Section 4 legalizes electronic records.⁶
- Digital Signatures are acknowledged in Section 5.⁷

⁵ Information Technology Act, No. 21 of 2000, § 2(1)(t).

⁶ Information Technology Act, No. 21 of 2000, § 4.

⁷ Information Technology Act, No. 21 of 2000, § 5.

- Retain electronic records as digital if the law requires documents to be retained - Section 7.⁸

The Act also made amendments to the Indian Evidence Act, 1872 allowing electronic records to be used as evidence in court.

II. INDIAN EVIDENCE ACT, 1872: The Information Technology Act inserted Sections 65A and 65B into the Indian Evidence Act, 1872 to specifically deal with electronic evidence.

- **Section 65A:** Section 65A provides that the contents of electronic records shall be proved according to the procedure prescribed under Section 65B. It is a special provision dealing exclusively with electronic evidence.
- **Section 65B:** Section 65B lays down the conditions under which electronic records become admissible in evidence. It provides that the electronic records containing, copied or printed from a computer can be considered as documents when statutory requirements are fulfilled. Most of the cases involving secondary electronic evidence require a Section 65B certificate to prove the authenticity of an electronic record. The source material lays emphasis on the fact that Section 65A states that special procedure for proving electronic records and Section 65B prescribes how such records are to be proved.

III. BHARATIYA SAKSHYA ADHINIYAM, 2023: The Bharatiya Sakshya Adhiniyam, 2023 replaced the Indian Evidence Act, 1872 and modernized the law relating to evidence.

The Act expressly recognizes electronic and digital records as evidence and contains provisions corresponding to Sections 65A and 65B of the earlier law.

- **Section 61** deals with proof of contents of documents.
- **Section 62** relates to primary evidence.
- **Section 63** governs the admissibility and proof of electronic records.⁹

The Bharatiya Sakshya Adhiniyam reflects the growing importance of technology in judicial proceedings and aims to simplify the legal framework relating to digital evidence while ensuring its authenticity and reliability.

⁸ Information Technology Act, No. 21 of 2000, § 7.

⁹ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63.

ADMISSIBILITY OF ELECTRONIC EVIDENCE

Admissibility-determining whether evidence is admissible in a court of law. Just having an electronic record does not mean that it is admissible. The record must adduce that the record is relevant, authentic in nature, trustworthy¹⁰, and it has been processed following the procedure prescribed by law.

Electronic records are prone to alteration, duplication, or manipulation. Hence, courts require that statutory protections are followed prior to relying on such evidence. Also, the difference between admissibility and evidentiary value. While a document may be permitted in evidence, the court will independently establish what weight or reliance it deserves based on all of the surrounding facts and context.

REQUIREMENT OF THE SECTION 65B CERTIFICATE

At any rate, one of the most critical prerequisites for conceding electronic proof is the Section 65B testament under the Indian Evidence Act (now Section 63 of the Bharatiya Sakshya Adhiniyam).¹¹

Certificate usually comes into play when secondary electronic evidence like a printout, CD, DVD or pen drives are produced.

A valid certificate usually contains:

- Details of the electronic record.
- Information about the computer or device.
- A statement that the device functioned properly.
- A declaration that the copy is accurate.
- Signature of a responsible official.

Where the original electronic device itself is produced before the court as primary evidence, a certificate may not always be necessary.

LANDMARK JUDICIAL DECISIONS

¹⁰ Indian Evidence Act, No. 1 of 1872, § 65B; Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63

¹¹ Indian Evidence Act, No. 1 of 1872, § 65B.

The Supreme Court of India has delivered several important judgments that have shaped the law relating to electronic evidence. These decisions have clarified the conditions for admissibility and the importance of maintaining the authenticity of electronic records.

- I. **STATE (NCT OF DELHI) V. NAVJOT SANDHU (2005)**¹²: The Supreme Court initially held that electronic evidence could, in certain cases, be admitted even without a Section 65B certificate through general rules of secondary evidence.
- II. **ANVAR P.V. V. P.K. BASHEER (2014)**¹³: This landmark judgment overruled *Navjot Sandhu* and held that:
 - Electronic evidence is governed exclusively by Sections 65A and 65B.
 - A Section 65B certificate is generally mandatory for secondary electronic evidence.
 - Oral evidence cannot replace statutory requirements.
- III. **SHAFHI MOHAMMAD V. STATE OF HIMACHAL PRADESH (2018)**¹⁴: The Court observed that a certificate might not always be required where the party producing the evidence does not possess the original device. This decision attempted to reduce practical difficulties.
- IV. **ARJUN PANDITRAO KHOTKAR V. KAILASH KUSHANRAO GORANTYAL (2020)**¹⁵: This judgment settled the law by holding that:
 - A Section 65B certificate is mandatory for secondary electronic evidence.
 - *Shafhi Mohammad* was overruled to the extent it relaxed this requirement.
 - Relaxation is permitted only in exceptional circumstances where obtaining the certificate is genuinely impossible.

CHALLENGES RELATING TO ELECTRONIC EVIDENCE

Although electronic evidence has in large extent improved the justice system, moreover it also creates several legal and practical challenges.

- I. **LIKELIHOOD OF MANIPULATION:** With digital records, information can be changed, edited and deleted in a matter of minutes or even fabricated. Computer

¹² *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.

¹³ *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

¹⁴ *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.

¹⁵ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

software used to manipulate images, video, email and electronic documents makes it impossible for a court to know if they are real.

- II. AUTHENTICATION:** Proving that the electronic record is actually genuine (this novel cannot be counterfeited) is another major obstacle. For example, the courts need to be satisfied that a record has not been amended between creation and submission such that it accurately reflects exactly what the original information was.
- III. COLLECTION AND PRESERVATION:** Proper forensic collection of the electronic evidence. Inappropriate sequencing can lead to data loss of crucial metadata, or can corrupt the original data, thus minimizing its evidentiary value.
- IV. INADEQUATE TECHNICAL KNOWLEDGE:** Judges, lawyers, investigating officers and police officials often do not have enough technical knowledge to comprehend complicated digital evidence. Disparity In the Contribution of Electronic Records During Trial
- V. CYBERCRIME AND DATA MANIPULATION:** The introduction and integration of artificial intelligence, deepfake technology (and similar technologies), hacking, cyber fraud, makes it easier to establish false electronic evidence. It urges courts to be more careful in assessing digital records.
- VI. CROSS-BORDER DATA:** A considerable number of electronic records are saved on cloud servers which lie outside India. Such hard evidence is rarely easy but often only possible by accessing international jurisdictions that aren't so obviously tethered to ransom-funded investigations and court processes.

CONCLUSION

In the current legal system, whether it is civil or criminal courts, electronic evidence has developed into one of the most potent types of evidence. Today, when communication, financial transactions, business and social activities are happened through digital platforms, facts before the courts need to be established via electronic records. Electronic evidence is produced by emails, WhatsApp messages, CCTV footage, digital photographs, and recorded calls (geospatial information), GPS data (global positioning system data or location data), social media post materials (including posts in the message form) forensic studies on electronic documents all these things have become an important part of civil as well as criminal litigation.

The Information Technology Act and the amendments to the Indian Evidence Act celebrated a major leap towards electronic records with evidence. The Bharatiya Sakshya Adhiniyam has

further modernized the law keeping electronic and digital records recognition intact but also streamlining the legal framework. Judgments such as *Anvar P.V. v. P.K. Basheer* and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*¹⁶ have satisfied conformation to Section 65B of the Indian Evidence Act, which governs the admissibility of electronic evidence, providing that the electronic record is automatic based on an information that it was required since if not it would defeat values of admissibility.

However, despite these regulatory improvements, other elements lead to inadequate access to electronic evidence –such as data manipulation and cybercrime; lack of technological capacity and skills; concerns related to privacy; and cross-border investigations. To respond to these challenges, it is imperative that advanced legal reforms and digital forensics infrastructure development take place, alongside training for judges and lawyers as well as raising of public awareness.

To conclude, electronic records have revolutionized the administration of justice in India. When it is collected, stored and presented in accordance with the law, it allows courts to get closer to the truth and thus deliver fair verdicts. Given technology's continuing evolution, the law must also continue to evolve, in order that electronic evidence is trustworthy and effective as an aid to protecting the rights of individuals and promoting the rule of law.

¹⁶ *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.