

Admissibility of Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023: A Critical Analysis of Evidentiary Standards and Judicial Challenges

¹Chanchal Meena., ²Dr. Pooja Jain

¹Research Scholar, School of Law, Mody University of Science and Technology, Lakshmangarh (Raj.)
332311

²Assistant Professor, School of Law, Mody University of Science and Technology, Lakshmangarh (Raj.)
332311

DOI: <https://doi.org/10.51584/IJRIAS.2026.11070073>

Received: 19 July 2026; Accepted: 24 July 2026; Published: 04 August 2026

ABSTRACT

This research investigates the admissibility of electronic evidence in accordance with the Bharatiya Sakshya Adhiniyam, 2023 (BSA), as well as the ways in which it has evolved as a result of the introduction of new technologies and the evolving views of the courts. Consequently, as a consequence of the rapid digitisation of communication, enterprises, and governments, contemporary court procedures are significantly dependent on electronic data such as emails, CCTV footage, call logs, and social media posts. An examination of the development of electronic evidence laws in India is presented in this article. Beginning with the Indian Evidence Act of 1872 and continuing all the way up to the Information Technology Act of 2000, which includes Sections 65A and 65B, the study begins with the Indian Evidence Act. It also examines the ways in which earlier instances have influenced current laws. The purpose of this research is to analyse Sections 61 and 63 of the BSA, 2023. These sections recognise electronic recordings as valid evidence and clarify certification criteria while putting an emphasis on authenticity and reliability. A fair trial and due process are guaranteed by Article 21 of the Indian Constitution, and the purpose of this research is to determine whether or not the BSA, 2023 achieves a satisfactory balance between these two conflicting objectives. However, the study indicates that the eventual success of the BSA, 2023 will be contingent on judicial interpretation, technology infrastructure, and continued legal training. This is despite the fact that the BSA, 2023 has made a promising beginning to modernizing evidential law. In light of this, the reform needs to be handled with caution and optimism.

Keywords: Electronic Evidence, Digital Records, Section, Bharatiya Sakshya Adhiniyam, Indian Evidence Act, Certificate, Admissibility, Data, Courts, Documents

INTRODUCTION

The rapid development of new technologies in the early and late 20th and 21st centuries has had a profound impact on the way evidence is presented. Online interactions are rapidly replacing more traditional methods of doing business, banking, government business, and even casual conversations. The use of electronic documents such as emails, digital signatures, CCTV video, GPS logs, call records, social media postings, and WhatsApp conversations has become more crucial in legal proceedings. Consequently, the reliability, validity, and admissibility of electronic records are often sought after by the courts.

As more and more crimes were committed using electronic devices, the judicial system had to adapt to this new reality. New gadgets are launched and utilised on a daily basis in the thousands. Computers' pervasiveness, IT's societal effects, and the capacity to store and gather data digitally have all prompted the need to revise Indian law to include criteria governing the recognition of novel evidence.

By adding Sections 65A and 65B to the Information Technology Act of 2000, lawmakers corrected the shortcomings of the previous framework and updated the Evidence Act of 1872. A unique procedure for deciding whether electronic records are admissible was set forth by these rules. Concerning the obligatory certification requirement under Section 65B in particular, the implementation of these rules caused considerable judicial debate and ambiguity.¹

The BSA, 2023, was introduced with the claimed goal of modernizing evidentiary rules and aligning them with digital reality. The new regulation specifically acknowledges electronic digital records within its definitional structure and restructures the admissibility framework.²

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.

Electronic evidence is becoming increasingly important in e-governance, e-commerce, and communication processes. Government agencies are adopting online governance norms and requiring frequent filings to oversee and control electronic industries.³ The use of electronic and digital evidence in court is steadily increasing. Authenticating electronic evidence such as CDs, DVDs, hard drives/memory cards, websites, social network communication, email, instant chat messages, SMS/MMS, and computer-generated documents provides distinctive difficulties.⁴

Evolution Of Electronic Evidence In India

The steady shift of the legal system from a paper-based evidential framework to a digitally responsive one is reflected in the historical development of electronic evidence in India. The Indian Evidence Act of 1872 was created for a colonial era when oral testimony and paper documents were the main forms of documentary evidence. Physical records served as the foundation for ideas like "documents," "primary evidence," and "secondary evidence." However, there was no mention of computers, digital communication, or electronic records in the act.⁵

The rapid growth of computers and internet communication in the late 20th century led to a major legal shift with the enactment of the Information Technology Act, 2000. This law added Sections 65A and 65B to the Indian Evidence Act of 1872, giving digital signatures and electronic recordings legal status. With Section 65B demanding a certificate to guarantee the validity and dependability of computer-generated documents, these provisions established unique guidelines for the admission of electronic evidence.

When considering electronic evidence, the Supreme Court was indulgent in the case of *State (NCT of Delhi) v. Navjot Sandhu*⁶. The court ruled that electronic documents might still be admissible if there was another method to prove their reliability and validity, even if Section 65B was not properly adhered to. Electronic documents, including call detail records, may nevertheless be accepted if their dependability and authenticity are otherwise shown adequately, the court decided, even if Section 65B of the Evidence Act is not strictly followed.

The Supreme Court's decision in *Anvar P.V. v. P.K. Basheer*,⁷ which required appropriate certification of electronic data for admission, prompted a reevaluation of this approach. Digital evidence that would have been crucial in proving a case's facts was often rejected due to this strict procedural requirement, even though its intention was to protect integrity. Electronic documents' evidentiary weight is determined by their legitimacy

¹ Indian Evidence Act, 1872, § 65B (4), No. 1, Acts of Parliament, 1872 (India).

² Bharatiya Sakshya Adhiniyam, 2023, Free Law (Feb. 26, 2026), <https://www.freelaw.in/legalarticles/Bharatiya-Sakshya-Adhiniyam-2023>.

³ Md Danish Azad, Admissibility of Electronic Evidence Under the Bharatiya Sakshya Adhiniyam, 2023: A Critical Analysis of Judicial Interpretation, 8 Indian J.L. & Legal Res. 4606 (2026).

⁴ Vivek Dubey, Admissibility of Electronic Evidence: An Indian Perspective, 4 Forensic Res. & Criminal Int'l J. 58, 58–63 (2017).

⁵ R.K. Bangia, Law of Evidence 45 (10th ed. 2020).

⁶ State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.

⁷ Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

and reliability, not only by their procedural conformance, as the Court made clear in *Arjun Panditrao Khotkar v. Kailash Kushanrao*⁸ Guarantee. The importance of electronic evidence was finally acknowledged in this verdict.

The Bharatiya Sakshya Adhiniyam codifies a more practical and explicit framework, building upon previous court judgements. In an effort to make the admission of digital data easier, the Act acknowledges their pervasiveness in today's society. The new legislation places a greater emphasis on credibility, dependability, and assessment of context than on procedural formalities, in contrast to the strict formalities of Section 65B. This shift shows that lawmakers recognise the importance of digital evidence in modern lawsuits and that the law has to alter to accommodate new technologies.⁹

Types Of Electronic Or Digital Evidence

- a) Digital evidence is anything that exists in digital form, such as data or information. The widespread use of technology in many parts of society has led to a rise in the diversity of digital evidence. Some examples of digital proof are as follows.
- b) Electronic messaging systems such as email, instant chat, and text messaging may provide digital evidence. Important digital evidence may be found in posts, messages, comments, and other information from social media sites like Facebook, Instagram, Twitter, and others.
- c) Other file types, such as spreadsheets, presentations, and digital documents, are also considered digital evidence. Metadata in these files could also include important information.
- d) Digital media such as photographs and videos may serve as compelling evidence. Metadata, such as timestamps and geolocation information, may be very useful in establishing the credibility and background of audiovisual assets.
- e) System logs, file access records, and browser histories are all examples of logs that chronicle internet and computer activity and may be used to evaluate digital evidence. Location data captured by mobile devices, certain digital cameras, and GPS systems are additional examples of digital evidence. Evidence in the digital realm might include call logs, durations, and time stamps.
- f) Records of financial transactions may be found in digital form as proof. Financial investigations may need this kind of information, which include online transactions, bank records, and electronic money transfers. Digital fingerprints, data for face recognition, audio recordings with unique voice characteristics, etc.

Admissibility Of Electronic Evidence Under Bsa, 2023

There are substantive changes which have been brought under the BSA, 2023 are as follows:

The BSA bolstered the admissibility of electronic evidence by adding Section 61, which states that its electronic form cannot be used to declare it inadmissible. Any document, digital or otherwise, shall be admissible and have the same validity, enforceability, and legal force as any other document provided that the conditions stated in Section 63 are met.

⁸ Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

⁹ D.J. Varghese, Evidentiary Value of Electronic Form Evidence Under Bharatiya Sakshya Adhiniyam, 2023, Judicial Vision, Nov. 2024, at [X].

*Section 61: Nothing in this Adhiniyam shall apply to deny the admissibility of an electronic or digital record in the evidence on the ground that it is an electronic or digital record and such record shall, subject to section 63, have the same legal effect, validity and enforceability as other document.*¹⁰

Except for information that is printed, stored, recorded, or duplicated on optical or magnetic media, this clause applies to electronic records held in semiconductor memory. The addition of the term "any communication device" in the BSA, 2023 has expanded the scope of this clause.¹¹

According to the BSA (2023), the certificate is still required, but it is now explicitly stated that the certificate must be provided with the electronic record every time it is shown for admittance.¹² In addition, the certificate was originally to be granted by an official in charge of the matter, but according to the BSA, 2023, the certificate may be issued by the owner of the computer or communication device as well as an expert.

Although the form of the certificate was not specified in the Evidence Act, it is now provided in the Schedule to the BSA, 2023. In Section A of the Schedule, the Party is required to fill out the form, and in Section B, the Expert is required to do the same. Under the BSA, 2023, the explanation that was previously provided under the Evidence Act is no longer there.¹³

Legal Framework Under The Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) is a landmark change in Indian law of evidence that supersedes the Indian Evidence Act, 1872, which dates back to the colonial period. The BSA, which will be put into effect on July 1, 2024, updates the legislation of evidence to reflect new technologies and the growing use of digital and electronic documents in court processes. In order to guarantee dependability, impartiality, and procedural integrity in both civil and criminal cases, the Act aims to provide a thorough framework for the admission, proof, and evaluation of electronic evidence.

Recognition of Electronic and Digital Records

The explicit inclusion of electronic data in the definition of "document" is one of the main characteristics of the Bharatiya Sakshya Adhiniyam, 2023. Emails, texts, social media postings, digital photos, CCTV footage, server logs, metadata, and cloud-based files are all included in this. The Act removes earlier uncertainty about whether electronic records should be treated as primary or secondary evidence.

The BSA works toward acknowledging some electronic documents as primary evidence where they are created from dependable systems or are in appropriate possession, in contrast to the prior framework that frequently classified electronic data as secondary evidence requiring stringent procedural verification. This illustrates the knowledge that digital records are not just copies but rather original electronic data.¹⁴

Certification and Procedural Safeguards

In accordance with the previous framework established by the Information Technology Act of 2000, Section 65B of the Evidence Act mandated that electronic evidence be admissible with an obligatory certificate. In instances like *Anvar P.V. v. P.K. Basheer*,¹⁵ judicial interpretation mandated this certification.

The BSA 2023 restructures criteria. The Act allows for more flexibility, but certification or verification remains essential. The court may not need a technical certificate in every situation if alternative trustworthy methods

¹⁰ The Bharatiya Sakshya Adhiniyam, 2023, § 61, No. 47, Acts of Parliament (India)

¹¹ Anjana Prakash & Anuj Prakash, The Bharatiya Sakshya Adhiniyam 385 (LexisNexis 2025).

¹² Shivam Pandey, A Study on Admissibility of Electronic Evidence with Reference to the Provisions of the Bhartiya Sakshya Adhiniyam, 2023, 2 Int'l J. L. Mgmt. & Humanities 1 (2024), <https://doi.org/10.5281/zenodo.11128137>.

¹³ Ibid.

¹⁴ Anmol Kumar, Aditi Srishti & Danish Sharma, Admissibility of Electronic Evidence in Criminal Proceedings: A Comprehensive Analysis, 5 Indian J. Integrated Res. L. 140 (2025).

¹⁵ *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

may confirm the integrity and validity of the electronic record. The process is simplified when acquiring a formal certificate is not feasible, such as when data is maintained by online platforms or third parties. The assumptions may be disproven. The opposite party might challenge the legitimacy, source, or integrity of electronic evidence via cross-examination or expert witness.

Electronic Evidence as Documentary Evidence

The Indian Evidence Act Section 65 specifies the admissibility of secondary evidence in particular cases. Section 65B specifies the procedure of proving the contents of electronic records which have been laid down under Section 65B.

Admissibility of electronic records mentioned as per Section 65B of Indian Evidence Act specifies that the printed any information of electronic records on a paper, or created a copy of that record on any optical or magnetic media shall also be deemed to be secondary evidence document if it satisfies the conditions mentioned under section 65B and original source of that information i.e. electronic device shall also be admissible without any further proof in any proceeding of the court of law.

Essentially elements of the electronic evidence as per the Indian Evidence Act are as follows:

1. Such produced information of electronic records should be produced by the person having legally authorized to have control over that electronic device.
2. That storage of information must take place during the day-to-day general course of the act of that person.
3. That stored information has been stored on that electronic device during the day-to-day general course of action of that person.

Electronic Signatures and Digital Authentication

A digital signature verifies an electronic record's legitimacy. It is a secure electronic code linked to a document to verify the sender and content. In addition to legal rules, courts must grasp technical procedures due to the growing use of electronic records. Judges and lawyers must analyse sophisticated digital material, which typically includes encryption, metadata, and data recovery. The change requires specialised training and skilled aid in processing electronic evidence. Technical inexperience might lead to misunderstanding or assessment of digital records. Law and technology must be integrated in contemporary judicial systems. Electronic evidence must not impair fairness, accuracy, or justice in courts. This shows how evidence law must adapt to technology.

Relationship with the Information Technology Act, 2000

There is no such thing as an independent Bharatiya Sakshya Adhiniyam. In tandem with the Information Technology Act of 2000, which establishes the legitimacy of electronic records, digital signatures, electronic governance, and safe electronic transactions, it contains laws pertaining to electronic evidence.

While the BSA controls whether electronic records may be included as evidence in court proceedings, the Information Technology Act provides the technical and regulatory groundwork for such documents. All of these laws work together to make electronic records easier to use while also protecting them from abuse and manipulation.

Evidentiary Standards For Digital Content In Courtrooms

Anvar P.K. vs. P.K.

Basheer This landmark case ruled that electronic evidence must conform to the requirements outlined in Section 65B of the Indian Evidence Act. The Supreme Court overturned previous decisions and clarified that a certificate under Section 65B (4) is mandatory for the admissibility of electronic evidence.

Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal¹⁶

Here, the Supreme Court addressed the admissibility of secondary evidence in the form of electronic records when the original records were not available. The court confirmed that the requirements of Section 65B (4) must still be met even when dealing with secondary evidence.

State (NCT of Delhi) v. Navjot Sandhu

This case focused on the interpretation of Section 65B (4) of the Indian Evidence Act. The Supreme Court emphasized the importance of strict compliance with the procedural requirements of Section 65B for the admissibility of electronic evidence.¹⁷

Anand Rajendran v. State

In this case, the Supreme Court of India examined the admissibility of electronic evidence in the form of call records obtained from a cellular service provider. The court held that to admit electronic evidence, including call records, it is necessary to comply with the provisions of Section 65B.

These cases demonstrate the evolving nature of digital evidence admissibility in Indian courts and the efforts made by the judiciary to adapt to the changing needs of society and technology. They serve as valuable precedents for future litigation involving digital evidence.¹⁸

Judicial Challenges In The Appreciation Of Electronic Evidence

Authenticity and Admissibility of Electronic Evidence: Implement stringent security measures throughout the collecting, preservation, and presentation phases to guarantee the validity and integrity of digital evidence. Make use of cryptography, digital signatures, and checksum techniques to ensure that digital evidence remains intact at all times.

Chain of Custody: Create and maintain an unbroken chain of custody to prove that the digital evidence has remained unchanged since its collection. Establish stringent protocols for dealing with digital evidence, and record all actions pertaining to the evidence.

Privacy, Digital Manipulation, and Cross-Border Data: Technology, cyber security, and digital privacy pose issues for courts. Electronic evidence may include personal chats, social media accounts, cloud data, and foreign server data. Artificial intelligence, deepfake technology, and sophisticated editing tools have made digital tampering simpler, forcing judges to be more cautious when examining electronic data. Judges must balance adequate criminal investigation with the constitutional rights to privacy and a fair trial.

Documentation and Record Keeping: Keep detailed records of the whole digital evidence lifecycle, from gathering to archiving to presentation. Ensure the integrity of evidence at all levels by creating thorough reports for each digital evidence file.

CONCLUSION

Electronic evidence is vital to India's legal system, and the BSA, 2023, provides a modern framework for its evaluation, preservation, and recognition. The Act ensures that justice is not denied due to small technological

¹⁶ Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, AIR 2020 SC 4908

¹⁷ <https://journals.sas.ac.uk/deeslr/article/download/2215/2149>

¹⁸ <https://www.linkedin.com/pulse/electronic-evidence-digital-cyber-law-india-adv-prashantmali->

faults, supporting Article 21 of the Constitution of India¹⁹'s personal liberty provision. Instead of procedural formality, it prioritises electronic evidence authenticity and reliability. The Indian judicial system must adapt to technology and use electronic evidence while preserving fairness and justice in its courtrooms. This judgement will create a precedent for electronic evidence admission in Indian courts for years to come.¹⁹

The BSA, 2023, modernises India's evidential framework for digital transformation. The Act balances authenticity with procedural practicality by acknowledging electronic and digital documents as admissible evidence and reorganising admission rules under Sections 61 and 63. Judgements like Anvar P.V. and Arjun Panditrao impact their interpretation. In the digital era, dependability and justice need effective implementation, forensic assistance, and judicial training.

REFERENCES

1. ANJANA PRAKASH, ANUJ PRAKAASH, THE BHARATIYA SAKSHYA ADHINIYAM 385 LexisNexis 2025
2. Basu, D. D. (2022). Law of Evidence (28th ed.). LexisNexis.
3. Batuk Lal. (2023). The Law of Evidence (26th ed.). Central Law Agency.
4. Government of India. (1973). The Code of Criminal Procedure, 1973. Ministry of Law and Justice. (Relevant for cases instituted before 1 July 2024.)
5. Government of India. (2000). The Information Technology Act, 2000 (Act No. 21 of 2000). Ministry of Law and Justice.
6. Government of India. (2023). The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023). Ministry of Law and Justice.
7. Government of India. (2023). The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023). Ministry of Law and Justice.
8. International Organization on Computer Evidence. (2002). Principles and Guidelines for Digital Evidence. IOCE.
9. Monir, M. (2021). Law of Evidence (12th ed.). Universal Law Publishing.
10. Pande, A. (2024). Bharatiya Sakshya Adhiniyam, 2023: A Commentary. Eastern Book Company.
11. United Nations Office on Drugs and Crime. (2013). Comprehensive Study on Cybercrime. United Nations.
12. Vivek Dubey, Admissibility of electronic evidence: an Indian perspective. Forensic Res Criminal Int J. 2017;4(2):58- 63

¹⁹ Astha Jain, Admissibility of Electronic Evidence Under the Indian Evidence Act, 1872, Manupatra (2022), <https://articles.manupatra.com/article-details/ADMISSIBILITY-OF-ELECTRONICEVIDENCE-UNDER-THE-INDIAN-EVIDENCE-ACT-1872>.