

International Journal Research Publication Analysis

Page: 01-09

DIGITAL EVIDENCE IN INDIAN COURTS: ADMISSIBILITY AND LEGAL CHALLENGES

*Aarti Valvi

India.

Article Received: 11 August 2026

*Corresponding Author: Aarti Valvi

Article Revised: 01 September 2026

India.

Published on: 21 September 2026

DOI: <https://doi-doi.org/101555/ijrpa.1288>

ABSTRACT

Digital technology has changed the way people communicate, conduct business, store information and create records. As a result, electronic material such as emails, WhatsApp chats, call detail records, CCTV footage, photographs, videos, social-media posts, GPS data and computer files has become increasingly important in legal proceedings. The admissibility of such material, however, depends not merely on its existence but also on its relevance, authenticity, integrity and the manner in which it is produced before a court. In India, the legal framework governing electronic evidence has undergone an important transition from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023. The new law specifically recognises electronic or digital records and provides a statutory framework for their proof and admissibility, particularly through Sections 61, 62 and 63. This article examines the legal position concerning digital evidence in Indian courts, the role of electronic-record certificates, and the practical difficulties associated with collection, preservation, authentication and presentation of digital material. It also discusses important Supreme Court decisions including *Anvar P.V. v. P.K. Basheer*, *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* and *Tomaso Bruno v. State of Uttar Pradesh*, while considering the transition to the new evidentiary regime. The article argues that effective digital-evidence law requires not only clear statutory rules but also technically competent investigation, reliable chain-of-custody practices, judicial awareness and standardised methods of preservation. A balanced approach is necessary so that courts can use technology as a reliable source of proof while protecting parties against fabrication, manipulation and unfair prejudice.

KEYWORDS: Digital Evidence; Electronic Records; Bharatiya Sakshya Adhiniyam, 2023;

Admissibility; Authentication; Cyber Law; Electronic Evidence.

1. INTRODUCTION

The rapid growth of digital technology has transformed the nature of evidence available in legal disputes. In earlier periods, courts mainly dealt with physical documents, registers, letters and oral testimony. Today, a large part of human activity leaves a digital trace. Communication through messaging applications, online transactions, emails, CCTV systems, smartphones, cloud services and social-media platforms can create records that may become relevant to a civil or criminal proceeding. Digital evidence is therefore no longer an exceptional category of proof; it is a regular part of modern litigation.

The legal importance of digital evidence lies in its ability to record events with considerable detail. A message may show the communication between two persons, a CCTV recording may show movement at a particular place, a call record may establish contact between individuals, and metadata may provide information about the creation or transmission of a file. At the same time, digital records can be copied, altered, deleted or manipulated without leaving obvious physical signs. This creates a central legal problem: a court must determine whether a digital record is genuinely what it is claimed to be and whether it has been preserved in a sufficiently reliable manner.

India's evidentiary law has responded to technological change over time. The Information Technology Act, 2000 gave legal recognition to electronic records, while the Indian Evidence Act, 1872 was amended to introduce Sections 65-A and 65-B dealing specifically with electronic records. The Supreme Court subsequently developed important principles concerning certification and admissibility. The Bharatiya Sakshya Adhiniyam, 2023 now provides the current statutory framework for electronic and digital records, replacing the earlier Evidence Act framework from the commencement of the new criminal-law regime.

This article examines the present legal framework, the development of judicial principles, practical challenges and possible measures for improving the handling of digital evidence in Indian courts.

2. Meaning and Nature of Digital Evidence

Digital evidence means information having evidentiary value that exists or is stored in digital or electronic form. It may be found on computers, mobile phones, servers, memory cards, cloud platforms, cameras, digital recorders, network systems and other electronic devices. Examples include emails, text messages, WhatsApp conversations, social-media content,

digital photographs, audio and video files, CCTV footage, call detail records, GPS information, browser history, transaction records and electronic documents.

Digital evidence differs from traditional documentary evidence in several ways. First, it is often intangible and dependent on a device or software environment for interpretation. Second, identical copies can be made easily, which makes the concept of an 'original' more complex. Third, metadata may contain important information about when, where and how a record was created or modified. Fourth, digital records may be vulnerable to alteration, deletion, compression or corruption. Therefore, reliability depends heavily on the process by which the evidence was collected, preserved and presented.

The court is not required to accept every digital file merely because it appears on a screen. Relevance, authenticity, integrity and compliance with applicable evidentiary requirements remain important. The evidentiary value of a screenshot, for example, may depend upon proof of its source, context and integrity. A digital record can be highly useful, but its reliability must be assessed through legally recognised methods.

3. Evolution of the Legal Framework in India

The Information Technology Act, 2000 was an important legislative step in recognising electronic commerce and electronic records. It helped establish the legal foundation for treating electronic information as legally significant. The Indian Evidence Act, 1872 was later amended to address electronic records specifically, particularly through Sections 65-A and 65-B.

Under the earlier regime, Section 65-B prescribed conditions for the admissibility of computer-generated electronic evidence. The Supreme Court's decisions made the certificate under Section 65-B central to the admission of certain forms of secondary electronic evidence. In *Anvar P.V. v. P.K. Basheer*, the Court clarified the importance of Section 65-B and rejected an approach that would bypass its statutory requirements for the relevant category of electronic evidence. In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, a Constitution Bench reaffirmed the mandatory character of the certificate requirement for secondary electronic evidence and addressed practical questions concerning its production.

The new Bharatiya Sakshya Adhiniyam, 2023 modernises this framework. Section 61 provides that an electronic or digital record cannot be denied legal effect merely because it is electronic or digital, subject to the statutory requirements. Section 62 states that the contents of electronic records may be proved in accordance with Section 63. Section 63 deals with the admissibility of electronic records and sets out conditions relating to the computer or

communication device, regular use, ordinary-course input, proper functioning and derivation of the information. It also provides for a certificate to accompany the electronic record when it is submitted for admission. The statutory text thus continues the emphasis on reliability and authentication while using terminology suited to contemporary digital systems.

4. Admissibility under the Bharatiya Sakshya Adhiniyam, 2023

The present framework gives electronic and digital records legal recognition while maintaining safeguards for their proof. Section 61 establishes that the electronic character of a record is not, by itself, a ground for exclusion. This is significant because digital records are now a normal part of social and commercial life.

Section 63 is particularly important. It treats qualifying computer output as a document and permits admissibility when the statutory conditions are satisfied. These conditions broadly concern regular use of the computer or communication device, regular feeding of information in the ordinary course of activities, proper operation of the device during the relevant period, and reproduction or derivation of the information from material fed into the system.

The certificate requirement under Section 63(4) is an important procedural safeguard. The certificate identifies the electronic record, describes how it was produced, provides appropriate particulars of the device involved and addresses the statutory conditions. The purpose is to provide the court with a basis for assessing the reliability of the electronic output rather than relying only on an unexplained printout or copy.

The distinction between primary and secondary evidence also remains relevant. The Act contains provisions concerning primary evidence and circumstances in which secondary evidence may be given. In digital cases, the practical question is often whether the material produced before the court is the original electronic record or a computer output, copy, printout or other representation. The applicable route of proof must therefore be identified carefully.

5. Important Judicial Decisions

Indian courts have played a major role in shaping the law of electronic evidence. The decisions under the former Evidence Act remain important for understanding the principles that influenced the present statutory framework.

In *Anvar P.V. v. P.K. Basheer* (2014), the Supreme Court considered the admissibility of electronic records and emphasised compliance with Section 65-B for the relevant form of electronic evidence. The decision moved the law towards a structured statutory approach rather than treating electronic evidence in the same way as ordinary documentary evidence

without regard to the special statutory provision.

In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), the Constitution Bench reaffirmed that the certificate required under Section 65-B was a condition precedent for the admissibility of secondary electronic evidence in the circumstances governed by that provision. The Court also discussed practical situations where a party may not possess the relevant device and explained that the law should not demand the impossible. The decision is significant because it attempted to balance procedural compliance with practical realities.

In *Tomaso Bruno v. State of Uttar Pradesh* (2015), the Supreme Court highlighted the importance of scientific methods and electronic evidence in modern investigation. The case involved CCTV-related evidence and the Court observed the significance of electronic records in establishing facts. The judgment illustrates that electronic evidence is not merely a technical issue; it can affect the search for the best available evidence.

These decisions demonstrate a consistent judicial concern with authenticity, reliability and proper procedure. With the *Bharatiya Sakshya Adhiniyam* now governing evidence, future courts will have to interpret the new provisions while drawing carefully on earlier principles where they remain relevant.

6. Types of Digital Evidence Commonly Used in Courts

Digital evidence can arise from many sources. CCTV footage is frequently relevant in criminal investigations, accidents, property disputes and security incidents. Mobile-phone evidence may include photographs, videos, messages, call records, location information and application data. Emails can be relevant in employment, commercial and contractual disputes. Social-media posts may become relevant in defamation, harassment, criminal and family-related proceedings.

Electronic financial records are also increasingly important. Bank transaction logs, payment confirmations, online invoices and digital-wallet records can establish the movement of money. Computer files and cloud-stored documents may be relevant to intellectual-property disputes, corporate investigations and contractual matters.

Each category presents different authentication issues. CCTV footage requires attention to the recording system, storage, continuity and possible alteration. Mobile-phone evidence requires careful seizure, preservation and extraction. Social-media material raises questions concerning account ownership, screenshots, source verification and context. Cloud records may involve third-party service providers and servers located in different jurisdictions. Therefore, a single uniform approach to all digital evidence may not always be sufficient.

7. Major Legal and Practical Challenges

The first major challenge is authenticity. A digital file can be copied or edited easily. A court therefore needs reliable information about the source and circumstances of the record. Screenshots can be particularly problematic because they may not contain all relevant metadata and can be altered.

The second challenge is preservation and chain of custody. Digital evidence can be damaged or modified during seizure, transfer or examination. Investigators should preserve the original device or data where appropriate, document each transfer and use reliable forensic methods. Weak chain-of-custody records can create disputes about whether the evidence presented in court is the same material that was originally collected.

The third challenge is technological complexity. Judges, lawyers and investigators may have different levels of technical knowledge. Digital evidence can involve metadata, encryption, cloud storage, hashing, device logs and forensic extraction. Without adequate understanding, courts may face difficulties in assessing technical claims.

The fourth challenge concerns access to devices and service providers. Evidence may be stored on a third-party platform or outside India. Investigators may need lawful processes to obtain records, while privacy and data-protection considerations must also be respected.

The fifth challenge is the rapid development of artificial intelligence and synthetic media. Audio, images and videos can now be generated or manipulated with increasing sophistication. This makes traditional visual or auditory assumptions less reliable. Courts may increasingly require expert assistance and technical verification when authenticity is seriously disputed.

The sixth challenge is delay. Electronic records may be voluminous. A single device can contain thousands of files and messages. Courts need practical procedures for identifying relevant material without compromising the rights of parties. Digital evidence management systems and forensic indexing can help reduce unnecessary delay.

8. Digital Evidence and Privacy

The collection of digital evidence must also be considered in the context of privacy. A mobile phone may contain intimate communications, photographs, financial information, location history and information concerning third parties. Investigators and litigants therefore need to avoid treating every piece of data on a device as automatically available for unrestricted use.

The right to privacy recognised by the Supreme Court has implications for the lawful collection and use of personal information. At the same time, privacy cannot be considered in

isolation from legitimate investigation and adjudication. The challenge is to maintain a proportionate balance between obtaining relevant evidence and avoiding unnecessary intrusion.

Courts may need to consider questions such as whether the data was lawfully obtained, whether the material is relevant, whether disclosure can be limited to necessary information, and whether sensitive information belonging to unrelated persons should be protected. Confidentiality directions, redaction and controlled access may become increasingly important in cases involving large digital datasets.

9. Role of Experts and Forensic Technology

Digital forensic experts can assist courts by explaining how data was acquired, preserved, examined and interpreted. Technical examination may involve forensic imaging, hash values, metadata analysis, log analysis and recovery of deleted information. Such processes can help establish whether a digital record has remained substantially unchanged and whether the claimed source is technically plausible.

Expert evidence does not replace the judge's legal role. The court must decide admissibility and evidentiary weight according to law. However, technical assistance can make complex evidence understandable and can help identify manipulation or inconsistencies.

There is also a need for standardised forensic procedures. Investigating agencies should maintain documented protocols for seizure, imaging, storage and examination. Secure evidence repositories and controlled access can reduce the risk of accidental modification. Training should be provided not only to forensic personnel but also to police officers, prosecutors and members of the judiciary.

10. Suggestions for Strengthening the Digital Evidence Framework

First, courts and investigative agencies should develop clear and uniform procedures for the collection and preservation of digital evidence. Every important step from seizure to courtroom production should be documented.

Second, forensic laboratories should be strengthened with trained personnel and modern infrastructure. Digital evidence is technically complex, and reliable examination requires appropriate tools and expertise.

Third, certificate procedures should be made practical and standardised. Clear formats and guidance can reduce avoidable disputes while preserving the safeguards intended by the law.

Fourth, judicial and legal education should include basic digital-forensics concepts. Lawyers

and judges need not become computer scientists, but an understanding of metadata, hashes, device extraction and chain of custody can assist in evaluating evidence.

Fifth, courts should encourage secure digital evidence management. Proper indexing, audit trails and restricted access can reduce the possibility of alteration or loss.

Finally, the legal system should continue adapting to emerging technologies such as cloud computing, encrypted communication, blockchain records and AI-generated or manipulated content. Technology changes quickly, so legal interpretation and procedural guidance must remain sufficiently flexible to address new forms of evidence.

11. CONCLUSION

Digital evidence has become an essential part of the Indian justice system. The transition from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023 reflects the increasing importance of electronic and digital records. Sections 61, 62 and 63 provide a structured statutory basis for recognising and proving such evidence, while maintaining safeguards concerning reliability and certification.

The principal challenge is not simply whether digital evidence should be admitted. The more important questions are whether it is authentic, intact, relevant, lawfully obtained and presented through a reliable process. Judicial decisions under the earlier law, particularly *Anvar P.V.*, *Arjun Panditrao Khotkar* and *Tomaso Bruno*, demonstrate the importance of these principles.

Future litigation will involve increasingly complex digital material, including cloud records, encrypted communications, location data and synthetic media. A sound legal system must therefore combine statutory clarity with technical competence. Better forensic infrastructure, consistent chain-of-custody procedures, judicial training and responsible handling of privacy can improve confidence in digital evidence.

Digital evidence can significantly strengthen fact-finding when properly collected and authenticated. At the same time, procedural safeguards are necessary to protect parties against fabrication, manipulation and misuse. The continuing task for Indian courts is to maintain this balance while ensuring that evidentiary law keeps pace with technological development.

REFERENCES

1. Bharatiya Sakshya Adhiniyam, 2023, especially Sections 59–63.
2. Information Technology Act, 2000.
3. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
4. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
5. Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178.
6. Supreme Court of India, judgments and official judicial resources relating to electronic evidence.
7. India Code, official text of the Bharatiya Sakshya Adhiniyam, 2023.
8. Relevant provisions and judicial decisions concerning electronic records, authentication, certification and digital forensic evidence.