



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.

DIGITAL EVIDENCE IN COURTS: ADMISSIBILITY, AUTHENTICATION, AND CHALLENGES IN THE DIGITAL AGE

- PRAKRITI TYAGI

ABSTRACT

The rapid advancement of information and communication technology has significantly transformed the manner in which information is created, stored, communicated, and utilised in the society and thus, it also has changed the nature of evidence presented before courts worldwide. In the contemporary era, individuals, businesses, and governmental institutions increasingly rely on electronic devices and digital platforms for communication, transactions, record-keeping, and daily activities. Consequently, a substantial amount of information relevant to legal disputes and criminal investigations now exists in digital form. This information, commonly referred to as digital evidence or electronic evidence and it has emerged as one of the most important forms of evidence in modern judicial proceedings. Traditionally documentary and oral evidence were used and now they are increasingly supplemented or replaced by digital evidence such as emails, text messages, social media posts, CCTV recordings, GPS data, call records, digital photographs, electronic contracts, cloud-based records, and metadata. Digital evidence has become indispensable in both civil and criminal litigation due to the extensive use of electronic devices in daily life. However, the unique characteristics of digital evidence raise significant legal and procedural challenges regarding authenticity, reliability, admissibility, privacy, and preservation.

In this paper we will examine the concept of digital evidence, its legal framework, methods of collection and preservation admissibility requirements, and challenges faced by courts in evaluating electronic documents. Special emphasis is placed on the Indian legal system, particularly the provisions of Bhartiya Sakshya Adhiniyam, 2023¹, and the Information Technology Act, 2000², the judicial pronouncements concerning electronic evidence. The study further analyses emerging concerns such as cybercrime, data manipulation, artificial intelligence-Generated content, and cross border digital investigations. The paper concludes by suggesting reforms and best practices for ensuring the integrity and reliability of the digital evidence and judicial proceedings.

INTRODUCTION

¹ Information Technology Act, No. 21 of 2000, India Code.

² Bharatiya Sakshya Adhiniyam, No. 47 of 2023, India Code.

The 21st century has witnessed the unprecedented Digital revolution. Computers, smartphones, cloud storage systems, social networking platforms and electronic communication tools have become an integral part of modern society. As a result, human activities increasingly leave digital footprints that can serve as valuable evidence in legal proceedings. Digital evidence refers to any information stored or transmitted in the digital form that may be used to establish facts in a court of law. Unlike traditional evidence, digital evidence is intangible, easily reproducible, susceptible to alteration, and often requires specialized technical experts for interpretation.

In India, the recognition of electronic evidence gained prominence with the enactment of the Information Technology Act, 2000, which amended the Indian Evidence Act, 1872³, particularly by section 65A and 65B which established the legal requirement for the admissibility of electronic records. Today digital evidence plays a crucial role in criminal investigation. Commercial disputes, cybercrime cases, matrimonial disputes, industrial disputes, intellectual property litigation, and national security matters.

The increasing dependence on digital technology has made it essential for the courts to establish reliable standards for the collection, preservation, authentication, and admissibility of electronic evidence. Failure to do so may undermine the administration of justice and compromise the percent sign rights of litigants and also negatively impact the Indian evidence system. Students Encompasses any information stored, generated, transmitted or received in electronic form that possesses evidentiary value and may be presented before a court to establish or disprove a fact in issue. Unlike conventional documentary evidence, digital evidence exists in intangible form and requires technological devices and specialized software for access, preservation, examination and interpretation. Electronic evidence includes email, instant messages, text messages, electronic documents, spreadsheets, database, Digital photographs, audio recordings, video recordings, surveillance footage, metadata, server logs, cloud-based records, internet browsing history, blockchain records, Biometric information, GPS Location data, internet protocol (IP) logs, cryptocurrency transaction records and numerous other forms of electronically stored information. The diversity and complexity of these resources have significantly expended the scope of evidence available to courts while simultaneously creating new legal and procedural challenges.

The increasing reliance upon electronic evidence has compelled the legal system across the world to reconsider traditional evidentiary principles. Developed during an era dominated by paper-based documentation conventional rules. Concerning originality, authenticity, hearsay and documentary proof often prove inadequate. When applied to electronic documents which may exist simultaneously in Multiple identical copies across various devices and cloud servers, unlike paper documents that possess identifiable physical characteristics, digital files and dynamics easily transferable and capable of instantaneous modification. Consequently Legislatures and courts have been required to formulate their specialized legal framework governing the admissibility and authentication. Preservation and evaluation of electronic evidence while ensuring fairness, reliability and procedural integrity within the judicial proceedings.

³ Indian Evidence Act, No. 1 of 1872, India Code.

Judicial interpretation has played an equally significant role in clarifying the legal status of electronic evidence in India. Over the past two decades, the Supreme Court of India has delivered several landmark judgments addressing complex issues relating to the admissibility and authentication of electronic records. Decisions such as *State (NCT of Delhi) v. Navjot Sandhu*⁴, *Anvar P.V. v. P.K. Basheer*⁵, *Shafhi Mohammad v. State of Himachal Pradesh*⁶, and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*⁷ have substantially influenced the legal standards governing digital evidence. These judgments illustrate the judiciary's evolving approach toward balancing technological realities with procedural safeguards, while emphasizing the importance of maintaining the integrity and reliability of electronic records. Collectively, these judicial pronouncements have established that compliance with statutory requirements is essential to ensure that digital evidence satisfies the standards of admissibility expected within the criminal justice system and civil adjudication.

Notwithstanding these developments, the use of digital evidence presents numerous legal, ethical, and practical challenges. The exponential growth of electronic data has significantly increased the complexity of investigations, often requiring authorities to examine enormous volumes of information spread across multiple devices, networks, and cloud-based platforms. Cross-border storage of digital information frequently raises jurisdictional issues requiring international cooperation through mutual legal assistance treaties and transnational investigative mechanisms. Encryption technologies designed to protect individual privacy may simultaneously impede lawful investigations by restricting access to relevant evidence. Moreover, concerns relating to cybersecurity, data breaches, unauthorized surveillance, unlawful interception, and misuse of personal information continue to generate debates regarding the appropriate balance between effective law enforcement and the protection of fundamental rights.

The constitutional dimension of digital evidence has acquired particular significance in light of the recognition of the right to privacy as a fundamental right under Article 21 of the Constitution of India. The collection, storage, and analysis of electronic data often involve access to highly personal information concerning an individual's communications, movements, financial transactions, health records, professional activities, and social interactions. Consequently, investigative authorities must ensure that the acquisition of digital evidence complies with constitutional guarantees of privacy, legality, necessity, proportionality, and procedural fairness. Courts are increasingly required to balance the state's legitimate interest in investigating offences with the individual's right to informational privacy, thereby making digital evidence an area where constitutional law, criminal procedure, forensic science, and information technology intersect.

MEANING OF DIGITAL EVIDENCE

The concept of evidence has evolved significantly with the advancement of information and communication technology. Traditionally, evidence consisted of oral testimony, written documents, physical objects, and expert opinions. However, the digital revolution has transformed the way information is created, stored, transmitted, and preserved. In the present

⁴ *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 S.C.C. 600 (India).

⁵ *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).

⁶ *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 S.C.C. 801 (India).

⁷ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1 (India).

era, a substantial portion of human interaction occurs through electronic devices such as computers, smartphones, tablets, servers, cloud platforms, and internet-based applications. Consequently, these interactions generate electronic records that possess immense evidentiary value in legal proceedings. Such electronically stored information is collectively known as digital evidence or electronic evidence.

Digital evidence may be defined as any information of probative value that is stored, generated, transmitted, received, or preserved in digital form and can be presented before a court to prove or disprove a fact in issue. Unlike conventional documentary evidence, digital evidence does not exist in a tangible form. Instead, it consists of binary data that can only be accessed through electronic devices and specialized software. This intangible nature distinguishes digital evidence from traditional forms of proof and necessitates the adoption of specific legal and forensic procedures to ensure its authenticity and reliability.

The *Scientific Working Group on Digital Evidence (SWGDE)* defines digital evidence as "information of probative value that is stored or transmitted in binary form." Similarly, the *International Organization on Computer Evidence (IOCE)* describes digital evidence as information stored or transmitted in digital form that may be relied upon in court proceedings. These definitions emphasize that the evidentiary value of digital information depends not merely upon its existence but also upon its relevance, authenticity, integrity, and reliability.

In modern litigation, digital evidence extends far beyond conventional computer files. Emails, instant messaging conversations, social media interactions, electronic contracts, surveillance recordings, mobile phone data, GPS coordinates, biometric records, cloud-based documents, internet browsing history, blockchain transactions, metadata, and even data generated by wearable devices constitute forms of digital evidence. As technology continues to evolve, new categories of digital evidence continue to emerge, reflecting the increasing integration of digital systems into every aspect of human activity.

NATURE OF DIGITAL EVIDENCE

Digital evidence possesses several characteristics that fundamentally distinguish it from traditional documentary and physical evidence. Understanding its unique nature is essential for appreciating the legal and procedural safeguards governing its admissibility.

Firstly, digital evidence is intangible. Unlike paper documents or physical objects, electronic records cannot be examined with the naked eye. They exist in the form of binary code comprising sequences of zeros and ones, which require electronic devices and software for interpretation. Consequently, courts often depend upon digital forensic experts to explain the technical aspects of electronic evidence.

Secondly, digital evidence is extremely fragile. A simple action such as opening a file, connecting a storage device to a computer, or switching on a mobile phone may alter metadata, modify timestamps, or overwrite existing information. Similarly, viruses, malware, hardware failures, software updates, or accidental deletion may permanently destroy valuable evidence. This fragility necessitates the adoption of forensic procedures that preserve the original state of electronic data throughout the investigation.

Another important characteristic is reproducibility. Unlike physical evidence, digital evidence can be copied an unlimited number of times without any degradation in quality. Every copy of a digital file is technically identical to the original, making it difficult to distinguish between the original record and its duplicates. Consequently, courts rely upon forensic techniques such as cryptographic hash values to establish the authenticity and integrity of electronic evidence.

Digital evidence is also highly susceptible to manipulation. Sophisticated software enables individuals to modify photographs, edit videos, fabricate documents, alter metadata, forge electronic signatures, and create entirely false digital identities. Recent developments in artificial intelligence have introduced deepfake technology capable of generating realistic but fabricated audio and video recordings. These technological capabilities make authentication one of the most critical aspects of electronic evidence.

Furthermore, digital evidence is persistent. Contrary to common perception, deleting a digital file does not necessarily eliminate it permanently. Deleted information often remains recoverable until overwritten by new data. Digital forensic experts can recover deleted files, emails, messages, browsing history, and even fragments of previously erased information using specialized recovery tools. This characteristic has greatly enhanced the effectiveness of criminal investigations and civil litigation.

Finally, digital evidence frequently contains metadata, commonly described as "data about data." Metadata records information such as the date of creation, author, modification history, device identification, file location, GPS coordinates, access times, and software used to create the document. Metadata often provides valuable contextual information that assists courts in determining authenticity and identifying possible tampering.

SCOPE OF DIGITAL EVIDENCE

The scope of digital evidence has expanded dramatically in recent decades owing to the widespread digitization of society. Today, electronic evidence plays a central role in almost every branch of law.

In criminal law, digital evidence is indispensable for investigating offences such as murder, terrorism, kidnapping, financial fraud, cybercrime, sexual offences, narcotics trafficking, corruption, organized crime, and money laundering. CCTV footage, call detail records, mobile phone location data, internet search history, emails, surveillance recordings, and social media communications frequently assist investigators in identifying suspects and reconstructing criminal events.

In civil litigation, electronic records determine contractual obligations, commercial negotiations, intellectual property rights, insurance claims, consumer disputes, banking transactions, taxation matters, and corporate governance issues. Modern commercial transactions rely extensively upon electronic documentation, making digital evidence the foundation of business litigation.

Family courts increasingly depend upon digital evidence in matrimonial disputes, including divorce, maintenance, domestic violence, and child custody proceedings. WhatsApp

conversations, emails, social media posts, digital photographs, and call records frequently establish cruelty, adultery, harassment, neglect, or financial misconduct.

Digital evidence has become equally important in administrative law, constitutional litigation, environmental disputes, labour law, competition law, consumer protection, arbitration proceedings, and international commercial disputes. The increasing digitalization of governance through e-governance initiatives further expands the role of electronic evidence in public administration and judicial review.

The emergence of electronic governance, digital banking, online education, telemedicine, cryptocurrency, artificial intelligence, blockchain technology, and the Internet of Things (IoT) has significantly broadened the scope of electronic evidence. Smart devices continuously generate electronic records that may become relevant in future judicial proceedings, making digital evidence an indispensable component of modern justice systems.

TYPES OF DIGITAL EVIDENCE

The rapid advancement of digital technology has resulted in the creation of numerous forms of electronic evidence, each possessing distinct evidentiary significance depending upon the nature of the dispute. Among the most common forms of digital evidence are electronic communications, including emails, SMS messages, and conversations conducted through instant messaging platforms such as WhatsApp, Telegram, Signal, and Facebook Messenger. These communications frequently establish contractual negotiations, criminal conspiracies, financial transactions, threats, admissions, or personal relationships, making them highly relevant in both civil and criminal proceedings.

Another important category consists of social media evidence. Platforms such as Facebook, Instagram, X (formerly Twitter), LinkedIn, Snapchat, and YouTube have become integral parts of daily communication. Posts, comments, photographs, videos, direct messages, live streams, and user interactions on these platforms often provide valuable evidence regarding an individual's intentions, activities, location, associations, or state of mind. Courts increasingly rely upon social media evidence in cases involving defamation, cybercrime, matrimonial disputes, hate speech, election offences, and intellectual property violations.

Digital photographs, audio recordings, and video recordings constitute another significant category of electronic evidence. CCTV surveillance footage, mobile phone recordings, dashcam videos, body-worn cameras, and security surveillance systems frequently assist investigators in reconstructing incidents and identifying suspects. Similarly, audio recordings may establish admissions, threats, contractual agreements, or other legally relevant conversations. However, because such recordings may be edited or manipulated, their authenticity must be carefully verified through forensic examination.

Electronic documents such as PDF files, word processing documents, spreadsheets, presentations, electronic contracts, invoices, and digital signatures also constitute important forms of digital evidence. Businesses, government agencies, and individuals increasingly conduct transactions electronically, making these records indispensable in commercial litigation, taxation matters, banking disputes, and corporate investigations.

Another rapidly expanding category includes mobile device evidence. Modern smartphones store vast quantities of information relating to communications, contacts, photographs, videos, browsing history, GPS locations, financial transactions, health records, and application usage. Mobile forensic analysis often enables investigators to reconstruct an individual's movements, communications, and activities with remarkable accuracy.

Digital evidence further extends to cloud-based information, including data stored on platforms such as Google Drive, Microsoft OneDrive, Dropbox, Apple iCloud, and similar services. Since cloud storage enables users to access data remotely from multiple devices, it has become an increasingly valuable source of evidence in civil litigation, commercial disputes, and cybercrime investigations.

An equally significant category consists of network and server records, including IP logs, firewall records, server logs, internet browsing history, login records, and network traffic data. These records assist investigators in identifying unauthorized access, tracing cyberattacks, determining user activity, and establishing digital timelines.

Emerging technologies have introduced entirely new categories of digital evidence. Information generated by Internet of Things (IoT) devices, wearable technology, smart home systems, vehicle navigation systems, biometric authentication devices, fitness trackers, and blockchain-based platforms is increasingly becoming relevant in judicial proceedings. These technologies continuously generate electronic records capable of establishing location, identity, health information, movement, and other legally significant facts. Consequently, the scope and diversity of digital evidence continue to expand alongside technological innovation.

EVIDENTIARY VALUE OF DIGITAL EVIDENCE

The evidentiary value of digital evidence has increased dramatically with the growing digitization of society. In contemporary legal proceedings, electronic records frequently provide more precise, objective, and comprehensive information than traditional forms of evidence. Unlike oral testimony, which may be influenced by memory lapses, bias, or perception, digital evidence is often automatically generated by electronic systems and therefore contains accurate timestamps, location information, user identifiers, metadata, and system-generated records. These characteristics enable courts to reconstruct events with greater accuracy and reliability.

The evidentiary value of digital evidence, however, depends upon several legal and technical considerations. The electronic record must first be relevant to the facts in issue and must satisfy the statutory requirements governing admissibility. Courts further require proof that the evidence is authentic, has not been altered, and has been collected and preserved according to accepted forensic standards. The maintenance of an unbroken chain of custody, compliance with statutory certification requirements where applicable, and expert forensic analysis significantly enhance the credibility of electronic records.

Digital evidence has become indispensable in criminal investigations, where CCTV footage, call detail records, mobile phone data, GPS information, surveillance recordings, and social media communications frequently establish motive, identity, presence at the crime scene, and the sequence of events. Similarly, in civil litigation, electronic contracts, emails, banking

records, electronic invoices, and digital correspondence often determine contractual rights, commercial obligations, and financial liabilities. The growing reliance upon electronic governance and digital transactions has further increased the evidentiary significance of digital records across virtually every branch of law.

Nevertheless, the evidentiary value of digital evidence is not absolute. Courts remain cautious because electronic records may be manipulated, fabricated, or altered using sophisticated technological tools. The emergence of artificial intelligence and deepfake technology has further complicated the assessment of authenticity by enabling the creation of highly realistic but fabricated images, videos, and audio recordings. Consequently, courts increasingly rely upon digital forensic examination, metadata analysis, cryptographic verification, expert testimony, and statutory safeguards to determine whether an electronic record can be regarded as trustworthy.

Despite these challenges, digital evidence has become one of the most persuasive forms of proof in contemporary legal systems. Its ability to provide objective, scientifically verifiable, and time-sensitive information has fundamentally transformed the administration of justice. As technological innovation continues to reshape society, the evidentiary importance of electronic records is expected to increase further, making digital evidence an indispensable component of modern judicial decision-making.

LEGAL FRAMEWORK GOVERNING DIGITAL EVIDENCE IN INDIA

In India, the legal recognition of digital evidence evolved gradually through legislative reforms and judicial interpretation. Before the enactment of the Information Technology Act, 2000, Indian evidence law was primarily designed for paper-based documents and physical evidence. The Indian Evidence Act, 1872 did not contain any provisions specifically addressing electronic records because digital technology was virtually nonexistent at the time of its enactment. Consequently, courts frequently encountered difficulties while determining the admissibility and evidentiary value of electronic information.

The rapid expansion of e-commerce, electronic governance, internet communication, online banking, and digital documentation made legislative intervention inevitable. Responding to these technological developments, Parliament enacted the Information Technology Act, 2000, granting legal recognition to electronic records and digital signatures while simultaneously amending the Indian Evidence Act, 1872 to incorporate provisions governing electronic evidence. More recently, the Bharatiya Sakshya Adhiniyam, 2023 (BSA) has modernized India's law of evidence by expressly recognizing electronic and digital records as primary evidence in appropriate circumstances. These legislative developments demonstrate India's commitment to adapting its legal system to the realities of the digital age.

A. Constitutional Foundation for Digital Evidence

Although the Constitution of India does not specifically mention digital evidence, several constitutional provisions significantly influence its collection, preservation, and admissibility.

Article 21 – Right to Life and Personal Liberty

Article 21 guarantees that no person shall be deprived of life or personal liberty except according to the procedure established by law. Over the years, judicial interpretation has expanded Article 21 to include the right to privacy, fair investigation, and fair trial. Since digital evidence often consists of personal communications, financial records, location history, biometric information, and private data, any collection of electronic evidence must comply with constitutional guarantees of fairness and legality.

The landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*⁸ recognized privacy as a fundamental right under Article 21. The Supreme Court held that informational privacy forms an integral component of personal liberty. Consequently, investigative agencies cannot arbitrarily seize digital devices, intercept electronic communications, or access personal data without following lawful procedures.

Thus, while digital evidence is essential for criminal investigation and prosecution, its collection must satisfy the constitutional principles of legality, necessity, proportionality, and procedural fairness.

B. Information Technology Act, 2000

The Information Technology Act, 2000 is India's first comprehensive legislation dealing with electronic records, electronic governance, cyber offences, and digital signatures. It was enacted to facilitate electronic commerce, provide legal recognition to electronic transactions, promote e-governance, and regulate cybercrime.

One of the most significant contributions of the Information Technology Act is that it formally recognized electronic records as legally valid documents. Prior to its enactment, transactions conducted electronically lacked statutory recognition, creating uncertainty regarding their enforceability.

Section 4 – Legal Recognition of Electronic Records

Section 4 provides that where any law requires information to be in writing or printed form, such requirement shall be deemed satisfied if the information is made available in an electronic form that is accessible for future reference.

This provision grants electronic records the same legal status as conventional paper documents, thereby facilitating electronic governance, online banking, digital contracts, and electronic commerce.

Section 5 – Legal Recognition of Digital Signatures

Section 5 provides legal recognition to digital signatures, enabling individuals and organizations to authenticate electronic documents securely. Digital signatures ensure authenticity, integrity, and non-repudiation of electronic communications.

Unlike handwritten signatures, digital signatures rely upon cryptographic technology and public key infrastructure, making them considerably more secure and resistant to forgery.

⁸ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

Section 79A – Examiner of Electronic Evidence

Recognizing the technical complexity of digital evidence, Section 79A empowers the Central Government to notify agencies as Examiners of Electronic Evidence. These expert agencies provide forensic analysis, verify authenticity, and assist courts in interpreting complex electronic records.

C. Indian Evidence Act, 1872

Although enacted more than a century before the digital revolution, the Indian Evidence Act continues to form the foundation of evidence law in India. Following amendments introduced by the Information Technology Act, electronic records were incorporated into the statutory framework.

Section 3 – Definition of Evidence

The definition of "document" was expanded to include electronic records, thereby recognizing digital information as documentary evidence. This amendment represented a fundamental shift in Indian evidence law by acknowledging that legally relevant information may exist in electronic rather than physical form.

Sections 65A and 65B: The Cornerstone of Electronic Evidence

Perhaps the most significant provisions governing digital evidence are Sections 65A and 65B of the Indian Evidence Act. These provisions establish a special procedure for proving electronic records.

Section 65A provides that the contents of electronic records may be proved only in accordance with Section 65B.

Unlike ordinary documentary evidence, electronic records require compliance with a separate statutory framework because of their unique characteristics. The provisions reflect legislative recognition that digital evidence presents distinct evidentiary challenges requiring specialized treatment.

Section 65B constitutes the heart of India's law relating to electronic evidence.

It provides that electronic records stored, copied, or produced from computers are admissible in evidence provided specified statutory conditions are satisfied. For admissibility, the following conditions must generally be fulfilled:

- The computer must have been regularly used.
- Information should have been fed into the computer during ordinary activities.
- The computer must have been functioning properly.
- The electronic record must accurately reproduce the original information.
- A certificate under Section 65B (4) must accompany the electronic record.

The purpose of these requirements is to ensure authenticity and prevent fabricated or manipulated electronic evidence from influencing judicial proceedings.

D. Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam, 2023 represents the most significant reform of Indian Evidence law since 1872.

Recognizing the digital transformation of society, the new legislation gives greater prominence to electronic and digital evidence. Unlike the earlier legislation, the Bharatiya Sakshya Adhiniyam explicitly recognizes: electronic records, digital records, emails, server logs, SMS, websites, cloud data, electronic messages, location data, and digitally stored information.

The legislation also modernizes evidentiary terminology to reflect contemporary technological developments. One of the most important developments under the Bharatiya Sakshya Adhiniyam is the explicit recognition that electronic records may constitute primary evidence, subject to statutory safeguards. This reflects Parliament's recognition that modern information frequently exists only in electronic form rather than paper documents.

ADMISSIBILITY OF DIGITAL EVIDENCE IN COURTS

The increasing use of electronic devices in everyday life has transformed the nature of evidence presented before courts. Emails, WhatsApp messages, CCTV footage, call records, social media posts, GPS data, electronic contracts, and cloud-stored documents have become important sources of proof in both civil and criminal cases. However, unlike traditional documentary evidence, digital evidence is highly vulnerable to alteration, deletion, and fabrication. Therefore, courts require strict legal safeguards to ensure that electronic records are genuine, reliable, and have not been tampered with. The admissibility of digital evidence in India is governed primarily by the Information Technology Act, 2000, the Indian Evidence Act, 1872 (now replaced by the Bharatiya Sakshya Adhiniyam, 2023), and various landmark judicial decisions of the Supreme Court.

Admissibility refers to the legal acceptance of evidence by a court. Digital evidence is admissible only when it satisfies certain legal requirements relating to relevance, authenticity, integrity, and reliability. The electronic record must be directly connected with the facts in issue and should accurately represent the original information. Courts also examine whether the evidence has been collected lawfully and preserved without any unauthorized alteration.

A crucial aspect of admissibility is authentication, which establishes that the electronic record is genuine. Authentication may be carried out through digital signatures, metadata, forensic examination, expert testimony, or system-generated information such as timestamps and server logs. These methods help the court determine whether the electronic record has remained unchanged from the time it was created until its production before the court.

The chain of custody is another essential safeguard. It refers to the complete documentation of every stage through which the electronic evidence passes, from its seizure and storage to forensic examination and presentation before the court. Maintaining an unbroken chain of custody ensures that the evidence has not been tampered with and enhances its credibility during trial.

The admissibility of electronic records was specifically addressed through Sections 65A and 65B of the Indian Evidence Act, 1872. Section 65A provided that electronic records must be

proved in accordance with Section 65B, while Section 65B laid down the conditions under which electronic records could be admitted as evidence. One of its most important requirements was the production of a Section 65B Certificate, certifying that the electronic record was produced from a properly functioning computer and had not been altered. The Bharatiya Sakshya Adhiniyam, 2023 has continued the recognition of electronic records while modernizing the law to accommodate contemporary technological developments and digital forms of evidence.

AUTHENTICATION OF DIGITAL EVIDENCE

Authentication is the process of establishing that digital evidence is genuine, accurate, and has not been altered or tampered with since its creation. Unlike traditional documents, electronic records can be easily modified, copied, or manipulated using advanced technological tools. Therefore, before relying on digital evidence, courts must be satisfied that it is authentic and reliable. Authentication may be established through various methods, including digital signatures, metadata analysis, hash values, forensic examination, server logs, timestamps, and expert testimony. Digital forensic experts play a crucial role in verifying the integrity of electronic records by examining the source device, recovering deleted data, and ensuring that the evidence has remained unchanged throughout the investigation. The maintenance of a proper chain of custody also strengthens the authenticity of digital evidence by documenting every stage of its collection, preservation, examination, and presentation before the court. In India, the provisions relating to electronic records under the Bharatiya Sakshya Adhiniyam, 2023, together with judicial decisions such as *Anvar P.V. v. P.K. Basheer*⁹ and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*¹⁰, emphasize that only properly authenticated electronic records should be admitted as evidence. Therefore, authentication serves as a fundamental safeguard against fabricated or manipulated digital evidence and plays a vital role in ensuring the fairness and credibility of judicial proceedings.

LANDMARK JUDICIAL DECISIONS

The Supreme Court of India has played a vital role in interpreting the law relating to electronic evidence. One of the earliest decisions was *State (NCT of Delhi) v. Navjot Sandhu*¹¹, popularly known as the Parliament Attack Case. The Court held that electronic evidence could, in certain circumstances, be admitted even without strict compliance with Section 65B. Although this approach made the admission of electronic evidence easier, it created uncertainty regarding the statutory procedure.

The legal position changed significantly in *Anvar P.V. v. P.K. Basheer*¹². In this landmark judgment, the Supreme Court overruled the view taken in *Navjot Sandhu* and held that compliance with Section 65B is mandatory for the admissibility of secondary electronic

⁹ (2014) 10 S.C.C. 473 (India).

¹⁰ (2020) 7 S.C.C. 1 (India).

¹¹ *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 S.C.C. 600 (India).

¹² *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).

evidence. The Court clarified that electronic records constitute a special category of evidence and must be proved strictly in accordance with the procedure prescribed by law. This decision strengthened the authenticity and reliability of digital evidence by ensuring that electronic records were supported by the necessary statutory safeguards.

Subsequently, in *Shafhi Mohammad v. State of Himachal Pradesh*¹³, the Supreme Court adopted a more flexible approach and observed that a Section 65B certificate may not be required where obtaining such a certificate was impossible. However, this judgment led to conflicting interpretations and uncertainty in the law.

The issue was finally settled in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*¹⁴, where a three-judge Bench of the Supreme Court reaffirmed the decision in *Anvar P.V.* The Court held that a Section 65B certificate is generally mandatory whenever secondary electronic evidence is produced before a court. At the same time, it recognized that where a party genuinely cannot obtain the certificate despite reasonable efforts, the court may exercise its powers to direct the concerned authority to produce it. This judgment presently represents the authoritative legal position regarding electronic evidence in India.

Another significant decision is *Tomaso Bruno v. State of Uttar Pradesh*¹⁵, in which the Supreme Court emphasized the importance of scientific investigation and electronic evidence. The Court observed that modern criminal investigations should rely increasingly on objective evidence such as CCTV footage, digital recordings, and forensic analysis rather than depending solely upon oral testimony. The judgment encouraged investigating agencies to make greater use of technological evidence in criminal proceedings.

CHALLENGES OF DIGITAL EVIDENCE

Despite its growing significance in the administration of justice, digital evidence presents several legal and practical challenges. Electronic records are highly vulnerable to alteration, deletion, and unauthorized manipulation, making it difficult to establish their authenticity and integrity. The rapid advancement of technologies such as artificial intelligence and deepfake software has further increased the risk of fabricated audio, video, and image evidence. Investigating agencies also face difficulties in collecting data from encrypted devices, cloud storage, and foreign digital platforms due to jurisdictional and technical limitations. In addition, inadequate digital forensic infrastructure, shortage of trained experts, delays in forensic examination, and the complexity of obtaining statutory certifications often affect the effective use of electronic evidence. Concerns relating to privacy, data protection, and cybersecurity also require courts to strike a careful balance between protecting individual rights and ensuring effective investigation. Therefore, continuous legal reforms, technological advancements, and specialized training for investigators, lawyers, and judges are essential to address these challenges and strengthen the reliability of digital evidence in judicial proceedings.

CONCLUSION

¹³ *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 S.C.C. 801 (India).

¹⁴ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1 (India).

¹⁵ *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 S.C.C. 178 (India).

Digital evidence has become an indispensable component of the modern justice system due to the rapid digitization of society. Its ability to provide objective, accurate, and scientifically verifiable information has significantly improved the process of fact-finding in judicial proceedings. At the same time, its vulnerability to manipulation necessitates strict legal safeguards concerning authentication, preservation, and admissibility. Through legislative reforms and landmark judicial decisions, India has developed a comprehensive legal framework that seeks to balance technological advancement with procedural fairness. As emerging technologies such as artificial intelligence, blockchain, cloud computing, and deepfake technology continue to evolve, the law governing digital evidence must also adapt to ensure that courts remain capable of delivering fair, reliable, and effective justice in the digital age.

