ILE JOURNAL OF EVIDENCE AND JURISPRUDENCE

VOLUME 3 AND ISSUE I OF 2024

APIS – 3920 – 0049 | ISBN - 978-81-964391-3-2

Published by

Institute of Legal Education

https://iledu.in

ANALYSIS AND ADMISSIBILITY OF DIGITAL EVIDENCE IN INDIA

AUTHORS - MOHAMED THARIC ILAHI* & DR. GURMINDER KAUR**

* (B.A., LL.B., LL.M), GRADUATE (CRIMINAL JUSTICE & HUMAN RIGHTS), AT SCHOOL OF LAW, PONDICHERRY UNIVERSITY.

** ASSISTANT PROFESSOR, SCHOOL OF LAW, PONDICHERRY UNIVERSITY.

BEST CITATION - MOHAMED THARIC ILAHI & DR. GURMINDER KAUR, ANALYSIS AND ADMISSIBILITY OF DIGITAL EVIDENCE IN INDIA, *ILE JOURNAL OF EVIDENCE AND JURISPRUDENCE (ILE JEVJ),* 3 (1) OF 2025, PG. 1-9, APIS – 3920 – 0049 | ISBN - 978-81-964391-3-2.

ABSTRACTS

The amendments to the Information Technology Act and the Evidence Act have had a profound impact on India's legal framework regarding electronic evidence, highlighting the importance of digital records. These changes have revolutionised legal proceedings, particularly with the expanded definition of "electronic record" under the Evidence Act to encompass digital evidence. This comprehensive framework encompasses a wide array of electronic evidence crucial for contemporary investigations, including emails, documents, and social media posts. Admissibility in court relies on stringent criteria, including relevance, authenticity, integrity, and compliance with Section 65 B's procedural norms. Section 65B(4) mandates an authentication certificate to ensure the accuracy of electronic records, safeguarding against manipulation or tampering. This abstract underscores the vital role electronic evidence plays in modern jurisprudence, encapsulating the intricate legal system that governs its use.

KEYWORDS: Evidence Act, Documents, Electronic Records

INTRODUCTION

Traditionally, electronically stored evidence has been regarded with suspicion and often classified as hearsay within the legal system. This was primarily because, in earlier times, no scientific or standardized methods were available to verify the authenticity or reliability of data stored in digital or electronic form. However, with the rapid advancements in information technology and the increasing dependence on electronic modes of communication, e-commerce, and digital information storage, the need for a robust legal framework governing information technology has become imperative. This includes clear rules on the relevance, admissibility, and evidentiary value of electronic records in both civil and criminal proceedings in India. Unlike conventional forms of evidence, electronic evidence requires specialized procedures for collection, preservation, and examination, as well as technical expertise in the domain of cyberspace. The process of investigating and evaluating data retrieved from electronic media for judicial purposes is therefore critical to ensuring the reliability of such evidence in courts of law.

This article seeks to analyze and evaluate the admissibility of electronic evidence within the Indian legal system by examining prevailing legal standards, judicial pronouncements, and the legislative intent behind relevant statutory provisions.

ILE JOURNAL OF EVIDENCE AND JURISPRUDENCE
VOLUME 3 AND ISSUE I OF 2024
APIS – 3920 – 0049 | ISBN - 978-81-964391-3-2
Published by
Institute of Legal Education
https://iledu.in

LEGAL FRAMEWORK

In India, the legal recognition of electronic evidence was formally established with the enactment of the Information Technology Act, 2000 which brought significant changes to the existing evidentiary framework under the Indian Evidence Act, 1872. Prior to these legislative developments, Indian courts were primarily reliant on traditional forms of evidence such as oral testimony, documentary evidence, and material objects. The exponential growth of information technology, electronic communication, and digital storage systems necessitated a legal mechanism to recognize, regulate, and admit electronic records as valid evidence in judicial proceedings.

The IT Act, 2000 amended various statutes, including the Indian Penal Code, the Bankers' Books Evidence Act, and most importantly, the Indian Evidence Act, 1872, to incorporate the concept of 'electronic records' and their evidentiary value. Section 2(1)(t) of the IT Act defines the term 'electronic record' to include 'data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer-generated microfiche.' This wide and inclusive definition ensures that almost every form of information processed or communicated through electronic means is covered within the ambit of 'electronic record.'

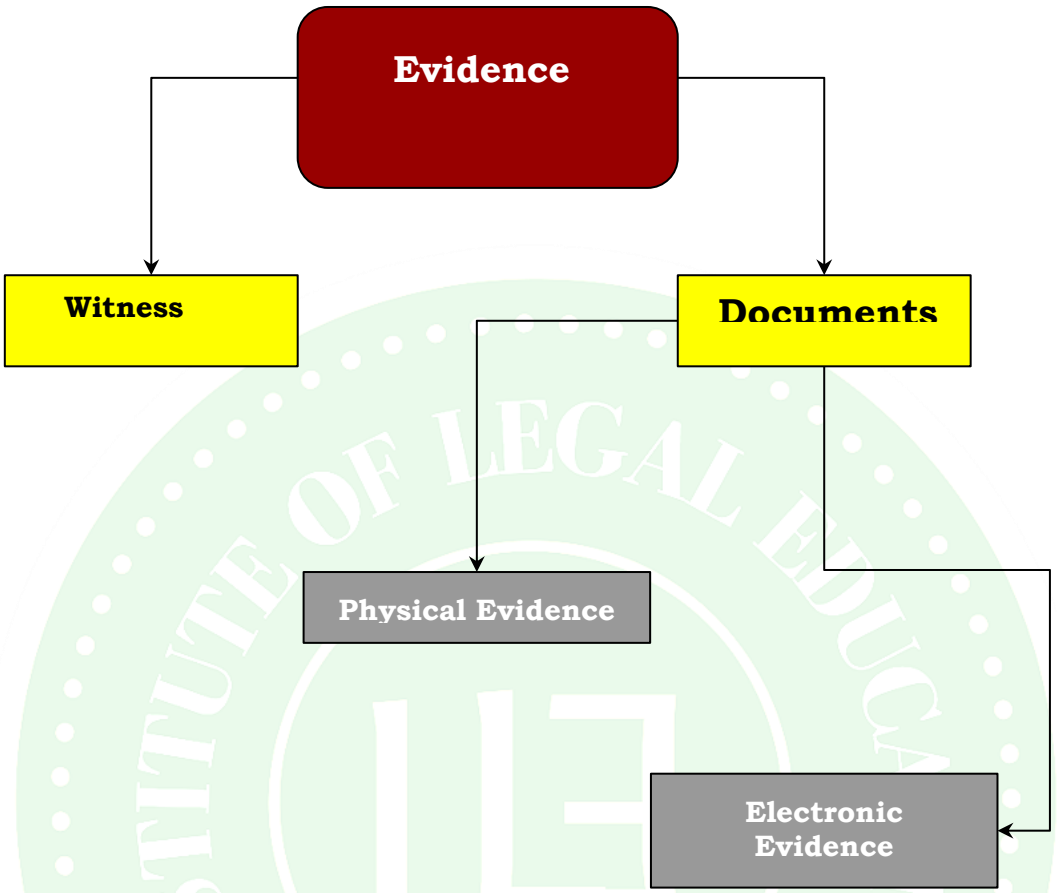
Further, Section 3 of the Indian Evidence Act, which defines 'evidence,' was amended to include electronic records alongside documents, thereby granting them legal recognition as admissible evidence. Subsequently, Section 65B of the Evidence Act was introduced, laying down the specific conditions under which electronic records may be admitted as evidence in a court of law. This provision acts as a safeguard to ensure the authenticity, reliability, and integrity of electronic data, given its susceptibility to manipulation, tampering, and unauthorized alteration.

Thus, the introduction of electronic evidence into the Indian legal system marked a significant step towards modernization and adaptation to technological developments. It not only provided a statutory framework for recognizing electronic records but also created a structured mechanism for ensuring their admissibility, thereby balancing the requirements of justice with the realities of the digital age[1], The IT Act acknowledges the value of using electronic records in place of traditional paper-based records and their legitimacy.[2]

- The evidence of witness i.e. oral evidence,
- Documentary evidence which includes electronic records produced for the inspection of the court.[3]

[1] *The Information Technology Act, 2000 (Act. No: 21 of 2000) S.2(1)(t)*
[2] *The Information Technology Act, 2000 (Act. No: 21 of 2000) S.4*
[3] *Dholam, Swarupa. (2017). Electronic evidence and its challenges Electronic evidence and its challenges.*

ILE JOURNAL OF EVIDENCE AND JURISPRUDENCE
VOLUME 3 AND ISSUE I OF 2024
APIS – 3920 – 0049 | ISBN - 978-81-964391-3-2
Published by
Institute of Legal Education
https://iledu.in



The Indian Evidence Act specifies the requirement and conditions of the Electronic Evidence. The Evidence Act was amended as a result of Section 92[4] The term "evidence" was amended to include "electronic record", thus allowing for the adoption of digital evidence. Prior to the legal recognition provided by electronic evidence, sections 63 and 65[5] were very active and provided the conditions for the admissibility of electronic evidence. As with these provisions, electronic evidence collected in various ways using cyber forensics was regarded as a "document" and printed products were considered as second proof, requiring professional confirmation from a competent signer who could not be questioned on the verified document.

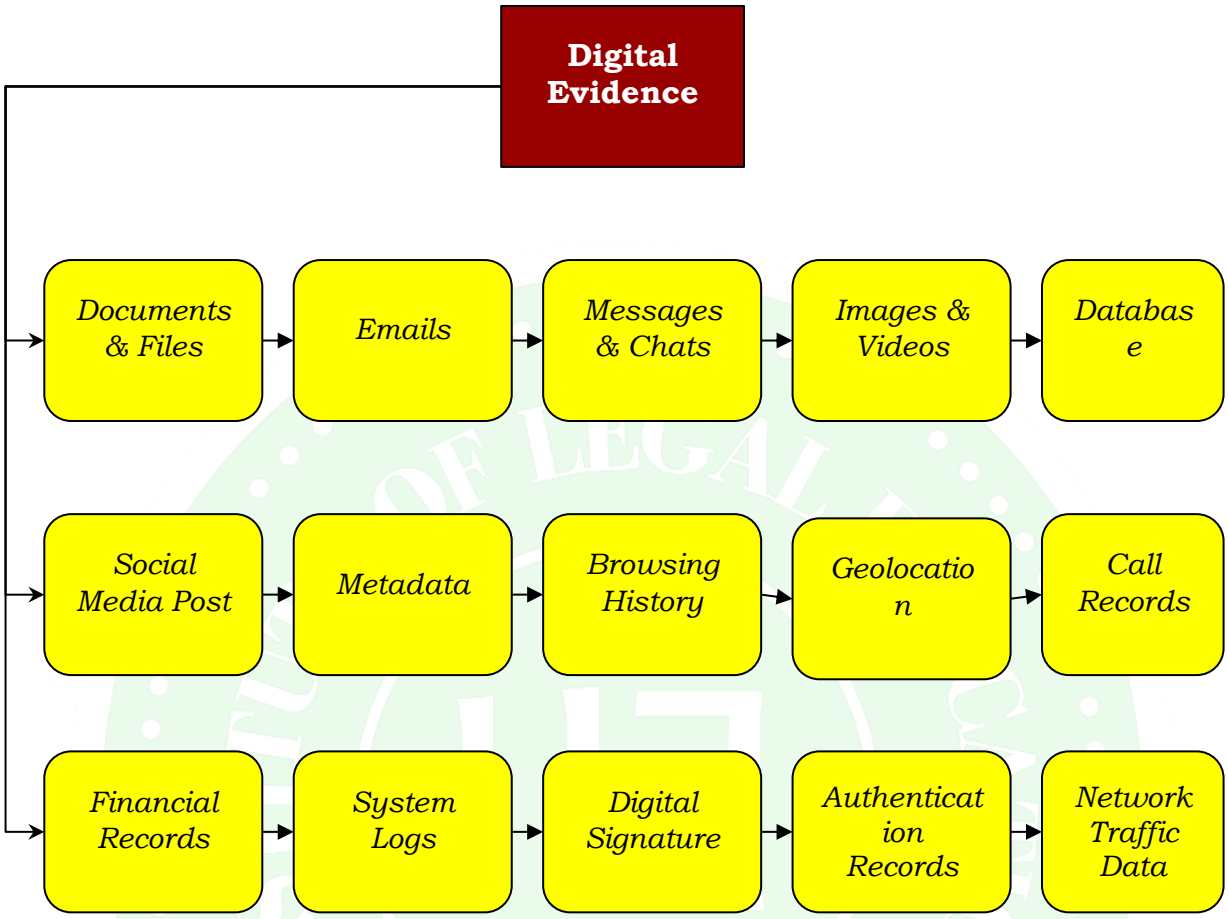
Special provisions as to evidence relating to electronic record. –– The contents of electronic records may be proved in accordance with the provisions of section 65B[6]

TYPES OF ELECTRONIC EVIDENCE

Digital evidence has been defined by the council of Europe as "any evidence obtained from data contained in or created by any device, the operation of which depends on software or data stored or transmitted through a computer system or network"[7] This definition provides much clarity as it not only includes digitally born evidence but recognises data which during its life is transformed and then stored or exchanged in electronic form as digital evidence as well.

[4] *The Information Technology Act, 2000 (Act. No: 21 of 2000)*
[5] *The Indian Evidence Act, 1872 (Act. No: 1 of 1872)*
[6] *The Indian Evidence Act, 1872 (Act. No: 1 of 1872) S. 65 A*
[7] *Council of Europe (2019) Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings < https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0c> (Last accessed Jan. 10, 2022)*

ILE JOURNAL OF EVIDENCE AND JURISPRUDENCE
VOLUME 3 AND ISSUE I OF 2024
APIS – 3920 – 0049 | ISBN - 978-81-964391-3-2
Published by
Institute of Legal Education
https://iledu.in



Documents and Files: These include text documents, spreadsheets, presentations, PDFs, and other electronic files that are relevant to the case.

Emails: Emails and their attachments can provide valuable information about communications and interactions between individuals.

Instant Messages and Chats: Conversations that occur on platforms like messaging apps, social media, and chat applications can be important in understanding relationships and context.

Images and Videos: Multimedia files can capture events, actions, or situations that are pertinent to an investigation or legal matter.

Databases: Data stored in databases can reveal patterns, transactions, and relationships that might be relevant to a case.

Social Media Posts: Posts, comments, likes, and shares on social media platforms can provide insights into an individual's thoughts, activities, and connections.

Metadata: Metadata contains information about other data. For example, the metadata of a photo might include the date and time it was taken, the location, and the device used.

Internet Browsing History: Information about websites visited, searches conducted, and online activities can provide context or a timeline of events.[8]

Geolocation Data: Location-based information from devices, apps, or

[8] *Kessler, Gary C., 'Computer Evidence: Collection and Preservation." [1992] Computers & Security [11, 4], 357-363.*

ILE JOURNAL OF EVIDENCE AND JURISPRUDENCE
VOLUME 3 AND ISSUE I OF 2024
APIS – 3920 – 0049 | ISBN - 978-81-964391-3-2
Published by
Institute of Legal Education
https://iledu.in

services can help establish a person's whereabouts at a certain time.

Call Records: Records of phone calls, including call logs and text messages, can be relevant in investigations involving communication patterns.

Financial Records: Digital records of financial transactions, bank statements, and payment histories can provide insights into a person's financial activities.

System Logs: Logs from operating systems, applications, and network devices can reveal actions taken on a device or network[9]

Computer Memory: Information stored in RAM or other forms of computer memory can provide real-time insights into a device's state and activities.

Deleted or Altered Files: Recovery of deleted or altered files can sometimes uncover evidence that was intentionally hidden.

Encryption and Decryption Records: Information about encrypted files, encryption keys, and attempts to decrypt data can be significant in cases involving cyber security.[10]

Digital Signatures: Digital signatures can be used to verify the authenticity and integrity of electronic documents.

Authentication Records: Records of user logins, access attempts, and account activities can help establish who accessed a system or service.

Network Traffic Data: Information about network connections, data transfers, and communication patterns can provide insights into cyber incidents[11]

ADMISSIBILITY

The admissibility of digital evidence in a court of law is contingent upon several critical factors, including its relevance to the case, the authenticity of its source, the integrity of the data, and the overall reliability of the evidence presented. Courts must be satisfied that the digital evidence directly relates to the issues in dispute and that it has not been altered, tampered with, or fabricated at any stage of its creation, storage, or transmission. To establish authenticity, parties are often required to demonstrate that the evidence originates from a credible source and that it accurately represents the information it purports to convey. Similarly, the principle of integrity demands that the data remain intact and uncorrupted, ensuring that it has not been modified in a way that could mislead or distort the truth. Reliability, in turn, emphasizes the trustworthiness of the methods used to collect, preserve, and present such evidence.

To safeguard these principles, courts across different jurisdictions adhere to specific statutory provisions, procedural rules, and evidentiary guidelines while determining the admissibility of digital evidence. Although the precise rules may vary depending on the jurisdiction and the governing legal system, certain common principles such as relevance, authenticity, integrity, and reliability are universally recognized as essential to ensuring the fair use of digital evidence in legal proceedings

Relevance: The digital evidence must be relevant to the case at hand. It should have a direct connection to the issues being discussed in the legal proceeding[12]

[9] *Rothstein, Samuel J., 'Digital Evidence and the New Criminal Procedure." Notre Dame Law Review' [2019] Notre Dame Law Review [94, 3], 1209-1270.*
[10] *Zeleznikow, John, 'Admissibility of electronically generated evidence: A dispute resolution perspective' [2019] Information & Communications Technology Law [28, 1], 51-66.*
[11] *Schwartz, J., & Ball, D., 'The admissibility of digital evidence in criminal prosecutions: A new approach' [2017] Virginia Journal of Law and Technology [21, 2], 1-52*
[12] *Zelechoski, Amanda, 'The Admissibility of Digital Evidence in Criminal Prosecutions' [2019] American Criminal Law Review [56, 3], 567-612.*

ILE JOURNAL OF EVIDENCE AND JURISPRUDENCE
VOLUME 3 AND ISSUE I OF 2024
APIS – 3920 – 0049 | ISBN - 978-81-964391-3-2
Published by
Institute of Legal Education
https://iledu.in

Authenticity: The party offering the digital evidence must establish its authenticity, proving that the evidence is what it claims to be. This can involve showing the origin of the evidence and how it was collected. Evidence must be collected in a way that does not allow alteration of crucial data. To prevent contamination[13]

Integrity: The digital evidence should be preserved and presented in a way that maintains its integrity and prevents tampering or alteration.

Hearsay: Hearsay refers to statements made outside of court that are offered as evidence to prove the truth of the matter. Digital evidence that contains hearsay might not be admissible unless it falls under an exception to the hearsay rule.[14]

Best Evidence Rule: The best evidence rule generally requires that the original or the most reliable form of evidence be presented. In the case of digital evidence, this might involve presenting the original file rather than a printout or a copy.

Expert Testimony: In cases where the digital evidence is complex or technical, expert witnesses might be called to testify about the authenticity, reliability, and interpretation of the evidence.

Chain of Custody: The chain of custody is the documented record of the individuals who had control of the evidence from the time it was collected to when it is presented in court. A proper chain of custody helps establish the integrity of the evidence[15]

Legal Requirements: Some jurisdictions might have specific legal requirements for the admissibility of digital evidence, such as electronic signatures, timestamps, and encryption standards.

Technology Reliability: Courts often consider the reliability of the technology and methods used to collect, store, and present digital evidence. Established and widely accepted technologies are more likely to be deemed reliable.

Authentication: Authenticating digital evidence might involve showing that it was generated by a specific device, software, or user. This can be done through metadata, digital signatures, or other forms of verification.

Privacy and Data Protection Laws: Digital evidence collection must also comply with privacy and data protection laws. Evidence obtained illegally or in violation of these laws might not be admissible.[16]

Fairness and Due Process: Courts consider whether the admission of digital evidence would violate a defendant's right to a fair trial or due process.

Moreover, the admissibility of digital evidence is a complex area of law, and legal professionals often work closely with experts in digital forensics and technology to ensure that evidence is properly collected, preserved, and presented in court. The rules and standards can vary widely, so it's essential to consult the relevant laws and legal professionals in the jurisdiction where the case is being heard[17]

ACCEPTANCE OF ELECTRONIC RECORDS

Section 65A of the Indian Evidence Act lays down that the contents of electronic records

[13] *IvyPanda. (2018, November 28). Computer Forensics and Other Information Technologies. Principles of Computer Forensics. https://ivypanda.com/essays/computer-forensics-and-other-information-technologiesprinciples -of-computer-forensics/*
[14] *Kohn, Alisha, 'The Emerging Admissibility of Snapchat Evidence' [2016] The John Marshall Journal of Information Technology & Privacy Law [32, 1], 153-171*
[15] *Casey, Mary, 'Digital Evidence and the US Federal Rules of Evidence' [2005] Digital Investigation [2, 4], 281-287.*
[16] *Rasinger, & Sebastian M., 'Digital evidence in court: A cross-national comparison of judicial perspectives' [2019] Digital Investigation [30], 48-S56.*
[17] *Oke, Gbenga, and Akinkunmi Akintunde, 'Admissibility of electronically generated evidence in Nigeria: An overview' [2019] Computer Law & Security Review [35, 6], 719-729*

ILE JOURNAL OF EVIDENCE AND JURISPRUDENCE
VOLUME 3 AND ISSUE I OF 2024
APIS – 3920 – 0049 | ISBN - 978-81-964391-3-2
Published by
Institute of Legal Education
https://iledu.in

may be proved only in accordance with the special provisions contained in Section 65B of the Act. This provision makes it clear that a written or printed record derived from an electronic source cannot be proved in the traditional manner but must strictly follow the procedure prescribed under Section 65B.

Section 65B provides the statutory framework for the admissibility of electronic evidence. It states that notwithstanding anything contained elsewhere in the Evidence Act, any information contained in an electronic record—whether it is in the form of a document, a file stored on a computer, or a copy made from optical or magnetic media—shall be treated as a 'document' and may be admitted in evidence, provided that the conditions mentioned in subsections (2) to (5) are duly satisfied. In other words, once these requirements are met, electronic records can be accepted as evidence without the need to produce the original device or medium from which the record was generated.

The section further provides for both technical and procedural safeguards to ensure the reliability of electronic evidence. Subsection (2) enumerates the specific technical conditions under which a duplicate or secondary copy of an electronic record—including printed copies, computer outputs, or copies made from CDs, DVDs, or other digital storage devices—may be considered valid evidence. These conditions focus on the regular and lawful use of the computer, proper functioning of the device during the relevant period, and the accuracy of the data reproduced. Thus, Sections 65A and 65B collectively carve out a self-contained code within the Evidence Act for proving electronic records, emphasizing both authenticity and reliability while balancing the need for practicality in admitting electronic evidence in courts of law

These are:

a) At the time of the electronic record, the computer that produced it must have been used regularly.

b) The type of information contained in the electronic record must be regularly entered and usually entered into a computer;

c) The computer was working properly; and

d) A duplicate copy must be a reproduction of the original electronic record.

As can be proven the above scenarios are related to the authenticity of the data. Circumstances have a double impact as they.

i) ensure that there is no unauthorised use of data; and

ii) the device was efficient, ensuring the accuracy and reliability of the extracted data.

Subsection (3) of Section 65B of the Evidence Act defines and ensures that if a user has used a networked device to store or process data, all connected devices will be regarded as a single device[18].

AUTHENTICATION CERTIFICATE

Section 65B of the Indian Evidence Act, 1872, inserted through the Information Technology Act, 2000, specifically governs the admissibility of electronic records as evidence. Sub-section (4) of Section 65B lays down the requirements relating to certification, which are procedural rather than technical in nature. This certificate serves a vital role in fulfilling the conditions prescribed under Section 65B(2), which deal with the prerequisites for admitting an electronic record in evidence.

According to Section 65B(4), the certificate must be issued and signed by a person who is in lawful control of the computer, device, or system from which the electronic record is generated. This individual must either be directly responsible for the operation of the

[18] *Mr. Dhanjay Singh Pundir, "CRITICAL ANALYSIS OF ADMISSIBILITY OF DIGITAL EVIDENCE" Volume 8, Journal of Emerging Technologies and Innovative Research, December 2021*

ILE JOURNAL OF EVIDENCE AND JURISPRUDENCE
VOLUME 3 AND ISSUE I OF 2024
APIS – 3920 – 0049 | ISBN - 978-81-964391-3-2
Published by
Institute of Legal Education
https://iledu.in

device or otherwise have lawful authority over the use of such equipment. The certificate must specifically:

1. Identify the electronic record in question.
2. Describe the manner in which the record was produced, including the process of generation, retrieval, or copying.
3. Provide particulars of the device involved in the production of the electronic record.
4. Address all matters fulfilling the conditions under Section 65B(2), thereby ensuring that the record is produced in the ordinary course of computer usage, without manipulation, and during a period when the computer was operating properly.

The primary object of the certificate is to ensure the authenticity and reliability of the electronic record. Given that electronic data is highly susceptible to alteration, tampering, or manipulation, the certification requirement provides a safeguard by establishing both the credibility of the source and the integrity of the record. Courts rely on this certification to develop confidence in the veracity of the information, as it assures that the data has been produced in accordance with lawful and regular usage of the device.

ANALYSIS & LEGAL PRESIDENTES

Digital evidence admissibility in court is a complicated and developing legal topic. Courts worldwide have been confronted with a range of concerns pertaining to the legitimacy, dependability, and consistency of digital evidence.

In the case of ***Anvar P.V. v. P.K. Basheer & Others***[19] The Supreme Court of India emphasised the importance of adhering to the rules of evidence while admitting electronic records, including secondary evidence of electronic records. The court stated that the person who seeks to rely on electronic records must prove its authenticity in the same way as any other document. ***State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru***[20] This case laid down the criteria for admissibility of electronic records under the Indian Evidence Act, 1872. The court held that the electronic evidence must be relevant, authentic, and properly identified.

Shamsher Singh Verma v. State of Haryana [21]: The Supreme Court held that digital evidence like electronic records, including CDs, DVDs, and pen drives, is admissible if it is proved in accordance with the provisions of the Indian Evidence Act. ***Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*** [22]: The Supreme Court clarified the requirements for admissibility of electronic evidence under Section 65B of the Indian Evidence Act. The court held that the certificate required under Section 65B(4) must accompany the electronic record when it is produced in evidence, and non-compliance with this requirement renders the electronic evidence inadmissible.

CONCLUSION

In conclusion, the legal framework surrounding electronic evidence in India, established through the Information Technology Act of 2000 and subsequent amendments to the Evidence Act of 1872, recognizes the importance and legitimacy of digital records. The acceptance and admissibility of electronic evidence are governed by stringent criteria, including relevance, authenticity, integrity, and compliance with technical and non-technical standards outlined in Section 65B of the Evidence Act. Recent legal precedents, such as the landmark cases of Anvar P.V. v. P.K. Basheer, State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru, Shamsher Singh Verma v. State of Haryana, and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, have provided clarity on the requirements for admitting electronic evidence in court. These rulings underscore the

[19] *(2014 10 SCC 473)*

[20] *Appeal (crl.) 373-375 of 2004 SC.*
[21] *2016 (15) SCC 485*
[22] *Admissibility of electronic evidence in India continues to face hurdles, India, Available at: https://www.scconline.com/blog/post/2021/06/07/electronic-evidence-2/ (Last accessed at 20.04.2024)*

ILE JOURNAL OF EVIDENCE AND JURISPRUDENCE
VOLUME 3 AND ISSUE I OF 2024
APIS – 3920 – 0049 | ISBN - 978-81-964391-3-2
Published by
Institute of Legal Education
https://iledu.in

need for meticulous authentication and adherence to legal standards, ensuring fairness and due process in the digital age. As technology evolves, legal professionals must continue to navigate the complexities of digital evidence, collaborating with experts in digital forensics to uphold the integrity of the judicial process.