ADMISSIBILITY OF ELECTRONIC EVIDENCE UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023: A CRITICAL ANALYSIS OF JUDICIAL INTERPRETATION

Md Danish Azad, Mumbai University

ABSTRACT

The admissibility of electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023 (BSA) is critically examined in this research in light of changing judicial interpretation and technical developments. Due to the rapid digitisation of communication, business, and government, electronic documents, including emails, CCTV footage, call logs, and social media posts, are now essential to contemporary legal proceedings. The paper examines how legal precedents influenced the development of electronic evidence law in India, starting with the Indian Evidence Act of 1872 and continuing through the Information Technology Act of 2000 with the addition of Sections 65A and 65B.

The paper evaluates the reforms introduced under Sections 61 and 63 of the BSA, 2023, which recognise electronic records as valid evidence and clarify certification requirements while emphasising authenticity and reliability. The paper further evaluates whether the BSA, 2023, effectively balances technological advancement with constitutional guarantees of fair trial and due process under Article 21 of the Constitution of India.

The study concludes that although the BSA, 2023, marks a significant step towards modernising evidentiary law, its success will ultimately depend on judicial interpretation, technological infrastructure, and continuous legal training, making the reform both promising and cautiously optimistic.

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

INTRODUCTION

The fast technological revolution of the late 20th and early 21st centuries has drastically altered the nature of evidence. Commercial transactions, financial dealings, government communications, and personal encounters are increasingly taking place digitally. Emails, digital signatures, CCTV footage, call data records, GPS logs, WhatsApp chats, and social media posts have all become important forms of evidence in litigation. As a result, courts are regularly asked to establish the validity, dependability, and admissibility of electronic records.

This transition obviously altered the legal system, as crimes involving electronic devices increased in tandem with technological advancements. Every day, thousands of new devices are introduced and used. The widespread use of computers, the impact of information technology on society as a whole, and the ability to store and collect data in digital form have all necessitated the updating of Indian law to include the standards controlling the acceptance of innovative proof.

Acknowledging the inadequacy of the original framework, the legislature amended the Evidence Act 1872, with the Information Technology Act of 2000, which included Sections 65A and 65B. These regulations established a special method for determining the admissibility of electronic records. However, the execution of these regulations resulted in significant legal discussion and interpretive confusion, particularly about the mandatory certification requirement under Section 65B (4)[1].

The Parliament introduced the Bharatiya Sakshya Adhiniyam 2023 (hereinafter BSA, 2023) which is a comprehensive legislative effort to amend India's evidentiary framework as part of a broader restructuring of criminal laws. The new act claims to modernize and simplify evidentiary rules, particularly those relating to digital and electronic evidence. The critical question, however, is whether this revision really changes the legal situation or just reorganises the existing laws. This legislation replaces the colonial-era Indian Evidence Act of 1872, reflecting the advancement of technology and social norms[2].

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 and

[1] The Indian Evidence Act, 1872, § 65B (4), No. 1, Acts of Parliament, 1872 (India).
[2] Free law, https://www.freelaw.in/legalarticles/Bharatiya-Sakshya-Adhiniyam-2023, 26.Feb.2026.

digital records within its definitional structure and restructures the admissibility framework.

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. 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[3].

DEFINITION OF ELECTRONIC EVIDENCE

The legal rules for the admissibility of digital evidence have been laid down in Section 2(e) of the Bhartiya Sakshya Adhiniyam, 2023. As a result, this section claims that there are two types of evidence. Both documentary and oral evidence fall under this category. The statements or information that court witnesses electronically provide to support in fact-finding are considered oral evidence. Such utterances are referred to as oral evidence and are allowed. Documentary evidence, on the other hand, comprises records that are expanded to include digital or electronic records that are brought before the court for review. As a result, the Section encompasses both oral and written electronic evidence.

> *2(e) "evidence" means and includes— (i) all statements including statements given electronically which the Court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry and such statements are called oral evidence; (ii) all documents including electronic or digital records produced for the inspection of the Court and such documents are called documentary evidence.*[4]

In general, the evidence is referred to as proof of documents or any pertinent data. Any information with values that is stored or transmitted electronically is considered electronic

[3] Vivek Dubey, Admissibility of electronic evidence: an Indian perspective. Forensic Res Criminal Int J. 2017;4(2):58- 63

[4] The Bharatiya Sakshya Adhiniyam, 2023, § 2(e), No. 47, Acts of Parliament, 2023 (India).

evidence, according to the explanation to Section 79A[5] of the Information Technology (Amendment) Act. This includes evidence like computer data, digital audio, digital video, cell phones, and digital fax machines. Information that has been stored, communicated, or gathered and utilized as proof in court is referred to as digital evidence. Digital media, such as computers, smartphones, and other electronic devices, are used to store, send, or gather the data. Digital evidence can take many different forms, such as messages, images, videos, and other digital formats. When it comes to digital evidence, handwritten notes and fingerprint testing are not required during an inquiry. Instead of being kept in conventional paper documents, it is always kept in an electronic format.

Electronic evidence was not specifically defined under the Indian Evidence Act, 1872. Nonetheless, "evidence" was defined in Section 3 as "*all statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry*[6]." Electronic evidence was included in this broad definition along with other types of evidence. Courts in India used their own interpretations to decide the admissibility and extent of electronic evidence as there was no clear definition. The Supreme Court of India ruled in the seminal case of **State of Maharashtra v. Dr. Praful B. Desai**[7] that computer-generated records and other electronic evidence may qualify as "documentary evidence" for Section 3 of the IEA.

SCOPE OF ELECTRONIC OR DIGITAL EVIDENCE

The scope of electronic or digital evidence in India is enormous and is growing. Any information that can be produced in a court of law that has been stored, recorded, or communicated digitally is referred to as electronic evidence. The Indian Evidence Act of 1872, as revised by the Information Technology Act of 2000, is the primary source of its legal validity because it clearly defines electronic documents as "evidence."

Digital evidence is frequently used in administrative, commercial, criminal, civil, and constitutional procedures. Electronic evidence is crucial to criminal investigations and prosecutions. Call detail records, CCTV footage, mobile phone data, GPS position tracking, emails, social media posts, and digital transaction records are often used to follow financial

[5] The Information Technology Act, 2000, § 79A, NO. 21, Acts of Parliament, 2000 (India).
[6] The Indian Evidence Act, 1872, § 3, No. 1, Acts Of Parliament, 1872 (India).
[7] State of Maharastra v. Dr. Praful B. Desai, 2003 (4) SCC 601.

trails, prove conspiracy, prove motive, or prove an accused person was at the crime scene. Digital evidence frequently serves as the main source of proof in situations involving cybercrime, terrorism, financial fraud, drugs, and organized crime[8].

In civil and commercial disputes, electronic evidence plays a vital role as most modern transactions are conducted through emails, electronic contracts, online banking systems, and digital signatures. Courts rely on such records to determine offer, acceptance, breach of contract, intellectual property infringement, corporate fraud, and even matrimonial disputes where chats, emails, photographs, or social media posts are produced as proof. Arbitration and commercial litigation increasingly treat electronic records as primary documentary evidence. The scope further extends to expert examination and forensic validation, and under Section 39 (2) of BSA, 2023 (earlier 45A of the Indian Evidence Act, 1872), the opinion of an examiner of electronic evidence is relevant. Techniques such as digital forensics, hash value verification, metadata analysis, and proper maintenance of chain of custody ensure authenticity and reliability, making electronic evidence technical yet highly dependable when properly handled.

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[9].

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

[8] Pruthvi Ramkanta Hegde, All about digital evidence, Ipleaders (26th Feb. 2026, 4:00 PM), https://blog.ipleaders.in/all-about-digital-evidence/
[9] R. K. Bangia, Law of Evidence, 10th Edition, Allahabad: Allahabad Law Agency, 2020.

unique guidelines for the admission of electronic evidence.

The Supreme Court took a lenient stance toward electronic evidence in **State (NCT of Delhi) v. Navjot Sandhu**[10]. It held that electronic records could be allowed even if Section 65B was not strictly followed if their dependability and authenticity could be demonstrated in another way. The Court held that even in the absence of strict compliance with Section 65B of the Evidence Act, electronic records such as call detail records could still be admitted if their authenticity and reliability were otherwise satisfactorily established. This strategy was re-examined when the Supreme Court ruled in **Anvar P.V. v. P.K. Basheer**[11] that electronic records needed to be properly certified in order to be admitted. Despite being intended to preserve integrity, this stringent procedural requirement often resulted to the rejection of digital evidence that would have been essential in establishing a case's facts. Later, the Court made it clear in **Arjun Panditrao Khotkar v. Kailash Kushanrao**[12] Guarantee that authenticity and dependability, not just procedural conformity, determine the evidential weight of electronic records. This ruling marked a step toward acknowledging the substantive significance of electronic evidence.

The Bharatiya Sakshya Adhiniyam builds upon these judicial interpretations by codifying a clearer, more practical framework. The Act recognises the inevitability of digital records in modern society and attempts to streamline the process of their admissibility. Unlike the rigid formalities of Section 65B, the new law prioritises authenticity, reliability, and contextual evaluation over procedural technicalities. This evolution demonstrates legislative acknowledgement that the law must adapt to technological change and to the increasing role of digital evidence in contemporary litigation.

TYPES OF ELECTRONIC OR DIGITAL EVIDENCE[13]

- Data or information in electronic formats is referred to as digital evidence. The variety of digital evidence has increased as a result of the pervasive use of technology in many facets of society. The following are a few categories of digital evidence.

[10] State (N.C.T. Of Delhi) v. Navjot Sandhu@ Afsan Guru, 2005 (11) SCC 600.
[11] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[12] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 2 SCC 650.
[13] Pruthvi Ramkanta Hegde, All about digital evidence, Ipleaders (26th Feb. 2026, 4:00 PM), https://blog.ipleaders.in/all-about-digital-evidence/

- Digital evidence can be derived from communications sent by email, instant messaging, text messaging, and other electronic messaging platforms. Posts, messages, comments, and other content from various social media sites, such as Facebook, Instagram, Twitter, and others, can be utilised as important digital proof.

- Digital evidence also includes spreadsheets, presentations, digital documents, and other file formats. These files' metadata may also include crucial information.

- Digital images and videos can provide as strong proof. Timestamps and geolocation information are examples of metadata that can be very important for proving the legitimacy and context of media assets.

- Digital evidence can be analysed from logs that document computer and internet activity, such as browsing history, file access, and system logs. Digital evidence also includes GPS and location data recorded by mobile devices and some digital cameras. Call logs, durations, and time stamps are among the call records that can be considered digital evidence.

- Digital evidence includes digital records of financial transactions. This includes electronic currency transfers, bank statements, and internet transactions, all of which might be crucial for financial investigations. Digital fingerprints, facial recognition information, and recordings of distinctive vocal traits, 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 added Section 61 to strengthen the admissibility of electronic evidence, stating that it cannot be deemed inadmissible merely because it is in electronic form. If the requirements outlined in Section 63 are fulfilled, it states that no digital or electronic record will be excluded from admissibility and will have the same legal force, validity, and enforceability as any other document.

> *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[14].

This provision applies to electronic records contained in semiconductor memories, besides which are printed on paper, stored, recorded, or copied in optical or magnetic media. Under the BSA, 2023, the applicability of this section has been widened by adding the word "any communication device[15]"

The BSA, 2023, maintains up the need that the certificate be supplied, but it has been made clear that the certificate must be submitted with the electronic record each time it is presented for admission. Further, a person occupying a responsible official position was supposed to issue the certificate, but under the BSA, 2023, the certificate may be issued by a person who is the owner of the computer or communication device, and an expert.

The Evidence Act did not specify the form in which the certificate was to be issued, but under the BSA, 2023, the specific form has been given in the Schedule. Part A of the Schedule provides for the form to be filled by the Party and Part B provides for the form to be filled by the Expert. Also, the explanation given under the Evidence Act has now been omitted under the BSA, 2023[16].

Admissibility of electronic evidence means the legal recognition and acceptance of digital records by a court, subject to compliance with statutory safeguards ensuring authenticity and reliability.

1. Recognition of Electronic Records as Primary Evidence

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

[14] The Bharatiya Sakshya Adhiniyam, 2023, § 61, No. 47, Acts of Parliament (India).
[15] ANJANA PRAKASH, ANUJ PRAKAASH, THE BHARATIYA SAKSHYA ADHINIYAM 385 LexisNexis 2025.
[16] ANJANA PRAKASH, ANUJ PRAKAASH, THE BHARATIYA SAKSHYA ADHINIYAM 385 LexisNexis 2025.

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.

2. Conditions for Admissibility under Section 63 of BSA, 2023

The very admissibility of an electronic record, which is called as a computer output, depends upon the satisfaction of the four conditions under section 65B (2) of the Evidence Act (now section 63(2) of the BSA, 2023), enumerated as below[17]:

Principles of relevance, authenticity, and reliability primarily govern the admissibility of electronic evidence under the BSA, 2023. Authenticity must be established. It must be proven that the electronic record is authentic and has not been tampered with or changed by the person presenting it. System logs, digital signatures, metadata analysis, forensic testing, hash values, and the testimony of the device's operator can all demonstrate this. It is necessary to prove the system's dependability from which the record was generated. Courts can investigate whether there is any hint of manipulation, whether regular processes were followed, and whether the gadget or computer system was operating correctly.

- The electronic record containing the information should have been produced the computer during the period over which the same was regularly used to store or process information for the purpose of any activity regularly carried on that period by the person having lawful control over the use of that computer,

- The information of the kind contained in an electronic record or of the kind from which the information is derived was regularly fed into the computer in the ordinary course of the said activity;

- During the material part of the said period, the computer was operating properly, and even if it was not operating properly for some time, and even though it wasn't working correctly for a while, the record and the accuracy of its contents were unaffected by the break; and

[17] The Bharatiya Sakshya Adhiniyam, 2023, § 63(2), No. 47, Acts of Parliament, 2023 (India).

- The information contained in the record should be a reproduction or derivation from the information fed into the computer in the ordinary course of the activity,

Where an electronic record is used as primary evidence the same is admissible in evidence without compliance with the conditions in section 65B of the Evidence Act (now section 63 of the BSA, 2023), Irrespective of the compliance with the requirements of section 65B of the Evidence Act (now section 63 of the BSA, 2023), which a special provision dealing with admissibility of the electronic record, there is no bar in adducing secondary evidence under sections 63 and 65 of the Evidence Act, 1872 (now sections 58 and 60 of the BSA, 2023), of an electronic records. The certificate required under section 65B (4) (now section 63(4) of the BSA to the admissibility of evidence by way of 2023) is a mandatory condition precedent electronic record, and oral evidence in place of such certificate cannot possibly suffice[18].

3. 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[19], judicial interpretation mandated this certification.

The BSA 2023 reorganises the criteria. The Act provides a more flexible method, but certification or verification is still crucial. Instead of rigidly requiring a technical certificate in every case, the court may determine if the integrity and validity of the electronic record are adequately proven by other trustworthy techniques. This reduces the procedural barriers in situations when obtaining a formal certificate would not be possible, such as when data is stored by online platforms or third parties. These assumptions can be refuted, though. Through cross-examination or expert testimony, the other side is still able to contest the authenticity, source, or integrity of the electronic evidence.

5. Role of Expert Evidence

The BSA highlights the value of expert advice due to the technical complexity of electronic records. Experts in digital forensics might assist the court comprehend encryption, tampering

[18] ANJANA PRAKASH, ANUJ PRAKAASH, THE BHARATIYA SAKSHYA ADHINIYAM 385 LexisNexis 2025.
[19] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

detection, recovery procedures, and metadata. Establishing chain of custody and system dependability requires expert testimony. This illustrates the judicial tendency of incorporating technological expertise into court proceedings, particularly in criminal cases involving financial fraud, cybercrimes, or digital monitoring[20].

CHALLENGES TO THE CREDIBILITY OF ELECTRONIC EVIDENCE

As digital technology has advanced, it has become more difficult to verify the legitimacy of electronic evidence. While the Bharatiya Sakshya Adhiniyam, 2023 offers a legal framework, practical challenges remain due to technical constraints, lack of experience, and the possibility of tampering.

- **Forgery and Data Manipulation**

One of the most significant issues with electronic evidence is that it may be readily faked or changed. Alteration to files, timestamps, and metadata can be made with modern editing tools without leaving visible traces, rendering digital records untrustworthy without adequate verification. Courts must thus rely on forensic experts to identify falsification and verify authenticity.

- **Volatility and Fragility**

Digital evidence is inherently volatile. Unlike physical documents, which can remain intact for years if stored properly, electronic data is fragile and prone to being lost due to hardware failures, software crashes, accidental deletion, or system malfunctions. If evidence is not promptly preserved or backed up in a secure environment, it risks becoming permanently inaccessible.

- **Threats from Deepfakes and Synthetic Media[21]**

Deepfakes, or extremely realistic fake audio and video recordings, are a new threat brought about by artificial intelligence. Even specialists find it challenging to spot falsification because these AI-generated files can make people appear to say or do things they never did. The validity

[20] The Bharatiya Sakshya Adhiniyam, 2023, § 39, No. 47, Acts of Parliament, 2023 (India).
[21] Prasad, N., & Nair, M. (2023). Emerging threats to electronic evidence: The rise of deepfakes and AI manipulation. Journal of Cybersecurity and Law, 4(2), 14-29

of audiovisual evidence is gravely threatened by this, necessitating the use of more robust forensic instruments and modernised legal requirements.

- **Technical expert gap**

One major issue is that many judges, attorneys, and police officers lack technological skills. The legal profession frequently lacks the expertise in digital forensics and cybersecurity needed to handle electronic evidence. Regular training and professional assistance are crucial because this gap may result in mistakes or delays.

JUDICIAL INTERPRETATION OF ELECTRONIC EVIDENCE

The Popular case **State (NCT of Delhi) v. Navjot Sandhu**[22], although it is more commonly referred to as the Parliament Attack Case. The 2001 terrorist attack on the Indian Parliament gave rise to it. Call records were used by the prosecution as electronic evidence, but the defence contended that they were not admissible due to the lack of the certificate mandated by Section 65B(4) of the Indian Evidence Act.

Depending on the circumstances, the Supreme Court ruled that electronic records could nevertheless be allowed even in the absence of the Section 65B(4) certificate. The Court stated that elements including production method, source, and dependability should be taken into account. This made the law more flexible, allowing parties to prove electronic evidence either as primary evidence or with a certificate.

The Supreme Court overturned earlier interpretations (**State (NCT of Delhi) v. Navjot Sandhu**) in **Anvar P.V. v. P.K. Basheer**[23], one of the most important rulings in this area. The court held that any electronic record that was meant to be used as evidence had to be accompanied by a certificate under Section 65B of the Indian Evidence Act. The ruling stressed that the certificate had to attest to the data's integrity and authenticity, as well as the fact that the electronic record was created using a device that was functioning correctly throughout normal business operations. This ruling established a new standard for the admissibility of electronic evidence, making it a landmark case. The decision also highlighted that courts must be cautious about the potential for digital tampering, and thus, stringent safeguards are

[22] State (N.C.T. Of Delhi) v. Navjot Sandhu@ Afsan Guru, 2005 (11) SCC 600.
[23] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

essential.

In **Shafhi Mohammad v. State of Himachal Pradesh**[24], the Supreme Court of India held that a Section 65B certificate is not always mandatory for electronic evidence. If the party does not have possession of the original device, the certificate requirement can be relaxed. The Court treated the requirement as procedural, not compulsory in all cases. However, this view was later overruled in *Arjun Panditrao (2020)*.

In **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal**[25], the concepts outlined in Anvar were further reinforced. The interpretation of Section 65B was reviewed in this case, and it was confirmed that secondary electronic evidence—such as printouts, screenshots, or copies of digital content—could not be accepted in the absence of a Section 65B certificate. The certificate must be received at the time the evidence is produced, the Court further explained, and it cannot be filed later unless the court permits it under extraordinary circumstances.

These decisions emphasized how crucial it is to uphold the chain of custody, verify the legitimacy of the data, and guarantee procedural compliance. Together, they created a fundamental framework that still shapes court thinking in light of the BSA's more recent provisions.

Comparative global approach on admissibility of electronic evidence

USA

The Federal Rules of Evidence (FRE), a body of procedural guidelines applied by all federal courts in the United States, regulate the admissibility of electronic evidence. The FRE places an emphasis on essential standards, including relevance, authenticity, and legitimate collecting, rather than treating digital evidence as a distinct category. A crucial prerequisite is that any party presenting electronic evidence must show that the information is authentic and comes from a reliable source[26].

A landmark case in this domain, **Lorraine v. Markel American Insurance Company**[27],

[24] Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.
[25] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 2 SCC 650.
[26] Pruthvi Ramkanta Hegde, All about digital evidence, Ipleaders (26th Feb. 2026, 4:00 PM), https://blog.ipleaders.in/all-about-digital-evidence/
[27] Lorraine v. Markel American Insurance Company, 241 F.R.D. 534 (D. Md. 2007).

emphasised the significance of several levels of verification. The court noted that having electronic records alone does not guarantee their acceptance. The parties are required to provide the court with appropriate paperwork outlining the creation, upkeep, and preservation of the data. This decision established a precedent that electronic evidence must be supported by unambiguous evidence of its validity and integrity in addition to being pertinent.

Additionally, U.S. courts frequently rely on expert witnesses in the field of digital forensics to assess whether electronic records have been tampered with or manipulated. The role of forensic certification bodies and strict chain-of-custody protocols further strengthens the reliability of electronic data submitted in court.

UNITED KINGDOM

The UK adopts a slightly different tack by giving the practical dependability of electronic evidence precedence above strict procedural criteria. The legal basis for the acceptance of computer-generated evidence in civil cases is established by the Civil Evidence Act of 1995[28]. According to the Act, even in the absence of extremely technical evidence, digital papers are acceptable provided they seem trustworthy and pertinent to the matter at hand. This adaptable approach aids in avoiding unduly technical obstacles that would make it impossible for relevant and helpful digital data to be taken into account during legal processes. Simultaneously, the UK has made investments to bolster its forensic institutions, giving courts access to expert evaluations where authenticity is in doubt.

Suggestions and Reform

- Establishing National Forensic Protocols, Uniform digital evidence handling guidelines that apply to all states and jurisdictions, will encourage uniformity and eliminate uncertainty.

- Judicial and Legal Training must close current knowledge gaps; lawyers, judges, and investigators should participate in specialised training programs in digital forensics and data verification.

- Public-Private Collaboration needed for developing tamper-detection technologies,

[28] Civil Evidence Act, 1995, c. 38. (United Kingdom).

data preservation strategies, and verification systems to support court processes can be facilitated by collaborating with private sector technology professionals.

- To establish and carry out **National Standards for Digital Evidence**, there is a compelling justification for the creation of an interagency task force or centralized regulatory organization. This organization might eliminate disparities between jurisdictions by developing uniform procedures for gathering, storing, and displaying electronic records.

- It should be obligated to include qualified digital forensic specialists in complicated cases involving substantial digital data, such as cyber fraud, intellectual property theft, or white-collar crimes. These professionals ensure that electronic documents are evaluated using appropriate tools and validated procedures by bringing specific knowledge to the table. To preserve the validity of digital evidence used in court, courts should set rules for the selection, certification, and testimony of these specialists.

- Lastly, investment in technology infrastructure is necessary if courts are to completely adopt the digital transformation of the evidentiary process. Secure mechanisms for uploading, storing, and examining digital files must be installed in e-courts. The court's capacity to manage electronic records effectively and securely would be substantially improved by features including controlled access to evidence databases, encryption for sensitive data, and real-time metadata inspection.

CONCLUSION

Today, electronic evidence is essential to India's judicial system, and the BSA, 2023, offers a contemporary framework for its review, protection, and acceptance. The Act supports the constitutional protection of personal liberty under **Article 21 of the Constitution of India**[29] by ensuring that justice is not denied because of minor technical defects. Instead of strictly focusing on procedural formalities, it gives greater importance to whether electronic evidence is genuine and reliable. As the realm of technology continues to evolve, the Indian legal system must remain adaptive and responsive, incorporating electronic evidence while upholding principles of fairness and justice in its courtrooms. This judgment serves as a beacon for the

[29] INDIA CONST.art. 21.

future, setting a precedent that will continue to guide and shape the admissibility of electronic evidence in Indian courts for years to come[30].

The BSA, 2023, represents a significant step toward modernising India's evidentiary framework in response to digital transformation. By expressly recognising electronic and digital records as valid evidence and restructuring admissibility requirements under Sections 61 and 63, the Act seeks to balance authenticity with procedural practicality. Judicial precedents such as Anvar P.V. and Arjun Panditrao continue to influence their interpretation. Effective implementation, forensic support, and judicial training remain essential to ensure reliability and justice in the digital age.

[30] Astha Jain, Admissibility of electronic evidence under the Indian Evidence Act, Manupatra, 2022, (26.Feb.2026, 8.00 PM) https://articles.manupatra.com/article-details/ADMISSIBILITY-OF-ELECTRONIC-EVIDENCE-UNDER-THE-INDIAN-EVIDENCE-ACT-1872