INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

EVIDENTIARY EVOLUTION: RELIABILITY AND AUTHENTICITY OF ELECTRONIC TESTIMONIES UNDER THE BHARTIYA SAKSHYA ADHINIYAM 2023

AUTHOR - NAMITA DADHICH, STUDENT AT AMITY UNIVERSITY, JAIPUR, RAJASTHAN

BEST CITATION - NAMITA DADHICH, EVIDENTIARY EVOLUTION: RELIABILITY AND AUTHENTICITY OF ELECTRONIC TESTIMONIES UNDER THE BHARTIYA SAKSHYA ADHINIYAM 2023, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 4 (4) OF 2024, PG. 541-555, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

In today's digital era, electronic evidence has become a cornerstone in civil and criminal legal proceedings, driven by the widespread use of digital communications and technology. The increasing reliance on electronic records, video and telephonic testimonies, and other forms of digital evidence has introduced both opportunities and challenges for the judiciary. Courts now face the critical task of determining the authenticity, reliability, and fairness of electronic evidence, which is inherently susceptible to manipulation, tampering, and technical discrepancies. The rise of remote testimonies has further emphasized concerns around witness credibility and the impact on cross-examination, raising questions about the adequacy of existing legal frameworks in addressing these issues. The Indian Evidence Act, particularly its provisions on electronic evidence, serves as a foundation for this transformation, but its practical application often reveals gaps in addressing the complexities of modern technological realities.

This research explores the legislative, judicial, and operational challenges in the admissibility and reliability of electronic evidence in India. It examines case law, statutory provisions, and technological advancements such as blockchain and artificial intelligence to understand their impact on evidence law. The study highlights the need for enhanced statutory clarity, judicial training, and standardized protocols for handling digital evidence, while also advocating for interdisciplinary collaboration between legal professionals and technologists. By proposing best practices and emphasizing the importance of fairness, this paper aims to contribute to the development of a robust framework that ensures justice and accountability in an increasingly digital legal landscape.

Keywords: Technology And Law, Digital Governance, Cybersecurity, Privacy Law, Artificial Intelligence, Digital Rights, Interdisciplinary collaboration.

Introduction: Understanding Digital Evidence in the Modern Legal Landscape

Digital evidence has become a fundamental element in modern legal systems, profoundly influencing investigations, litigation, and courtroom procedures. The widespread adoption of technology has reshaped communication, commerce, and daily life, while simultaneously introducing new dimensions to criminal activities and civil disputes. Defined as information stored or transmitted in digital formats, such as emails, social media interactions, digital files, and metadata, digital evidence plays a pivotal role in determining legal outcomes. Recognizing this shift, the Bharatiya Sakshya Adhiniyam (Indian Evidence Act, 1872) underwent a significant revision in 2023 to include digital evidence, aligning Indian law with global trends and highlighting its growing importance in criminal, civil, and corporate litigation. As digital interactions become central to modern life, the challenges of ensuring the admissibility, authenticity, and security of digital evidence require a

comprehensive understanding and adaptation by the legal community.

Unlike traditional forms of evidence, digital evidence is intangible, existing as binary data on electronic devices like servers, computers, and smartphones. This immaterial nature makes it vulnerable to manipulation, hacking, and unauthorized alterations, presenting unique hurdles for legal practitioners and investigators. Its transient nature further complicates its use, as digital evidence can be easily deleted or modified. However, traces often persist and can be retrieved using advanced forensic tools, such as those that analyze metadata, which reveals critical details about a file's creation, modification, and transmission. This highlights the growing importance of digital forensics, a specialized discipline that enables experts to extract, analyze, and verify the integrity of electronic evidence.

In India, the admissibility of digital evidence is governed by its authenticity, relevance, and compliance with procedural laws. The Information Technology Act, 2000, introduced the foundation for recognizing electronic records as valid evidence, with Section 65B of the Indian Evidence Act providing a statutory framework. This section mandates that electronic records must be accompanied by a certificate attesting to their reliability and the integrity of the system producing them. The landmark Supreme Court case *Anvar P.V. v. P.K. Basheer (2014)*[863] emphasized the critical role of Section 65B, underscoring the necessity for strict adherence to its requirements to ensure the admissibility of digital evidence. The case further highlighted the need for legal professionals to be proficient in handling and presenting digital records in court.

The revision of the Bharatiya Sakshya Adhiniyam reinforced the importance of integrity and reliability in digital evidence, establishing safeguards against manipulation and tampering. With the rise in cybercrimes and the reliance on digital trails in investigations, these amendments have become essential for maintaining justice. Despite these advancements, the integration of digital evidence into the judicial process remains fraught with challenges, including the massive volume of digital data, complexities of encryption, and cross border data transfers, which require international cooperation and adherence to data protection regulations.

Emerging technologies like blockchain, artificial intelligence (AI), and the Internet of Things (IoT) further complicate the legal landscape. While these innovations offer novel sources of digital evidence, they also raise critical concerns regarding data privacy, ownership, and authenticity. For instance, evidence generated by AI or IoT[864] devices like smart home systems may play a crucial role in future cases, but their reliability and admissibility will demand careful evaluation. Digital evidence has undeniably reshaped the legal landscape, introducing both opportunities and challenges for the judiciary. As frameworks like the Bharatiya Sakshya Adhiniyam evolve to address technological advancements, the integrity, security, and authenticity of digital evidence must remain central to legal reforms. In an increasingly digitized world, the legal profession must continuously adapt to the complexities of digital evidence, ensuring that the pursuit of justice keeps pace with technological progress while upholding the rule of law.

Historical Evolution: From the Indian Evidence Act to the Bharatiya Sakshya Adhiniyam

The transition from the Indian Evidence Act (IEA), 1872, to the Bharatiya Sakshya Adhiniyam (BSA), 2023, represents a monumental shift in India's legal framework for evidence. This evolution underscores the pressing need to modernize laws to address changes in society, technology, and governance. Spanning over 150 years, this transformation reflects the dynamic nature of legal norms shaped by colonial

[863] AIR 2015 SUPREME COURT 180, 2014 AIR SCW 5695

[864] Stalford, R. B. "The Role of IoT in Digital Evidence," Computers & Law, 2020.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

history, advancements in digital technology, and the ongoing push for judicial reforms.

1. The Indian Evidence Act, 1872: A Colonial Milestone

Enacted during the British colonial era, the Indian Evidence Act was a cornerstone in the establishment of a standardized legal framework for evidence across Indian courts. Drafted by Sir James Fitzjames Stephen, the IEA sought to unify the fragmented and diverse laws of evidence that varied significantly across India's regions prior to British consolidation.

The Act, grounded in principles of English common law, introduced a uniform set of rules governing the admissibility of evidence in civil and criminal proceedings. It delineated the types of evidence, such as oral and documentary, and laid out procedures for witnesses, presumptions, and the allocation of the burden of proof. The IEA aimed to simplify and streamline legal processes, which was revolutionary at the time.

However, the Act's reliance on physical and testimonial evidence reflected the technological and societal context of the 19th century. While it served the needs of the colonial administration, it did not anticipate the challenges posed by modern technological advancements, such as the digital revolution, cybercrimes, and the growing importance of electronic records.

2. Challenges Faced by the Indian Evidence Act

Despite its historical significance, the Indian Evidence Act encountered several challenges over time, particularly in adapting to the changing technological and social landscape:

a. Digital Evidence and Technological Advances : The advent of computers, emails, and digital communication highlighted the limitations of the IEA. Initially, the Act did not account for electronic records, which became increasingly integral to both civil and criminal cases. Although the Information Technology (IT) Act, 2000, amended the IEA to include electronic evidence, these updates were not comprehensive. The complexity, volume, and susceptibility of digital evidence to tampering underscored the need for a more robust and nuanced legal framework.

b. Changing Socioeconomic Realities : The IEA was conceived in a colonial era marked by vastly different societal, economic, and political conditions. As India evolved into a modern democracy with diverse legal and social challenges, the Act struggled to address contemporary issues such as cybercrimes, digital transactions, and privacy concerns. Additionally, the rise of constitutional safeguards and human rights further necessitated updates to the principles of evidence law to align with modern jurisprudence.

c. Judicial Inefficiencies and Backlogs : India's judicial system has long grappled with procedural inefficiencies and an overwhelming backlog of cases. The rigid procedural requirements of the IEA often added to delays, creating a mismatch between traditional evidentiary principles and the demands of contemporary legal practice. This highlighted the need for reforms that could introduce flexibility, promote efficiency, and better accommodate the complexities of modern litigation.

The Bharatiya Sakshya Adhiniyam, 2023, was introduced as a response to these limitations, aiming to modernize the law of evidence in India. It reflects a progressive approach to addressing the challenges posed by digitalization, changing societal needs, and the demand for judicial efficiency while preserving the core principles of fairness and justice.

The Bharatiya Sakshya Adhiniyam, 2023: A Modern Reformation

The Bharatiya Sakshya Adhiniyam (BSA), 2023[865], represents a transformative

[865] Bharatiya Sakshya Adhiniyam 2023.

development in India's legal framework, aimed at modernizing the evidentiary system to address contemporary challenges. It forms part of a comprehensive overhaul of the criminal justice system, introduced alongside the Bharatiya Nyaya Sanhita (BNS), 2023, which replaces the Indian Penal Code (IPC), and the Bharatiya Nagarik Suraksha Adhiniyam (BNSS), 2023, replacing the Criminal Procedure Code (CrPC). Together, these legislations signal a progressive shift towards a more efficient, equitable, and technologically adaptive legal system.

Key Aspects of the Bharatiya Sakshya Adhiniyam

1. Integration of Digital Evidence : A primary driving force behind the BSS is its emphasis on effectively incorporating digital evidence into the legal framework. Recognizing the increasing reliance on electronic communication, digital transactions, and technological tools in modern disputes and crimes, the BSA provides detailed provisions for the collection, preservation, and admissibility of electronic records. Unlike the Indian Evidence Act, which struggled to keep pace with advancements in technology despite amendments like those under the Information Technology (IT) Act, 2000, the BSA bridges these gaps and ensures alignment with international standards for handling digital evidence. This makes it more robust in addressing issues like cybercrime and electronic fraud.

2. Modernization of Definitions and Procedures: The BSA introduces updated and streamlined definitions to better capture the nuances of contemporary forms of evidence. Key advancements include the explicit recognition of new evidentiary categories such as digital signatures, blockchain records, and AI generated data. By broadening the scope of admissible evidence, the BSA moves beyond the limitations of traditional evidence (oral and documentary) and embraces forensic and cyber forensic reports. This ensures the legal framework is equipped to deal with the complexities of a technology driven era, where digital records often hold crucial probative value.

3. Emphasis on Speedy Justice : Judicial delays and backlogs have long plagued India's legal system. The BSA tackles this issue by introducing measures aimed at streamlining procedures for presenting and scrutinizing evidence. Simplified protocols for evidence submission, coupled with the encouragement of alternative dispute resolution (ADR) mechanisms, aim to reduce the burden on courts. By promoting efficiency without compromising fairness, the BSA seeks to make justice more accessible and timely for litigants.

4. Alignment with Constitutional Principles: The BSA places significant emphasis on safeguarding constitutional values, particularly in the context of evidence collection and use. It seeks to ensure that individuals' privacy, dignity, and liberty are protected, even as digital and forensic evidence become more prevalent. This is especially relevant given the growing concerns over surveillance, data breaches, and misuse of state powers. The BSA adopts a balanced approach, recognizing the need for reliable evidence while protecting individuals from intrusive practices.

Key Judicial Precedents and Case Law

1. Anvar P.V. v. P.K. Basheer (2014)[866] This landmark case underscored the procedural rigor required for the admissibility of electronic evidence under Section 65B of the Indian Evidence Act. The Supreme Court held that electronic records must be accompanied by a certificate ensuring their authenticity, as mandated by Section 65B. This ruling emphasized the importance of technical compliance to ensure that digital evidence is reliable and tamperproof, setting a high standard for its use in legal proceedings.

2. Shafhi Mohammad v. State of Himachal Pradesh (2018)[867] Recognizing the practical challenges in obtaining a Section 65B

[866] AIR 2015 SUPREME COURT 180, 2014 AIR SCW 5695
[867] 2018 (1) SCC473

certificate, especially in cases involving third-party electronic records, the Supreme Court relaxed the strict procedural requirements in certain scenarios. This case highlighted the need for flexibility in dealing with digital evidence while maintaining its credibility, particularly when procedural compliance is not feasible.

3. State of Maharashtra v. Dr. Praful B. Desai (2003)[868] In this pioneering decision, the court expanded the interpretation of the term "evidence" to include electronic evidence under the Indian Evidence Act. The judgment emphasized that technological advancements must be matched by corresponding legal adaptations, reinforcing the importance of embracing digital tools and methods in the evidentiary process.

The Bharatiya Sakshya Adhiniyam, 2023, represents a bold step towards modernizing India's evidentiary framework. By integrating digital evidence, redefining admissibility standards, and streamlining procedures, it aligns the legal system with the demands of a technology driven era. Grounded in constitutional principles, the BSA ensures that justice remains fair and efficient while adapting to the complexities of the digital age. Through its provisions and alignment with landmark judicial interpretations, the BSA establishes a strong foundation for a future ready judicial system.

Admissibility of electronic record or electronic document

The word 'admissible' means the evidence which can be admitted in court and taken on record. The concept of admissibility is completely different from concept of relevancy and probative value of the evidence adduced. Section 65 B makes electronic evidence admissible, it does not dispense with the relevancy and probative value. In *State of Uttar Pradesh Vs. Raj Narain*[869], it has been held that facts should not be received in evidence unless they are both relevancy and admissible. The Apex Court in *State of Bihar Vs Sri Radha Krishna Singh*[870] has further held that admissibility of document is one thing and its probative value is quite another thing – these two aspects cannot be combined. In *Arjun Panditrao Khotkar*[871] the Hon'ble Supreme Court has observed that Section 65 differentiates between existence, condition and contents of a document. Whereas existence goes to 'admissibility' of a document 'contents' of a document are to be proved after a document becomes admissible in evidence. Section 22-A of the Evidence Act provides that if the genuineness of the electronic record produced is questioned, the oral evidence would be admissible as to the contents of the electronic records. However, the Hon'ble Madras High Court reiterated the same in *Santhosh Kumar Vs State rep. by Inspector of Police Perundurai Police Station*[872] wherein it has been held that oral evidence cannot take the place of section 65-B (4) certificate. Further Section 4 of IT Act also provides that if a document in electronic form is (a) rendered or made available in an electronic form and (b) accessible so as to be usable for a subsequent reference, then it would be sufficient compliance. Moreover, the electronic evidence is made admissible by the amendment of section 92 of Information Technology Act-2000 in the Indian Evidence Act. Section 3(2) of Indian Evidence Act states that evidence includes all documents including electronic records produced for the inspection of the court. Such documents are called as documentary evidence. As stated supra, the word 'electronic records' is defined under section 2(t) of Information Technology Act. It has been held in *Thana Singh Vs Central Bureau of Narcotics (2013)*[873] that a digital charge sheet was held to be a document and it can be accepted as electronic record. Hon'ble Supreme

[868] AIR 2003 SUPREME COURT 2053, 2003 (4) SCC 601
[869] (1975)4 SCC 428
[870] 1983 AIR 684
[871] (2020 (5) CTC 200)
[872] 2021(2) MLJ (Crl) 225
[873] 2 SCC 590)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Court has directed to supply of charge sheet in electronic form additionally.

Defining Digital Evidence: Scope and Applicability under Indian Law

Digital evidence refers to any information or data that is stored or transmitted in digital format and is used in court to prove or disprove facts in a legal proceeding. As technology continues to advance, digital evidence has become increasingly significant in both civil and criminal cases. In India, digital evidence is governed by a combination of the Information Technology Act, 2000, and the Indian Evidence Act, 1872, with specific provisions added to address the growing reliance on electronic records. The Bharatiya Sakshya Adhiniyam (BSS), 2023, which aims to replace the Indian Evidence Act, promises to offer a more comprehensive and updated framework for digital evidence.

Scope of Digital Evidence under Indian Law

The **Information Technology Act, 2000** (IT Act) laid the groundwork for the admissibility of digital evidence in India. Under Section 65B of the Indian Evidence Act, 1872, electronic records are admissible in court if certain conditions are met. This section was introduced by an amendment in 2000 to accommodate the IT Act and to align the laws of evidence with technological advancements[874].

According to Section 65B, any electronic record, such as emails, text messages, computer files, or even social media content, can be presented as evidence in court if a certificate authenticating the source of the data is produced. This certificate must be signed by a person in a responsible position over the operation of the device from which the electronic record was generated, ensuring its authenticity and integrity.

Digital evidence can range from simple computer-generated documents to complex datasets like digital forensics, computer logs, and metadata. It plays a critical role in cases involving cybercrime, intellectual property disputes, and even traditional crimes where digital communication or digital footprints may be relevant, such as in murder or fraud cases.

The Indian courts have been relatively proactive in recognizing and dealing with the complexities surrounding digital evidence. The Supreme Court of India has, in several judgments, laid down guidelines on how digital evidence should be handled. **Anvar P.V. v. P.K. Basheer (2014)** In this landmark case, the Supreme Court ruled that any electronic evidence must comply with the conditions laid out in Section 65B for it to be admissible. The court stressed the need for certification to ensure that the digital evidence is authentic and untampered. This judgment clarified the procedures for admitting electronic records as evidence and overruled previous judgments that allowed digital evidence to be admissible without such certification. This decision marked a turning point in how digital evidence would be handled in Indian courts. **Shafhi Mohammad v. State of Himachal Pradesh (2018)** The Supreme Court in this case recognized that in certain situations, obtaining a Section 65B certificate may be impractical. For example, in cases where the electronic evidence is not directly under the control of the person presenting it, the requirement for certification could be relaxed. This judgment provided some flexibility in handling digital evidence and ensured that justice would not be delayed due to procedural technicalities.

Admissibility of Digital Evidence under the Indian Evidence Act

The incorporation of digital evidence into the Indian legal system has revolutionized evidence law, enabling courts to address the complexities of modern technological advancements. The Indian Evidence Act, 1872[875], as amended by the Information Technology Act, 2000, introduced specific provisions for the admissibility of

[874] Ministry of Electronics and Information Technology. (2021). Draft Personal Data Protection Bill. Available at: Personal Data Protection Bill

[875] The Indian Evidence Act, 1872

electronic records. Among these, Sections 65A and 65B play a pivotal role in ensuring the integrity and authenticity of digital evidence while laying down the framework for its admissibility in judicial proceedings.

Key Provisions of the Indian Evidence Act

Section 65A establishes that electronic records may be proved in accordance with the procedure outlined in Section 65B. This provision serves as the foundation for treating electronic records as secondary evidence. Section 65B, on the other hand, provides detailed conditions under which electronic records, such as computer outputs, emails, and CCTV footage, can be admissible in court. These conditions include requirements for the proper functioning of the computer, consistent usage for storing or processing information, and assurance that the data has not been altered. Furthermore, Section 65B mandates the submission of a certificate under Section 65B(4) to authenticate electronic records, ensuring their reliability as evidence.

Landmark Judgments on Digital Evidence : Several judicial decisions have shaped the legal framework for digital evidence in India:

1. Anvar P.V. v. P.K. Basheer (2014): This landmark ruling established the mandatory requirement of a certificate under Section 65B for the admissibility of electronic records. It overruled the earlier decision in State v. Navjot Sandhu (2005), clarifying that primary electronic evidence must be accompanied by a certification to confirm its authenticity.

2. Tomaso Bruno & Anr. v. State of Uttar Pradesh (2015): The Supreme Court emphasized the importance of digital evidence, such as CCTV footage, in criminal trials. The Court reiterated that compliance with Section 65B is essential to ensure the admissibility of such evidence.

3. Shafhi Mohammad v. State of Himachal Pradesh (2018): Recognizing practical challenges in obtaining Section 65B certificates, the Court provided flexibility in cases where acquiring the certificate was not feasible, provided the integrity of the evidence could be independently established.

4. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020): Reaffirming the significance of Section 65B certification, the Supreme Court ruled that this requirement is mandatory, except in cases where proving its impracticality is conclusive.

Challenges and Future Directions

While the inclusion of digital evidence has expanded the scope of legal proceedings to address cybercrime, financial fraud, and other technology-driven offenses, it has also introduced challenges. Digital evidence is vulnerable to tampering, manipulation, and data breaches, necessitating rigorous verification and proper chain-of-custody protocols. Digital forensics has thus become critical to preserving and presenting digital evidence effectively.

The rapid development of technologies such as artificial intelligence and blockchain is likely to further broaden the spectrum of digital evidence. This underscores the need for continuous updates to legal frameworks to ensure they remain robust and relevant.

The Way Forward

India's legal framework for digital evidence, built around Section 65B of the Indian Evidence Act and subsequent judicial interpretations, is evolving to meet the demands of a technology-driven world. While the current provisions provide a solid foundation, the growing reliance on digital evidence demands ongoing training for law enforcement and legal practitioners to enhance their ability to handle and present such evidence effectively. Balancing technological advancements with rigorous evidentiary standards will be crucial in ensuring fair trials, maintaining judicial integrity, and delivering justice in an increasingly digital society.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Bharatiya Sakshya Adhiniyam: New Provisions for Digital Evidence

The **Bharatiya Sakshya Adhiniyam** (BSA), which aims to replace the Indian Evidence Act, brings forth new provisions for digital evidence, reflecting modern technological advancements. Digital evidence, which includes emails, digital contracts, CCTV footage, and social media data, has gained paramount importance in the legal realm. With evolving cybercrimes and electronic transactions, these updates are crucial for the effective administration of justice.

Key provisions under the BSA related to digital evidence include:

1. **Digital Documentation and Contracts**: Digital signatures and electronic agreements are now considered admissible, ensuring that business transactions and online communications can be accepted as evidence in courts.
2. **Authenticity and Admissibility of Electronic Records**: Just as under Section 65B of the Indian Evidence Act, the BSA continues to emphasize the requirement for certification to authenticate digital evidence, but with modernized rules that allow for greater flexibility, especially in cases where obtaining certificates is challenging.
3. **Focus on Cybercrime**: With an uptick in cybercrimes, the BSA enhances the handling of electronic evidence in such cases. It specifies the procedure for gathering, preserving, and presenting digital evidence, ensuring that its integrity remains intact[876].
4. **Streamlined Procedure for Digital Evidence in Court**: The BSS proposes an updated framework for how digital evidence is to be submitted and assessed in courts, with stringent measures to prevent data tampering, hacking, or forgery.
5. **Chain of Custody and Forensics**: The BSA outlines the importance of maintaining a proper chain of custody for digital evidence, ensuring that the source of the evidence and the process of obtaining it can be verified.

The new provisions under the **Bharatiya Sakshya Adhiniyam** signify India's commitment to embracing technology in legal proceedings while balancing the need for rigorous standards in evidence admissibility. These provisions will ensure that digital evidence is treated with the same level of seriousness and scrutiny as traditional forms of evidence.

Authentication and Integrity: Establishing the Reliability of Digital Evidence

Authentication and integrity are critical to ensuring the reliability of digital evidence in legal proceedings. Given that digital data can be easily altered, tampered with, or corrupted, the legal system has developed stringent requirements to establish its authenticity and maintain its integrity.

1. Authentication: To be admissible in court, digital evidence must be authenticated—proving that the data is what it purports to be. Section 65B of the Indian Evidence Act and similar provisions globally require that a certificate accompany the electronic record, certifying that the record was produced by a reliable computer system, and that the process of creating it was trustworthy. This certificate must be signed by a person responsible for the management of the computer system from which the data was extracted. The idea is to ensure that the source of the evidence is legitimate and that the evidence itself has not been tampered with.

2. Chain of Custody: The integrity of digital evidence is preserved through an unbroken chain of custody. From the moment digital evidence is collected, every individual who

[876] Privacy International. (2021). Public Engagement in Digital Rights.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

handles it must record their involvement to prevent allegations of tampering or mishandling. This ensures that the evidence remains in its original state and has not been altered between the time of collection and its presentation in court. Proper documentation of each stage, from collection to analysis, strengthens the credibility of the evidence.

3. Forensic Procedures: In order to maintain the integrity of digital evidence, forensic techniques are employed. Experts create hash values (unique identifiers for digital data) when digital evidence is collected. By comparing the hash values of the original and the copied data, experts can verify that the data has not been altered. For instance, during investigations, law enforcement ensures that only read-only access is used when examining hard drives or servers to prevent any unintentional alterations.

4. Challenges to Reliability: While these measures help authenticate and maintain the integrity of digital evidence, challenges arise due to the complexities of technology. Cyberattacks, human error, or flaws in the preservation process may raise questions about reliability. Therefore, courts must often rely on expert testimony to establish the credibility of digital evidence.

5. Jurisprudence: The Indian Supreme Court, in *Anvar P.V. vs P.K. Basheer*, upheld the importance of the certification under Section 65B of the Indian Evidence Act, emphasizing that digital evidence is not admissible without fulfilling this statutory requirement. Similarly, in the U.S., the *Frye* and *Daubert* standards require that the method used to gather digital evidence must be generally accepted by the scientific community.

The authentication and integrity of digital evidence are fundamental to its admissibility in court. These processes ensure that digital evidence remains untampered and reliable, providing a solid foundation for its use in modern legal proceedings.

Comparative Analysis: Key Differences between the Indian Evidence Act and Bharatiya Sakshya Adhiniyam

The introduction of the Bharatiya Sakshya Adhiniyam (BSA) aims to overhaul India's legal framework regarding evidence, particularly addressing the growing importance of digital evidence in today's legal landscape. It builds upon and updates the century old Indian Evidence Act (IEA), 1872, which, though amended over the years, struggled to address the complexities of digital and electronic data in legal proceedings.

1. Recognition and Definition of Digital Evidence

- **Indian Evidence Act**: Digital evidence became part of the IEA through the Information Technology (IT) Act of 2000. Section 65B of the IEA, introduced in this amendment, allows electronic records to be admitted as evidence, provided certain conditions are met. However, the rigidity of Section 65B—particularly the requirement of a certificate from the person managing the system—often posed challenges in practical cases, especially when access to the certifier was limited.
- **Bharatiya Sakshya Adhiniyam**: The BSA simplifies the admission of digital evidence by modernizing its approach to the management and admissibility of electronic records. The focus has shifted towards ensuring the reliability and authenticity of the data rather than procedural bottlenecks, thereby streamlining the process for admitting such evidence. The BSA recognizes the evolving nature of technology and the need for judicial systems to keep pace.

2. Authentication of Digital Evidence

- **Indian Evidence Act**: Section 65B laid down stringent rules for the authentication of digital evidence, including a mandatory certification

process, which often resulted in procedural delays. This rigid requirement for the issuance of a certificate stating that the electronic record is a true and accurate representation of the original is viewed as a potential barrier to the swift administration of justice.

- **Bharatiya Sakshya Adhiniyam**: The BSS broadens the scope of authentication by emphasizing technological standards such as digital signatures, cryptographic keys, and other modern techniques to verify the authenticity of digital evidence. This allows for a more adaptable process, where evidence can be evaluated based on its digital footprint and chain of custody rather than relying strictly on certification.

3. Evidentiary Standards for Digital Evidence

- **Indian Evidence Act**: The IEA requires the production of primary evidence, except in cases where it is not possible. Digital evidence, classified as secondary evidence under the IEA, often required additional steps for its admission in court. The court must be convinced of the original source's integrity and reliability.
- **Bharatiya Sakshya Adhiniyam**: The BSA introduces a more nuanced approach to handling digital evidence. The act acknowledges that digital records are often inherently duplicable and that their reliability lies not in the format but in their source and how they were handled. This paradigm shift allows courts to give digital evidence greater weight without unnecessary procedural roadblocks, provided that the integrity of the data is proven.

4. Chain of Custody

- **Indian Evidence Act**: Under the IEA, maintaining a chain of custody for digital evidence was crucial, but the law lacked specific provisions to handle the unique characteristics of electronic data. Breaches in the chain of custody could lead to the disqualification of crucial evidence.
- **Bharatiya Sakshya Adhiniyam**: The BSA explicitly addresses the importance of chain of custody in digital evidence. It mandates stricter documentation and procedural standards to ensure that the evidence remains untampered from collection to presentation. This requirement is essential in preventing the corruption of digital records, which are more susceptible to alteration than traditional forms of evidence.

5. Admissibility of Digitally Stored Evidence

- **Indian Evidence Act**: Section 65A and Section 65B of the IEA primarily govern the admissibility of electronic records, including emails, text messages, and social media interactions. Despite these amendments, the law was perceived as outdated, given the rapid growth of digital communication platforms and the widespread use of cloud storage, blockchain, and other advanced digital storage systems.
- **Bharatiya Sakshya Adhiniyam**: The BSA provides more expansive provisions for admitting digitally stored evidence. It acknowledges the prevalence of cloud based services and introduces flexibility in the admissibility of records stored on decentralized platforms like blockchain. The legal framework has been updated to reflect the changing technological landscape, allowing the court to consider a wider range of digital evidence.

6. New Provisions for Privacy and Data Protection

- **Indian Evidence Act**: While the IEA recognizes the importance of

confidentiality in certain circumstances, it lacks a comprehensive framework for handling sensitive digital data that involves privacy concerns, especially under the lens of recent data protection debates.

- **Bharatiya Sakshya Adhiniyam**: The BSA incorporates provisions that align with India's data protection laws, such as the proposed Digital Personal Data Protection Act. It ensures that the collection, storage, and presentation of digital evidence comply with privacy standards, safeguarding personal data while ensuring the admissibility of evidence that is critical to legal proceedings.

7. Presumptions Relating to Digital Evidence

- **Indian Evidence Act**: Section 85A of the IEA introduces a presumption regarding the validity of electronic agreements, particularly those executed digitally. However, the act does not provide a comprehensive framework for handling presumptions related to digital communications, metadata, or blockchain records.
- **Bharatiya Sakshya Adhiniyam**: The BSA expands on these presumptions, recognizing the increasing reliance on digital contracts, emails, and metadata in both commercial and criminal cases. It creates a more robust presumption of authenticity for these forms of digital records, provided that the opposing party cannot prove tampering or forgery.

The Bharatiya Sakshya Adhiniyam represents a forward-thinking approach to the admissibility, handling, and evaluation of digital evidence, addressing the shortcomings of the Indian Evidence Act in this regard. By modernizing procedural requirements, expanding the scope of admissible digital evidence, and incorporating contemporary technological practices, the BSA ensures that India's legal framework can better respond to the realities of the digital age. This shift is crucial for the efficient administration of justice in cases where digital evidence plays a central role, from cybercrimes to corporate disputes.

Challenges in Admitting Digital Evidence: Legal and Technical Complexities

Admitting digital evidence into court presents unique challenges that combine both legal and technical complexities. While the introduction of the Information Technology Act in India, along with the Indian Evidence Act's provisions under Section 65B, laid down a framework for dealing with electronic records, various hurdles persist.

1. Authentication and Reliability: One of the major legal challenges involves the authentication of digital evidence. Section 65B of the Indian Evidence Act mandates that digital evidence must be accompanied by a certification from a responsible individual attesting to its authenticity. However, this requirement often poses significant difficulties, especially when the originator of the document or data is unavailable, or in cases where obtaining such certification is impractical, such as cloud based or foreign hosted data.

Courts have frequently debated whether the stringent requirement of certification is a barrier to justice, leading to discussions on relaxing or modifying this provision.

2. Data Integrity and Chain of Custody: Maintaining the chain of custody for digital evidence is crucial. Digital evidence, unlike traditional physical evidence, is easily altered, deleted, or tampered with. Ensuring that the data has remained unaltered from its creation to its presentation in court is essential for its admissibility. Courts are becoming increasingly aware of the need for a reliable and secure chain of custody, but this also places additional burdens on law enforcement agencies and legal professionals to maintain rigorous documentation and security protocols.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

3. Technological Obsolescence and Complexity: Technological advancements outpace the legislative framework. The nature of digital evidence is rapidly evolving, including data stored in cloud servers, blockchain technology, and the rise of artificial intelligence systems. Traditional laws struggle to adapt to the complexities of such technologies, creating gaps in understanding and addressing the admissibility of new forms of digital data. Legal professionals must stay updated on technological advancements to navigate these challenges.

4. Cross Border Jurisdiction and Data Localization: In many cases, digital evidence is stored in servers located outside the country, raising jurisdictional issues. Obtaining such evidence from foreign countries is complex and often requires mutual legal assistance treaties (MLATs), which can take considerable time. Additionally, different countries have varying standards for handling digital evidence, further complicating its admissibility in Indian courts.

5. Privacy Concerns and Data Protection: The admissibility of digital evidence also brings up concerns regarding the right to privacy. The Indian Supreme Court's judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India[877] established the right to privacy as a fundamental right. Digital evidence, especially when it involves personal data, must balance the evidentiary needs of the court with the privacy rights of individuals, adding another layer of complexity in legal proceedings. While digital evidence is increasingly critical to modern legal proceedings, its admission into court remains fraught with challenges. Both legal reforms and advances in technology are necessary to streamline the process and ensure that justice can be administered efficiently without compromising the integrity of the evidence or individual rights.

Impact on Criminal Investigations: How Digital Evidence Shapes Trials

The advent of digital evidence has revolutionized criminal investigations and significantly impacted the judicial process. With the proliferation of digital technology, law enforcement agencies increasingly rely on electronic data to gather evidence, solve crimes, and secure convictions. This shift has brought both advantages and challenges to the criminal justice system.

1. Types of Digital Evidence

Digital evidence encompasses a wide range of materials, including:

- **Electronic communications**: Emails, texts, and social media interactions often serve as critical evidence in establishing intent, motive, and relationships between parties.
- **Digital footprints**: Data from websites, search histories, and online activity logs can provide insight into a suspect's actions and state of mind.
- **Surveillance footage**: Video recordings from CCTV and other surveillance systems can corroborate or refute witness testimonies and provide timelines of events.
- **Forensic data**: Computer and mobile device forensics can reveal deleted files, messages, and data, often crucial for understanding the full context of a case.

2. Enhancing Investigative Techniques

The integration of digital evidence into criminal investigations allows law enforcement to adopt more sophisticated and targeted approaches. For instance, data analysis and forensic tools can help identify patterns, link suspects to crimes, and establish connections between different cases. Technologies like geographic information systems (GIS) enable investigators to visualize crime scenes and analyze crime patterns, aiding in the identification of hotspots and trends.

[877] AIR 2017 SC 4161

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

3. Legal Implications and Challenges

While digital evidence can strengthen cases, it also presents legal challenges. Courts must ensure that such evidence is collected and handled according to established protocols to prevent violations of privacy rights and ensure its admissibility. The landmark case of *R v. Hennessey* (1998) highlighted the necessity of proper procedures for digital evidence collection, reinforcing that mishandling can lead to suppression in court.

Moreover, the sheer volume of digital data can overwhelm investigators and juries, complicating the trial process. Legal practitioners must be adept at interpreting and presenting this evidence clearly and concisely.

4. Public Perception and Expectations

The portrayal of digital evidence in popular media often influences public perception of criminal investigations. High-profile cases that rely on digital evidence can lead to heightened expectations regarding the speed and efficiency of investigations. For example, cases like the Boston Marathon bombing relied heavily on digital surveillance, leading to rapid identification and apprehension of suspects. This creates a dichotomy where the public demands quick justice, but the legal system must balance thorough investigations with constitutional rights.

5. Future Trends

As technology continues to evolve, so too will the methods of gathering and analysing digital evidence. Emerging fields such as artificial intelligence (AI) and machine learning are beginning to play roles in predictive policing and evidence analysis, potentially increasing the efficiency of investigations. However, these advancements also raise ethical concerns regarding privacy, bias, and the potential for misuse.

Digital evidence has become an integral part of modern criminal investigations, shaping the way cases are built and prosecuted. While it offers numerous advantages, it also necessitates careful handling to uphold legal standards and protect individual rights. As society becomes increasingly digitized, the implications of digital evidence on criminal justice will continue to evolve, warranting ongoing dialogue and reform to address the challenges that arise.

Future Trends: Digital Evidence and Emerging Technologies

As the legal landscape evolves, the integration of emerging technologies in the realm of digital evidence is transforming criminal investigations and judicial processes. The future trends indicate significant advancements that not only enhance the effectiveness of gathering and analysing evidence but also present new challenges in legal practices and ethical considerations. Here are some key areas where emerging technologies are expected to shape the future of digital evidence:

1. Artificial Intelligence (AI) and Machine Learning

AI and machine learning are at the forefront of transforming how digital evidence is collected and analysed. These technologies can process vast amounts of data quickly, identifying patterns and anomalies that human investigators might miss. For instance, AI can assist in facial recognition, enabling law enforcement to identify suspects from surveillance footage rapidly. Machine learning algorithms can also analyze social media interactions and digital communications to establish connections between individuals and events.

2. Blockchain Technology

Blockchain technology is emerging as a powerful tool for ensuring the integrity of digital evidence. By providing a decentralized and immutable record of transactions, blockchain can be used to secure the chain of custody for digital evidence. This technology can verify the authenticity of digital files, making it more

difficult for tampering or alteration to go undetected.

3. Cloud Computing and Data Storage

The rise of cloud computing offers new opportunities and challenges for the management of digital evidence. While cloud services provide scalable and secure storage solutions, they also raise concerns about jurisdiction, data privacy, and access rights. Legal frameworks will need to adapt to address these issues, ensuring that digital evidence stored in the cloud remains accessible and admissible in court.

4. Internet of Things (IoT) and Smart Devices

The proliferation of IoT devices creates an unprecedented amount of data that can serve as digital evidence. Smart home devices, wearables, and connected vehicles generate data that can provide insights into a suspect's activities. However, this also complicates issues of privacy and data ownership, as well as the admissibility of evidence collected from these devices.

5. Virtual Reality (VR) and Augmented Reality (AR)

VR and AR technologies are beginning to play roles in presenting evidence in court. These immersive technologies can recreate crime scenes or visualize data in ways that make it easier for juries to understand complex evidence. As these technologies evolve, they will likely become more integrated into legal proceedings.

The future of digital evidence is intricately linked to technological advancements that offer new possibilities and challenges for law enforcement and the judiciary. As AI, blockchain, cloud computing, IoT, and immersive technologies continue to develop, they will redefine the landscape of digital evidence, necessitating updated legal frameworks and ethical considerations. Adapting to these changes will be crucial for ensuring that justice is served while respecting individual rights and privacy.

Rights of the accused and digital records:

Once we deal about proof of electronic records, it is equally important that opportunity must be given to disprove it. Needless to say, right to fair trial is a fundamental right and valuable right to an accused. In *Manu sharma Vs State NCT of Delhi*[878], it has been observed in Para 220 that the right of the accused with regard to disclosure of document is a limited right but it is codified and is the foundation of a fair investigation and trial. On such matters, the accused cannot claim an indefeasible legal right to claim every document of the police file or even the portion which are permitted to be excluded from the document annexed to the report under Section 173(2) as per order of the court. It has been further held that right of the accused to claim documents stemmed from the sections 207, 243 and 91 CrpC. Therefore, when the prosecution proposes to rely upon the tap recorded conversation, accused is entitled to get copies of the same. In a case, the court has to proceed on the basis that the CBI proposes to rely upon the 19 CDs containing 768 calls in addition to the document listed by it in the annexure to the charge sheet. Therefore, each of the accused is entitled to be provided with copies of the 19 CDs containing the 768 calls: *Dharambir; Jagdish Chandra; Ajay Khanna; Anand Mohan Sharan V/S Central Bureau Of Investigation*[879] Regarding the right of the accused to get copies and fair trial, the Supreme Court in P. Gopalakrishnan Vs. State of Kerala 2019 has held that it is cardinal that a person tried for serious offence should be furnished with all the material and evidence in advance, on which the prosecution proposed to rely against him during the trial. Any other view would not only impinge upon the salutary mandate contained in the 1973 code, but also the right of the accused of a fair trial enshrined in Article 21 of the Constitution of India.

[878] (2010)6 SCC 1
[879] 148 (2008) DLT 289).

Conclusion

In today's rapidly advancing digital landscape, the convergence of technology and law has become increasingly crucial. The continuous evolution of technological innovations poses both significant challenges and exciting opportunities for the legal system. To effectively navigate these changes, legal frameworks must be flexible and adaptive, ensuring they address new issues while upholding foundational principles of justice. Bridging the gap between these two domains requires a multifaceted approach, including legislative adaptation, ongoing education, collaboration across sectors, and fostering public engagement.

To stay relevant in the face of technological progress, existing legal frameworks must evolve. This requires revising traditional laws and introducing new regulations that are attuned to emerging technologies. Data privacy, cybersecurity, artificial intelligence, and digital evidence are prime examples of areas requiring modernized legal provisions. For instance, the General Data Protection Regulation (GDPR) in the EU has set a global benchmark for data protection, while India's Personal Data Protection Bill seeks to establish a robust framework to protect individual privacy in the digital sphere. These adaptations are crucial for maintaining legal relevance and ensuring that the rights of citizens are protected in an increasingly digital world. The legal profession must also continuously evolve to keep pace with technological advancements. Legal professionals, from lawyers to judges, must be equipped with the knowledge and skills necessary to navigate complex technological issues such as handling digital evidence, understanding AI's ethical implications, and responding to cybersecurity threats. This can be achieved by integrating technology focused modules into legal education, offering specialized training for practitioners, and providing resources to ensure that legal experts can engage with new technologies competently. Such an educational investment will not only enhance the quality of legal proceedings but also promote confidence in the judicial system's ability to handle modern challenges. Finally, tackling the complexities of technology in law requires collaboration between legal experts, technology professionals, and policymakers. Multistakeholder initiatives can foster dialogue and innovative strategies to address issues like cybercrime and digital forensics. By working together, these sectors can help create a comprehensive legal framework that not only addresses current technological challenges but also ensures the fair and responsible use of technology in society. This collective effort will ultimately bridge the gap between technology and law, enhancing justice and protecting individual rights in a rapidly changing digital landscape.