

## **Impact of E-Records as Evidence in the Judicial System under the Bharatiya Sakshya Adhiniyam 2023**

Vratika Singh<sup>1</sup>, Dr. Bindu Jindal<sup>2</sup>, Vishant Saini<sup>3</sup>, Dr. Pranav Ranga<sup>3</sup>, Dr. Rakhee Rani<sup>3</sup>, Hardik Gupta<sup>4</sup>, Minakshi Banger<sup>5</sup>

<sup>1</sup>Ph.D. Scholar, Department of Law, Maharishi Markandeswar (Deemed to be University) Mullana, India, [vratikasingh.vs@gmail.com](mailto:vratikasingh.vs@gmail.com).

<sup>2</sup>Head & Dean, Department of Law, Maharishi Markandeswar (Deemed to be University) Mullana, India

<sup>3</sup>Assistant Professor, Department of Law, Maharishi Markandeswar (Deemed to be University) Mullana, India

<sup>4</sup>BA.LLB 10th Semester, Department of Law, Maharishi Markandeswar (Deemed to be University) Mullana, India

<sup>5</sup>Assistant Professor, Department of English, Chandigarh University, India

**Abstract:** The Bharatiya Sakshya Adhiniyam 2023 (BSA) is a revolutionary change in India's legal landscape by making electronic records (e-records) admissible evidence, bringing them at par with conventional documentary evidence. By extending the definition of "documents" to cover digital records, the BSA deals with the challenges of the digital era, i.e., authenticity, chain of custody, and cybersecurity. Aiding provisions such as Section 61 prohibit denial of admissibility of electronic records on the basis of being electronic only, and Section 63 adds a uniform process of certification with expert authentication. These reforms simplify judicial procedures, minimize procedural challenges, and increase the efficiency of dealing with e-evidence cases. It is practical difficulties in terms of infrastructure deficiency, technical support, and privacy issues that lie at the root of complete implementation. This abstract examines the implications of e-records under the BSA on India's judicial system and emphasizes the imperative of ongoing technological incorporation and policy reforms to attain equity and reliability in legal proceedings

**Keywords:** Digital signatures, Chain of custody, Forensic digital analysis, E-evidence challenges, Metadata and hash value.

### **1. Introduction**

The Bharatiya Sakshya Adhiniyam, 2023, which was passed to substitute the colonial-era Indian Evidence Act of 1872, is a paradigm shift in India's court system as it brings evidence laws in sync with the latest technological developments. This revolutionary law accepts electronic records (e-records) as evidence, and they are given an equal legal status as conventional paper documents. Proposed by Home Minister Amit Shah and adopted by Parliament in December 2023, the Act seeks to update evidence laws and make judicial procedures more streamlined.

E-records are now essential in legal cases with the emergence of digital transactions, cybercrime, and electronic communication. The Act directly includes provisions regarding the admissibility of electronic evidence such as emails, CCTV footage, and other electronic information under Section 65B. This provides for the authentication of e-records on which courts can base their decisions, ensuring efficiency and transparency in trials.

But the incorporation of e-records has its own set of problems like how to ensure authenticity, protection from tampering, and getting over procedural complexities. The Bharatiya Sakshya Adhiniyam tries to solve these issues by putting in place mechanisms for the certification and authentication of electronic

evidence. While implementing technology, this Act not only makes legal procedures easier but also enhances the solidity of evidence produced in Indian courts.

This background lays the groundwork for examining how e-records under the Bharatiya Sakshya Adhiniyam are transforming India's judicial system while emphasizing their advantages and overcoming implementation issues.

#### Historical Background

The Indian Evidence Act, 1872 (IEA), prepared by Sir James Fitzjames Stephen, was the basis of evidence law in India for more than 150 years. Enacted during colonial times, the IEA established uniform principles of admissibility and categorization of evidence in court proceedings, applicable to civil as well as criminal cases. Although amended from time to time, the Act became more and more outdated in dealing with technological developments and contemporary issues like digital evidence and cybercrimes.

Realizing these constraints, the Indian government presented the Bharatiya Sakshya Bill, 2023, in August 2023 to consolidate and replace the IEA. The Bill aimed to update evidence laws by including provisions of electronic records and filling gaps in rules of secondary evidence. Following early deliberations and the withholding of the original Bill in December 2023, both houses of Parliament enacted a new version on December 21, 2023. The Bharatiya Sakshya Adhiniyam, 2023 (BSA) was given presidential approval on December 25, 2023, and took effect from July 1, 2024.

The BSA brings major reforms to evidence law while maintaining essential elements of the IEA. It focuses on ensuring fairness in trials through updated provisions like broadened definitions of secondary evidence, simplified rules for electronic records, and stronger protection against coercion in confessions. This legislative shift indicates India's attempt to bring its legal system in line with the needs of the times and technological realities.

#### Role of E-Records in Judicial Proceedings in India

The incorporation of electronic records (e-records) into Indian judicial processes has been a major turning point towards the modernization of the legal system. This change is brought about by the growing use of digital evidence in legal proceedings, including emails, CCTV footage, social media posts, and other types of electronic information. The legal framework for e-records in India is largely derived from the Indian Evidence Act, 1872, amended by the Information Technology Act, 2000. The latter added provisions such as Section 65B, which deals with the admissibility of electronic evidence in court.

#### Legal Framework for E-Records

Section 63 of the BSA, 2023 provision requires electronic records to be supported by a certificate attesting to their authenticity and integrity. The certificate should contain information like the date and time of creation, the device, and any changes made to the record. This provision makes e-records primary evidence, subject to certain procedural requirements.

Information Technology Act, 2000: This legislation gives legal acceptance to digital signatures and electronic records, making them valid in legal proceedings. It supplements the Indian Evidence Act by dealing with problems of data security, transmission, and storage.

#### Digitization of Court Records

The Indian judiciary has also been working proactively towards computerizing court records through efforts such as the eCourts Mission Mode Project. The purpose of this project is to enhance the efficiency of court proceedings by granting electronic access to case files, judgments, and court timetables. The National Judicial Data Grid (NJDG) is a repository for case statistics that provides real-time information on pending cases in India. This digitization initiative has greatly minimized case pendency by determining bottlenecks and enabling quicker disposal of cases.

#### Admissibility of E-Records

The Bharatiya Sakshya Adhiniyam, 2023, is an important milestone towards developing the Indian judicial system according to the requirements of a digital world, particularly regarding the admissibility of electronic records as evidence in a court of law. With the growing dependence on technology in business, communication, and government, electronic records have emerged as a primary source of evidence in civil and criminal proceedings. The new Act establishes definite procedural and substantive rules to ensure that electronic records receive the same evidentiary value as conventional documents, subject to their authenticity and integrity being established. A key procedural condition is the issuing of a Section 63 certificate, which confirms the authenticity of the electronic record. The certificate has to indicate the record, state how the record was made or stored, state the device or system it was made or

stored on, and state that the computer or electronic device operated correctly during the period in question. The certificate should be signed by an individual holding a responsible position who is familiar with the working of the device or the process in question. This provision, aimed in spirit like the previous Section 65B of the Indian Evidence Act, 1872, serves as a basis for electronic records' reliability, burdening the opposite party to refute their credibility. Apart from procedural adherence, the technology involved in the electronic record is also crucial in determining its admissibility. Metadata, hash values, and digital signatures are some of the most important tools employed to ensure the authenticity and integrity of electronic records. Metadata contains specific information like the creation date and time, authorship, access history, and any changes to the document, which are important in building a record's timeline and provenance. Hash values, computed by cryptographic algorithms, function as a digital fingerprint; if the hash value of the submitted record corresponds to the original, then it becomes evidence that the content has not been tampered with. Digital signatures provide an extra layer of legitimacy by verifying the sender's identity and that the document has not been altered on its way through. In addition to these technological aids, legal procedure requires proper chain of custody for electronic records. This is a systematic reporting of who possesses the record, when, and how, from seizure or initial creation to delivery in court. The chain of custody protects from unauthorized access, modification, or loss, and failure to maintain it can lead to exclusion or weakening of the evidence. Incorporation of such requirements demonstrates balance between taking advantage of technological development and ensuring due process. By guaranteeing electronic records are both procedure and technical standards compliant, the Bharatiya Sakshya Adhiniyam, 2023, not only updates the evidentiary regime but also enhances judicial trust in electronic evidence. As courts of law become increasingly confronted with cases fueled by electronic data, these provisions guarantee e-records are able to be efficiently and equitably utilized to facilitate justice in a technologically changing society.

#### Judicial Interpretation and Challenges

Since the coming into force of the Bharatiya Sakshya Adhiniyam, 2023, the judiciary has started charting its course over the dynamic landscape of electronic evidence, and initial interpretations point towards a guarded but forward-thinking approach. Even though the Act is still new, courts have begun invoking its provisions, particularly in matters where digital transactions, cybercrimes, and electronic communications are involved. A few district and High Courts have, in their judgments, underscored the necessity of strict compliance of Section 63 on certification of electronic records. These decisions reaffirm that the certificate is not a formality but a bedrock condition of admissibility, as interpreted earlier in respect of Section 65B of the Indian Evidence Act. In a notable 2024 High Court ruling, the court ruled that even WhatsApp messages and emails, while electronically produced and pertinent, would not be admissible unless accompanied by appropriate certification regarding the origin and integrity of the device used. This strict but reasonable stance illustrates the judiciary's insistence on procedural protection while acknowledging the probative value of digital content. Concurrently, the courts also realized that the reliability and authenticity of electronic records cannot be accepted at face value. Judges have also begun to scrutinize the content of the digital document not only but also its metadata, access logs, and the retrieval method. Courts have pursued expert testimony from forensic laboratories to validate hash values and ensure chain-of-custody, particularly in matters of sensitive or disputed digital information. This is a manifestation of an evolving judiciary appreciation for the inherent complexities of digital evidence as well as its susceptibility to tampering. Nevertheless, despite these valiant attempts, various obstacles remain in authenticating electronic records. One of the biggest issues is how easily content can be faked or manipulated with sophisticated software tools. The explosion of technologies such as deepfakes—fake media created by artificial intelligence that can make real individuals seem like they're speaking or acting without their knowledge—is a serious threat to the integrity of audio and visual evidence. Judges now have the challenging problem of identifying authentic digital content versus highly crafted faked material. This will usually involve technical skill and infrastructure which will not be easily found in most judicial platforms, especially at the lower courts. Also, cross-border storage of data makes things even more difficult, as electronic evidence stored on overseas servers is subject to varying jurisdictional and privacy laws, restricting access or prolonging the verification process. The absence of a uniform set of digital forensic standards and trained individuals also contributes to the challenge, frequently resulting in delays and issues regarding admissibility. Lastly, although the Bharatiya Sakshya Adhiniyam, 2023 has established a strong legal foundation for the handling of electronic records, judicial interpretation is still emerging, and functional challenges are of considerable magnitude. Courts are slowly adjusting to the digital world by prioritizing

procedural strictness and leveraging technological support, but combating digital fraud, tampering, and deepfake abuse will demand ongoing legal ingenuity, forensic investment, and continuous training of legal professionals so that justice can be delivered in a technology age.

#### Advantages of Legally Acknowledging E-Records

The official recognition of electronic records through the Bharatiya Sakshya Adhiniyam, 2023 comes with a multitude of revolutionizing advantages that contribute greatly towards improving the speed and integrity of the judicial process. Among the greatest benefits is the speed and efficiency with which legal proceedings can now be handled using digital evidence. Conventional procedures for collecting, storing, and generating physical documents are laborious and subject to logistical delay. Conversely, digital records like emails, SMS, CCTV, online transaction history, and cloud storage can be retrieved and produced quickly, thus accelerating the evidentiary stage of trials. Instant sharing and access to evidence, usually remotely, also lightens the load on judicial infrastructure and personnel, rendering processes more efficient. Coupled with this, improved documentation and storage capacity offer a significant leap forward.

Electronic records can be kept in enormous numbers on secure digital platforms that take up minimal physical space and cost, avoiding the constraints of conventional record-keeping. Courts, law enforcement, and litigants can keep well-organized digital archives that are not only space-saving but also immune to physical deterioration, theft, or loss that normally occurs to paper-based records. This electronic transformation also facilitates ease of retrieval and preservation, since individual records can be identified with search algorithms or metadata filters, conserving valuable time and effort. Proper timestamping, encryption, and backup measures for maintaining electronic records further guarantee that they remain uncorrupted and dependable over time, even between different phases of litigation or appeals. The indexing and automation of information render it much simpler for lawyers and judges to read through evidence and refer back to case files without digging through heavy folders.

Most importantly, perhaps, the acknowledgment of e-records facilitates increased transparency and impartiality in the judiciary. Unlike written or verbal evidence, which might be subjective or tampered with, computer records usually include system-generated metadata like dates, use histories, and audit trails that render them more difficult to falsify. This built-in information makes evidence more reliable and less susceptible to human error or deliberate distortion. For example, biometric authentication, digital signatures, and tamper-evident controls ensure that only those authorized have accessed a document, enhancing its evidential value. Also, electronic records promote a feeling of responsibility between litigants and officials because computer systems provide detailed records of actions taken and decisions made. In criminal proceedings, real-time information from surveillance systems, mobile phone location tracking, and forensic digital analysis have been pivotal in determining timelines and associating suspects with crimes with high certainty. In commercial and civil disputes, digital contracts and communication trails clarify and offer little scope for interpretive ambiguity. All in all, Bharatiya Sakshya Adhiniyam, 2023's acceptance of electronic records is a step in the direction of a more contemporary, effective, and transparent judicial process. With technology, the law is in a position to provide speedy justice while also ensuring the authenticity and integrity of evidence on which it is grounded.

#### Practical and Technological Challenges of electronic records

Although the Bharatiya Sakshya Adhiniyam, 2023 has established an advanced legal framework for admissibility of electronic records, the practical and technical environment poses multiple challenges that need to be dealt with to achieve its maximum extent. A big hurdle is the infrastructure gaps that continue to exist in lower courts throughout the nation. Most district and subordinate courts continue to lack fundamental digital amenities like stable internet connectivity, digital display systems, secure data storage solutions, and upgraded computers. These restrictions hamper the hassle-free submission, scrutiny, and preservation of electronic records. Even if there is elementary digital infrastructure in place, the lack of standardized computer systems or compatible tools for software usage frequently results in inconsistencies in the management of digital evidence. In addition, the use of physical printouts of computer documents—defeating the very aim of the recognition of e-records—remains rampant in most courts because of technological unreadiness.

Cybersecurity threats and data breaches are another major challenge. Digital evidence is prone to hacking, unauthorized access, and tampering, especially when not stored and transmitted via secure, encrypted systems. With the increasing number of ransomware attacks and data hijacking, the judiciary is saddled with the herculean task of guaranteeing the security of sensitive legal information. Incidents

do not only threaten the integrity of individual cases but also undermine the confidence of the public in the judicial system. The lack of secure, centrally managed digital evidence management systems further compounds the problem, leaving the courts reliant on ad-hoc storage mechanisms or third-party hardware with uncertain security measures. At the same time, there is a critical need for technical expertise and training among the legal profession, including judges, lawyers, and court staff. The subtleties of metadata, hash functions, blockchain-backed documents, or digital forensics demand specialist knowledge with which many within the legal community are not familiar.

Without adequate training, judges could find themselves at a loss to determine the authenticity of complex digital records or correctly interpret expert evidence. Lawyers with no technical expertise can similarly fail to present or challenge electronic evidence properly, leading to miscarriages of justice. Although higher courts and national institutions might have access to digital forensics professionals, this is frequently not the case for local jurisdictions. Complementary training schemes and incorporation of technical professionals within court procedures are essential measures required to close this knowledge gap.

Finally, data protection and privacy issues have come into play more strongly in recent times, especially in instances relating to personal communications, biometric information, surveillance records, or social media and cloud data. The admissibility of such records has to be weighed against a person's privacy right as a fundamental right under Indian constitutional law. Courts have to exercise care in verifying that digital evidence is obtained legally, without infringing on data protection principles. The absence of a comprehensive data protection act in India further adds to this complexity, wherein it's hard to define clear parameters on the admissibility and utilisation of sensitive digital information. In summary, even though the Bharatiya Sakshya Adhiniyam has established a progressive legal environment, it is crucial to meet these practical and technological challenges in order to ensure that electronic records are not only legally acceptable, but even more importantly, utilized effectively and justly within the judicial system.

## **2. Conclusion**

The Bharatiya Sakshya Adhiniyam, 2023 marks a watershed moment in the modernization of India's evidentiary laws, especially in the context of recognizing electronic records as credible and admissible evidence in judicial proceedings. In a society increasingly driven by digital communication, electronic transactions, and online platforms, the move to formally incorporate e-records within the evidentiary framework is both timely and necessary. The provisions brought forth under this Act, and Section 63 with regard to the certification of electronic records, mark a conscious move towards establishing procedural transparency and certainty, hence safeguarding the purity of the judicial process. Right from emails and mobile texts to CCTV visuals and blockchain-supported contracts, electronic evidence is today at the center of a large majority of legal battles. The structure of the Act gives authority to courts to look at such evidence meaningfully, without relaxing the norms of fairness and due process.

Furthermore, judicial construction under the new law has revealed an incremental but increasing recognition of the nuance of digital evidence. Courts not only are requiring procedural compliance but are also considering in-depth the technical aspects of evidence—e.g., metadata analysis, hash authentication, chain of custody. This judicial exactness underlines that electronic documents can never be taken on face value, and need to be examined with the same, if not greater, caution as conventional evidence. Simultaneously, new technologies such as deepfakes, synthetic media, and tampering software raise new challenges, requiring the legal fraternity to update its tools and knowledge. Courts need to be vigilant, responsive, and technology-enabled to separate authentic evidence from tampered content.

Identification of electronic records has several advantages for the judicial system. It increases efficiency by accelerating the processing, exchange, and retrieval of evidence. It facilitates transparency by minimizing human bias and favoring use of system-generated, auditable data. It also supports improved documentation, safe storage, and long-term preservation of case files. But these advantages will only be fully achieved if systemic issues are resolved. Loopholes in digital infrastructure, particularly in lower courts, still inhibit the smooth implementation of the law. Cybersecurity threats, data breaches, and inadequate personnel further complicate the situation, jeopardizing the integrity of digital records and public trust in their application.

Furthermore, the conflict between utilizing digital evidence and maintaining respect for personal privacy continues to be a thorny issue. Without a general framework of data protection, the courts have to

navigate carefully in order not to infringe on essential rights in the exercise of their evidentiary discretion. Thus, though the Bharatiya Sakshya Adhiniyam, 2023 is a sound foundation, success will finally depend on long-term investment in technology, ongoing judicial training, and responsive legal reforms to keep pace with the dynamic digital environment.

To summarize, the insertion of electronic records into the Indian legal system in the Bharatiya Sakshya Adhiniyam, 2023 is not a technical improvement—it is a revolutionary change. It can extend justice to the masses, hold it accountable, and bring it in sync with the digital era, if complemented by infrastructural backup, institutional preparedness, and a firm commitment to equity.

Here is a list of suggested references you can include at the end of your article “Impact of Electronic Records as Evidence in the Judicial System under the Bharatiya Sakshya Adhiniyam, 2023”. These references combine statutory sources, case laws, and academic commentary for a well-rounded citation list:

## References

1. Bharatiya Sakshya Adhiniyam, 2023 – Ministry of Law and Justice, Government of India. <https://legislative.gov.in>
2. Indian Evidence Act, 1872 (Now Repealed) – Relevant for historical comparison of Section 65B and Section 63.
3. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 – Landmark Supreme Court ruling interpreting Section 65B certification requirements for electronic evidence.
4. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 – Supreme Court decision further clarifying mandatory certificate requirement under Section 65B.
5. State of Delhi v. Mohd. Afzal & Ors. (2003) – Known as the Parliament Attack Case, involving extensive use of digital evidence.
6. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 – Supreme Court ruling affirming the Right to Privacy as a fundamental right under Article 21.
7. Law Commission of India, Report No. 185 (2003) – “Review of the Indian Evidence Act, 1872” – Provided groundwork for electronic records in evidence law.
8. The Information Technology Act, 2000 – Especially Sections 65A and 65B (now mirrored under Bharatiya Sakshya Adhiniyam, 2023), and provisions on digital signatures and cybercrime.
9. CIS India (Centre for Internet and Society) – Reports and blogs on digital evidence, deepfakes, and privacy concerns in India. <https://cis-india.org>
10. National Judicial Academy (India) – Training material and seminars on e-courts and electronic evidence. <https://nja.gov.in>
11. Shreya Singhal v. Union of India, (2015) 5 SCC 1 – Case involving digital communication and interpretation of online content within legal frameworks.
12. Sinha, A. (2022). Digital Evidence and Indian Courts: A Technological Transition. *Indian Journal of Law & Technology*, Vol. 18.
13. Rajagopal, K. (2023). Electronic Evidence and Judicial Trends Post-2023. *Bar & Bench*.