The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

ELECTRONIC EVIDENCE IN COURTS: ADMISSIBILITY, CHALLENGES, AND JUDICIAL APPROACH IN INDIA

~ ***Hrithika Ranjan***

ABSTRACT

The growing digitalization of human conduct has made the use of electronic evidence essential in today's judicial process in India. This article focuses on the statute regarding the admissibility of electronic records in Section 65B of the Indian Evidence Act, 1872 and its succeeding sections of the Bharatiya Sakshya Adhiniyam, 2023. The development of the interpretation of the law is analyzed based on the landmark cases of Navjot Sandhu, Anvar P.V. and Arjun Panditrao. Further, the article outlines additional structural problems such as verification of authenticity, chain of custody requirements, and the failure of the certificate structure in dealing with algorithmic evidence and deepfake technologies. It is concluded from the article that even though the BSA represents a step forward legally speaking, there are still severe shortcomings in forensics.

INTRODUCTION

The ubiquitous use of digital technology in all aspects of human life has fundamentally transformed the form of evidence in the legal process. Contracts are entered into via emails, payments go through payment gateways, and personal conflicts take place via messaging applications. Under such conditions, it would be unwise for the court system to rely solely on legal framework governing evidence based on paper records. The laws on evidence in India, embodied in the Indian Evidence Act, 1872 (IEA hereinafter), could not cope with this challenge, which prompted the legislature to adopt Section 65B of the Information Technology Act, 2000. [1]

[1] Indian Evidence Act, 1872, § 65B, inserted by the Information Technology Act, 2000 (No. 21 of 2000), § 92.

The enactment of Bharatiya Sakshya Adhiniyam, 2023 constitutes the largest legislative overhaul of the Indian laws on evidence since independence. While the provisions of the BSA are mostly consistent with those of the IEA, it contains some additional clarifications regarding electronic records based on experience in the judiciary.[2] The article explores the laws related to the use of electronic evidence in Indian law, discusses the circumstances for their admissibility, provides an overview of judicial interpretations of the relevant issues in some landmark cases, and critically analyses the ongoing difficulties that need to be addressed.

MEANING AND NATURE OF ELECTRONIC EVIDENCE

In general, electronic evidence refers to any evidence presented in the form of data that can serve as proof. According to the IT Act, "an electronic record means data, record or data generated, image or sound stored, received or sent in an electronic form".[3] This definition is quite broad because it can refer to various types of electronic data including emails, text messages, metadata, CCTV footage, GPS locations, server logs, social media postings, cloud-stored documents, and algorithmic output.

Unlike documentary evidence, electronic evidence requires more consideration due to its malleability. On the one hand, a paper document bears the signs of manipulation that occurred, while electronic data can be manipulated without leaving any clues. On the other hand, electronic evidence is usually accompanied by metadata and cannot be considered independently from this context. Therefore, certain rules should be established that can be helpful in proving such information.[4]

LEGAL FRAMEWORK GOVERNING ELECTRONIC EVIDENCE IN INDIA

Prior to the IT Act, computer printouts were presented in the Indian courts as secondary evidence according to general rules of secondary evidence enshrined under the IEA. In Section 65B of IEA, there is a specific process whereby computer-generated printouts become admissible as evidence of any fact contained in it provided all the conditions of sub-section (2) are satisfied and are accompanied by a certificate issued under sub-section (4).[5]

The BSA adopts this procedure under Sections 61 to 63 of BSA with some amendments. According to Section 61 of the BSA, the term "document" is defined much wider than in IEA,

---

[2] Bharatiya Sakshya Adhiniyam, 2023 (No. 47 of 2023) [hereinafter 'BSA'], §§ 61–63.
[3] Bharatiya Sakshya Adhiniyam, 2023 (No. 47 of 2023) [hereinafter 'BSA'], §§ 61–63.
[4] Indian Evidence Act, 1872, §§ 3, 59; see also BSA, §§ 2(1)(d), 57.
[5] Indian Evidence Act, 1872, § 65A (inserted by IT Act, 2000); BSA, § 61(2).

which explicitly refers to electronic and digital documents, thus bringing such documents into the main scope of admissibility as primary rather than an exception under the statute. The certificate required under Section 63 of the BSA has basically the same composition as that of Section 65B(4). The difference lies in the provision of Section 63 of the BSA that allows the court to waive this certificate for justice's sake in certain cases where it could not be obtained, unlike under the IEA.[6]

The issue of admissibility of electronic evidence is also covered in the IT Act, 2000. Under Section 4 of the Act, electronic records shall be considered equivalent to traditional paper records. Section 65A of the IEA (BSA Section 61(2)) states that evidence relating to the contents of an electronic record may be given in accordance with the provisions of Section 65B.

SECTION 65B OF THE INDIAN EVIDENCE ACT

Section 65B applies on the basis of four limbs. Firstly, the document should be generated by a computer which has been regularly used during the period in question. Secondly, the information in the document must have been entered into the computer in the ordinary course of business. Thirdly, the computer must be functioning well, or any malfunction in the computer should not affect the data. Finally, the document should represent the data fed into the computer.

This provision was formulated to strike a balance between the necessity of quick investigation and the perils of digital fabrication. It is a provision that has proven highly controversial. The requirement that the conditions must be viewed from the standpoint of the person operating the computer during creation, and not from that of the party who wants to use the evidence, has posed major problems in criminal proceedings, particularly in cases where the computer

According to the Law Commission of India's 185th report on the Evidence Act, there were various shortcomings in the drafting of this provision. The provision had a high level of complexity which made it strategically difficult to comply with and Indian courts would benefit from adopting a simplified approach such as other jurisdictions have done.

CERTIFICATE REQUIREMENT UNDER SECTION 65B (4)

The section mandates the production of a certificate showing the identity of the electronic

[6] BSA, § 63, proviso.

requirements of sub-section (2) have been met. The certificate shall be made by an individual who holds an official position in connection with the operation of the concerned device.

This issue has never been considered in a straightforward manner by the Supreme Court. As far as State (NCT of Delhi) v. Navjot Sandhu[7] is concerned, the secondary evidence of electronic documents can be led by way of oral evidence in accordance with Sections 63 and 65 of the IEA considering Section 65B just to be a route among others. While it may sound pragmatic, it was rather unrealistic to insist on a certificate in every instance and at the same time it rendered the requirement of certification as discretionary in nature and hence irrelevant.

As decided by the Constitution Bench in Anvar P.V. v. P.K. Basheer[8], the approach adopted in Navjot Sandhu was firmly overturned by making it clear that Section 65B constitutes an exception to the ordinary rule in respect of secondary evidence as contained in Sections 63 and 65 of the IEA. The decision was applauded because of its success in reinstating doctrinal balance; however, the inflexibility of the same decision generated other issues, that is, the confusion that arose regarding the status of parties who would have great difficulty securing a certificate emanating from a computer used by the opposite party or even from an independent agency.

Such an issue was answered to some degree by the Constitution Bench in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal.[9] First and foremost, it reiterated that Section 65B (4) is indeed mandatory and that secondary evidence in respect of electronic records cannot be provided using Section 63 and 65. More importantly, it stated that in cases where a party finds it difficult to secure the necessary certificate, a court can ask for it through Section 165 of the IEA from the opposite party or any third party.

LANDMARK JUDICIAL PRONOUNCEMENTS

The judgments described below can be considered the major milestones in Indian law in terms of electronic evidence.

State (NCT of Delhi) v. Navjot Sandhu: The judgment passed in connection with the attack on Parliament case contained several observations related to electronic evidence, which were obiter dicta. Nonetheless, the Supreme Court ruled that the call records could be introduced in

[7] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
[8] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[9] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

court as secondary evidence via witness statements, and this approach was later proven to be wrong.

Anvar P.V. v. P.K. Basheer: This case involved a petition filed against a candidate in an election, where some CDs containing speech clips were intended to be introduced into evidence, but without a certificate. In this landmark Constitution Bench decision, the Court provided extensive analysis confirming that the statute at hand is a complete code concerning electronic evidence, that a certificate is compulsory for secondary evidence, and that original documents do not need a certificate.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal: This case further elaborated on the Anvar judgment by determining the point at which the certificate needed to be produced and confirming that a certificate can be compelled from a witness. In Justice Nariman's concurring opinion, an exhaustive discussion on the policy considerations behind the provision has been made. It highlights the importance of authentication in order to establish the reliability of electronic evidence.

Tomaso Bruno v. State of Uttar Pradesh[10]: This murder case dealt with the admission of CCTV footage in evidence, which was done without any certificate from the expert witness. Although the judgment in this matter had not relied on such evidence, some important observations about electronic evidence were made by the Court, which underlines the need for forensic integrity.

CHALLENGES IN ADMISSIBILITY OF ELECTRONIC EVIDENCE

The difficulties in admitting electronic evidence in Indian courts are many, and they add up to each other. Authenticity is the first hurdle. Whereas a written document would have a signature, a digital document does not carry any such indication. Hash checking, metadata analysis, and digital signatures are technical measures of authenticating electronic documents. The next difficulty is the possibility of altering the document without leaving any visible mark of alteration. Disputes over the authenticity of electronic records have been common in courts, and since no forensic examination protocol is required to be followed by the court, the disputable electronic records are often admitted based on nothing but an unsigned certificate.

The second difficulty arises from the practical problem of obtaining a Section 65B certificate. Where the record pertains to telecommunication companies, financial institutions, social media sites, or governmental organizations, it is possible that the relevant responsible officer does not

[10] Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178.

want, cannot, or will not give out the certificate. While a theoretical solution exists in the form of court-ordered delivery of the same, it can prove difficult to implement, especially in heavily packed trials.

The final challenge deals with the issues arising in relation to cloud computing. Where data is scattered across several computer locations across different jurisdictions, the question of determining which computer it originates from as mandated under Section 65B is virtually impossible.

CYBER FORENSICS AND CHAIN OF CUSTODY

Apart from section 65B compliance, the admissibility of electronic evidence has wider implications. For instance, even if a particular electronic record is admissible according to section 65B, it may be treated as possessing less probative value because of issues related to chain of custody. The chain of custody, as regards electronic evidence, means the systematic collection, preservation, analysis and transmission of electronic records in such a way that the integrity of those records is preserved right up to the stage of presentation of such records before the court.

More frequently, courts have begun evaluating chain of custody cases. In Vikram Singh v. State of Punjab, the Supreme Court reiterated the importance of establishing the integrity of electronic evidence through continuous custody. Any gap in the custody of the document for reasons of insecurity or improper handling may result in a reasonable doubt about integrity.

This relationship got even more tangled in light of the Supreme Court's comments in Shafhi Mohammad v. State of Himachal Pradesh, , in which a two-judge bench, apparently in conflict with Anvar, ruled that the need for a certificate should not be enforced rigorously when mobile phone evidence is seized from an accused person. Arjun Panditrao cleared up this additional confusion by emphasizing again the compulsory nature of the certificate, albeit pointing out that Shafhi Mohammad was a case per incuriam.

RECENT DEVELOPMENTS AND EMERGING ISSUES

In addition to the certificate dispensation provision, the other aspect of the BSA where electronic records get special consideration is in being recognized as primary evidence rather than secondary evidence which requires a special dispensation under the law, which suggests a paradigm shift.

New challenges relate to the admissibility of evidence resulting from use of artificial intelligence and algorithms. As intelligence agencies begin to employ facial recognition technology, predictive policing algorithms, and traffic monitoring via AI, courts are faced with the challenge of evaluating evidence from conclusions reached by algorithmic computation. The Section 65B structure which is based upon a human operator working on a computer is inadequate to address issues related to the epistemology of algorithms.

The emergence of deepfake technology also constitutes a different but related problem area. Deepfake video will not be visually obvious as such while being backed up by a technically legitimate certificate that would show that the file came from a functioning computer while not addressing whether the content has been manufactured or not. The certificate proves the procedure but not the legitimacy of the content.

There is also a question of encrypted communications and messaging applications with end-to-end encryption. In such cases when the interception of communications is performed by the police but does not include plaintext log files stored on servers, it is hard to prove the chain of custody and it is problematic to provide a Section 65B certificate since in this case, the computer is a private individual's device and not institutional property.

CRITICAL ANALYSIS

As one examines the progression of case law on the interpretation of Section 65B, what comes out most strikingly is not the doctrinal development itself, but rather its toll. The back and forth between Navjot Sandhu and Anvar, followed by the partial limitation on that doctrine through Shafhi Mohammad, and now Arjun Panditrao correcting the error of Shafhi Mohammad is two decades worth of unnecessary litigation during which both litigants and tribunals have been unable to rely on certainty regarding the law of the game.

The approach adopted by the Court in Arjun Panditrao, namely, that objections to non-compliance with the certificate requirement cannot be entertained by the appellate tribunal where not raised during the trial process, is a sensible approach; however, it cannot fix the problem that there was no compelling need for litigators under Navjot Sandhu to insist on compliance with the certificate requirement.

However, at a more fundamental level, the framework of certificates rests on the presupposition that the reliability of electronic evidence lies in whether the computer was working well and whether the information was being input regularly. This covers issues of hardware and process reliability, but says nothing about the accuracy, completeness, or authenticity of the information. An otherwise functioning computer can easily store manipulated information. Certificates prove processes, not truths. Unfortunately, the Indian courts have not taken into account this aspect, and neither does the BSA.

Moreover, the practical unavailability of the certificate in many instances, especially in the case where criminal defendants need to question electronic information provided by the prosecution, is another issue. Even though Arjun Panditrao allows the court to direct production, the burden of doing this will be placed on the defendant who is at a disadvantage in terms of information.

Lastly, there is no legislation that sets out guidelines for digital forensic examinations and provides for minimum standards in collecting, preserving, and analyzing electronic evidence.

CONCLUSION

Evidentiary use of digital evidence in India is a strange phenomenon where on the one hand it becomes imperative while at the same time it becomes questionable. It becomes imperative because all transactions and crimes have become digital. But they become questionable because the conditions under which their admissibility in court can be claimed have always remained a contentious area and the authenticity of evidence cannot be taken care of with mechanical certificatory procedures alone.

The BSA is an attempt to create an effective framework for handling digital evidence. Viewing digital evidence as a primary piece of evidence and providing limited discretion to forego a certificate are positive aspects of the law. However, what this Act fails to incorporate and needs incorporation through some other means in the future would be a well-defined framework for forensic reliability, proper chain-of-custody protocols, and proper interpretation of metadata and algorithmic processes.