



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

This is an Open Access article distributed under the terms of the Creative Commons Attribution- Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Admissibility of Electronic Records under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023: Practical Challenges before Trial Courts

SUHAIL SALAFI M

ABSTRACT

The rapid digitisation of communication, commerce, governance and personal activity has changed the form and the nature of evidence adduced before Indian courts.. Emails, call-detail records, closed-circuit television footage, mobile-phone extractions, social-media messages, cloud data, server logs and electronic contracts now feature regularly in civil and criminal proceedings. The Bharatiya Sakshya Adhiniyam, 2023 (“BSA”)¹, was enacted on 25th December 2023 and was brought into force on 1st July 2024, updates India’s law of evidence by explicitly acknowledging the existence of electronic and digital records, and by replacing the framework provided by sections 65A and 65B of the Indian Evidence Act, 1872 (“IEA”) with new provisions (sections 61–63 of the BSA).

Section 63 is the key provision regarding the admissibility of electronic records produced as computer output. While largely retaining the basic principles of section 65B of the IEA, it contains significant modifications, including an acknowledgment of the role of intermediaries, a reference to communication devices and a certificate-based formulation incorporating both the person responsible for the relevant device or activity and an expert.²

Whilst many of these developments are designed to serve reliability, they have introduced practical challenges to trial courts. Conflicts arise over the difference

¹ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 1, 61–63 (India); Ministry of Home Affairs, Notification No. S.O. 849(E), Gazette of India, Extraordinary, pt. II, sec. 3(ii) (Feb. 23, 2024) (appointing July 1, 2024 as the date on which the Act came into force).

² Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63(3)–(4), sch. (India).

between primary and secondary electronic evidence, certification requirements, identification of the proper certifier, retention of metadata, possession, cloud storage, third-party possession of devices and production of certificates late. This paper analyses the statutory regime provided by section 63, the continued applicability of Supreme Court decisions under section 65B of the IEA and the practical difficulties confronting trial courts.

It argues that the language used in section 63 should be interpreted as a reliability based provision, not just a simple exclusionary statement of reliability. Courts hearing charges need to adopt a structured approach to evidence in order to preserve the protective evidentiary rights and avoid procedural irregularities which could frustrate the introduction of reliable electronic record items. The paper then concludes with a series of recommendations in relation to judicial case management, standardisation of certificates, forensic preservation protocols and other guidance in relation to expert participants..

KEYWORDS: electronic evidence, Bharatiya Sakshya Adhiniyam, section 63, section 65B, digital records, certificate, trial courts, chain of custody.

INTRODUCTION

The evidentiary landscape of Indian litigation has changed substantially due to the fact that facts are increasingly created, stored and communicated electronically. A transaction may be recorded by an electronic invoice, an alleged threat may be sent by an encrypted messaging application, a person's movement may be established by location data and a contractual relationship may be evidenced by electronic correspondence. In criminal trials, prosecution cases may rely upon CCTV footage, call-detail records, mobile-phone data, social-media posts, computer files, digital photographs and forensic reports.

The legal implementation of such evidence into criminal proceedings therefore raises critical issues of proof and the prevention of misuse. Electronic records are inherently more susceptible to tampering and forgery than are paper-based records, since they may be copied with no perceivable loss of quality, manipulated in ways that often leave no trail, generated by default by third-party applications, and stored on a range of devices, or across jurisdictions.

The BSA answer to these challenges by explicitly referring to electronic and digital records in the definition of "document". Its illustrations recognise emails, server logs,

computer and smartphone documents, messages, websites, locational evidence and voice-mail messages as documents.³ Section 61 further provides that an electronic or digital record cannot be denied admissibility merely because it is electronic or digital subject to section 63. This legislative approach confirms that electronic evidence is not inferior in legal status to conventional documentary evidence.

Section 63 prescribes conditions concerning the manner in which a computer output was produced, the regular use and functioning of the device, the ordinary-course input of information and the certification of the record. The provision attempts to ensure that a printout, copied file, exported database or other computer output is sufficiently connected to a functioning system and reliable process.⁴

The central research question is whether section 63 provides trial courts with a workable mechanism for determining the admissibility of electronic records. The issue is of great importance because excessive technicality may exclude reliable evidence whereas laxity may allow in forged or unreliable material. This paper studies that tension and proposes a practical framework for trial courts.

STATUTORY FRAMEWORK

RECOGNITION OF ELECTRONIC RECORDS

Section 2(1)(d) of the BSA defines a document broadly and expressly includes electronic and digital records.⁵ Its illustrations refer to emails, server logs, records stored on computers, laptops or smartphones, messages, websites, location evidence and voice-mail messages. Section 2(1)(e) includes within “evidence” statements given electronically that the court permits or requires witnesses to make, as well as documents, including electronic and digital records, produced for the court’s inspection.

Section 61 establishes the general principle that an electronic or digital record has the same legal effect, validity and enforceability as any other document, subject to section

³ Id. § 2(1)(d) & illus.

⁴ Id. § 63(1)–(4).

⁵ Id. § 2(1)(d).

63.,⁶ At the same time, the reference to section 63 preserves the special safeguards applicable to computer-generated or computer-stored material.

PRIMARY AND SECONDARY ELECTRONIC EVIDENCE

Section 57 defines primary evidence as the document itself produced for the inspection of the court.⁷ It contains specific explanations dealing with electronic records. Where a record is created or stored simultaneously or sequentially in multiple files, each such file may constitute primary evidence. Similarly, where a video recording is simultaneously stored and transmitted or transferred, each stored recording may constitute primary evidence.

These provisions create an important distinction. If the original device or original electronic record is produced before the court, the party may rely upon primary evidence. If, however, the party produces a printout, screenshot, copied file, exported report, compact disc, pen drive or other computer output in substitution for the original, section 63 becomes central.⁸

A CCTV system may store footage on a digital video recorder, while a pen drive supplied to the investigating agency may contain a copied version. A cloud account may not have a single physical “original” accessible to the producing party. Courts must therefore identify the source record, the manner of extraction and the relationship between the original and the tendered copy.

CONDITIONS UNDER SECTION 63

Section 63(1) provides that information contained in an electronic record, when printed, stored, recorded or copied in an electronic form and produced by a computer or communication device, may be treated as a document and admitted without further proof of the original if the statutory conditions are satisfied.[scconline]

Section 63(2) contains four principal conditions:

1. The computer or communication device must have been regularly used during the relevant period to create, store or process information for activities regularly carried on by the person having lawful control over it.

⁶ Id. § 61.

⁷ Id. § 57.

⁸ State of Karnataka v. T. Naseer, 2023 INSC 976, ¶¶ 30–34 (India).

2. Information of the kind contained in the record, or information from which the record is derived, must have been regularly fed into the device in the ordinary course of those activities.
3. The computer or any other communications device had to have been operating normally during the relevant period unless it did not operate normally and the malfunction did not affect the electronic record or the accuracy of its contents.
4. The record must reproduce or be derived from information fed into the device in the ordinary course of the relevant activity.

Section 63(3) deals with situations in which the activity is performed through multiple computers or communication devices. All such devices may be treated as constituting a single computer or communication device for the purposes of the provision.

This is a significant development because modern data is rarely confined to one machine. Banking records may pass through customer devices, servers, payment gateways and intermediary systems. Messaging data may involve a phone, application server and cloud backup. CCTV footage may be recorded, compressed, stored and exported through several interconnected devices.

CERTIFICATION REQUIREMENT

Section 63(4) requires a certificate to be submitted along with the electronic record each time it is submitted for admission. It must provide appropriate particulars of the device or devices involved and address the statutory conditions under section 63(2). It must purport to be signed by the person in charge of the computer or communication device or the management of the relevant activities, as appropriate, and an expert.

The BSA Schedule prescribes a certificate format divided into Part A and Part B. Part A is generally intended to contain information supplied by the party producing the record, while Part B concerns technical details supplied by an expert. The requirement of expert participation is one of the most important practical changes from the earlier section 65B framework.

The certificate is not intended to prove every fact contained in the electronic record. It primarily establishes the conditions under which the computer output was generated and the reliability of the relevant system.

JUDICIAL DEVELOPMENT UNDER THE EARLIER LAW

ANVAR P.V. V. P.K. BASHEER

Before the enactment of the BSA, the Supreme Court in *Anvar P.V. v. P.K. Basheer* held that electronic records produced as secondary evidence must comply with section 65B of the IEA.⁹ The Court treated the certificate under section 65B(4) as a mandatory requirement for admissibility of computer-based secondary evidence. It also clarified that the ordinary rules concerning documentary evidence could not be used to bypass the special procedure prescribed for electronic records.

The decision was important because it replaced uncertainty with a specific statutory method. At the same time, strict application of the certificate requirement created difficulties where the producing party did not control the device or where the certificate could only be obtained from a service provider.

ARJUN PANDITRAO KHOTKAR V. KAILASH KUSHANRAO GORANTYAL

In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, the Supreme Court reaffirmed that the certificate requirement under section 65B was mandatory for secondary electronic evidence.¹⁰ The Court distinguished between the original electronic record contained in the original computer or device and copies made from that record. A certificate was unnecessary when the original electronic record itself was produced as primary evidence.

The Court also held that the certificate could be produced at a later stage where the trial had not concluded, subject to the court ensuring that the opposing party was not prejudiced. The Court emphasised that the certificate is a procedural safeguard and that courts should not automatically allow reliable evidence to be excluded where the defect can be cured.

PRACTICAL CHALLENGES BEFORE TRIAL COURTS

IDENTIFYING THE NATURE OF THE RECORD

The first challenge is classification. Often, parties refer to a document as “electronic evidence” without clarifying if it is an original or a copy, A screenshot, printout, screen recording, pen drive, exported chat, forensic image and server-generated report may all contain similar information but may have different evidentiary characteristics.

⁹ *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473, 491–93 (India).

¹⁰ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1, 23–25 (India).

Trial courts should require the producing party to specify:

- the original source of the information;
- the device or system on which it was first stored;
- the method by which it was extracted or copied;
- whether the tendered record is complete or selective;
- whether metadata is available; and
- whether the original device remains available for inspection.

Without classification, courts may either demand admit a secondary copy without the safeguards of section 63.

DETERMINING THE PROPER CERTIFIER

Section 63 requires certification by the person in charge of the relevant computer or communication device or the management of the relevant activities, as appropriate, together with an expert¹¹.

For a bank's transaction database, the relevant person may be an information-technology officer, records custodian or authorised manager. For CCTV footage, it may be the security manager, system administrator or person responsible for the premises. For a social-media message, the platform provider may control the relevant system, while the individual litigant controls only the receiving device. For a cloud account, the account holder may possess access but not control the underlying servers.

A mechanical insistence that the certificate can only come from one particular defined by the owner of the platform would frustrate proof beyond reasonable doubt. On the other hand, allowing any certificate that comes from someone not familiar with the system would defeat the very purpose of the statutory certification. The courts must instead be looking at the functional responsibilities. The certificate should explain the certifier's relationship with the device, system or activity and the basis of the certifier's knowledge.¹²

¹¹ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63(4)(c), sch. (India).

¹² *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1, 29–32 (India).

EXPERT CERTIFICATION AND INSTITUTIONAL CAPACITY

The requirement of the expert is aimed at promoting technical reliability, but he poses the problem of their availability, independence, and qualifications. Trial courts have the opportunity to rely on certificates from private consultants, company directors, police staff, forensic laboratories, or technical officers. BSA does not respond to the question of which level of expertise is considered satisfactory.

According to section 39¹³, expert opinion is relevant when the court is obliged to form an opinion on science, technology, or another special field. Otherwise, an expert's opinion may be presented, but it is not required. The judge should examine whether the expert analyzed a particular device submitted to him.

A certificate should be regarded as an institution-dependent evidence. In case of reasonable suspicion concerning the authenticity of a certificate, the expert should testify in court and be subjected to cross-examination. On the other hand, an official record with an adequate explanation should not require detailed justification simply because of the fact of being an electronic document.

CHAIN OF CUSTODY

Electronic evidence is vulnerable to alteration at every stage: seizure, transportation, examination, copying, storage and presentation.¹⁴

A proper chain-of-custody account should identify:

- the date, time and place of seizure or acquisition;
- the person who seized or received the device;
- the condition of the device;
- whether it was powered on or off;
- the method of imaging or extraction;
- hash values or equivalent integrity checks;
- each transfer of possession;
- the location and conditions of storage; and
- the person who produced the record in court.¹⁵

¹³ Id. § 39.

¹⁴ *Arjun Panditrao Khotkar*, (2020) 7 S.C.C. at 40–41.

¹⁵ National Judicial Academy, Digital Forensics Collection, Preservation and Appreciation of Electronic Evidence 17–22 (2022).

Trial courts often receive a certificate that describes the computer system but says little about the period between acquisition and production. Section 63 focuses primarily on the production conditions of the computer output, but authenticity also depends on the preservation of the source record.

METADATA AND INCOMPLETE COPIES

Metadata may include such items as creation time, modification time, location, device identity, user information and the software used to create a file. A screenshot may contain little or no metadata.¹⁶ A forwarded message may conceal the origins of the message. A video extracted from a surveillance system may involve a different file format or may lose system information.

The issue may be the weight to be given to the record and its authenticity. Weight and authenticity are matters for the court. The court will be concerned whether the absence of metadata goes to the root of the matter in dispute and whether technical examination of the record is relevant.¹⁷

Section 33 of the BSA provides rules about statements which form part of a conversation, document, electronic record, book or series of letters or papers. Courts must ensure that the extract tendered is not misleading because of the withholding of relevant context. It is not enough that the extract is admissible.

CLOUD STORAGE AND INTERMEDIARIES

Modern records may be created or stored in the cloud, online marketplaces, payment gateways and messaging intermediaries. Section 63(3) expressly recognizes intermediaries and permits that multiple computers or communication devices can be considered a single system. This is a helpful provision in addressing distributed technologies.¹⁸

Nevertheless, there remains a practical concern: the requesting party may have no control over the servers of an intermediary. It may have the capacity to download but

¹⁶ Arjun Panditrao Khotkar, (2020) 7 S.C.C. at 40–41.

¹⁷ Id.

¹⁸ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63(3) (India).

lack the ability to get a certificate from the provider.¹⁹ The court may consider using summons, judicial direction, expert examination or any other means permitted by law to obtain the provider records.²⁰

MOBILE PHONES AND PRIVATE DEVICES

A phone can contain a message received from another phone, a downloaded file, an automat-generated location history and a screenshot made by the user. All are different evidentiary pathways.

The court may not presume that possession of a phone establishes the authorship of each item found on it. Section 63 deals with the reliability of the computer output, but authorship and attribution require further evidence in the form of admissions, subscriber records, witness testimony, device linkage, account credentials or forensic analysis.²¹

LATE PRODUCTION OF CERTIFICATES

Earlier Supreme Court decisions suggests that a certificate may be permitted to be filed before the trial concludes, subject to the prevention of prejudice. Section 63 specifically provides that the certificate is to be submitted together with the record in each case where it is submitted for admission²². This specification may stimulate greater front-loaded compliance with the BSA.

Nonetheless, trial courts must distinguish between a willful withholding, an incurable failure of proof and a curable omission. If the other party has received the record, can inspect the device and can cross-examine the certifying witness, late production may be permitted with appropriate safeguards. If late production alters the substance of the record, denies the other side a meaningful opportunity to reply or occurs after the close of trial, more stringent consequences may be justified.

¹⁹ Arjun Panditrao Khotkar, (2020) 7 S.C.C. at 29–32.

²⁰ 37. Id. at 29–32.

²¹ See Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473, 492–93 (India).

²² Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63(4) (India).

WEIGHT AND ADMISSIBILITY

Section 63 determines whether a computer output is capable of being introduced into the evidentiary record. Once admitted, the court must weigh its probative value.

For example, an authenticated screenshot may prove the existence of an image in a particular device, but not the authorship of the work or the truth of the facts contained in the image. A certified call-detail record may show that a number was associated with a tower at a particular time, but may not in and of itself prove possession of the phone. A properly certified email may show that a message was sent and received, but the contents are subject to interpretation.

Trial courts should avoid the temptation to use the certificate requirement to substitute for an evaluation of relevance, attribution, completeness and credibility.

A PROPOSED JUDICIAL FRAMEWORK

A proposed judicial framework can help trial courts apply Section 63 consistently.

First: classify the evidence

The court should identify whether the item comprises the original device or original electronic record, forensic image, direct copy, exported file, printout, screenshot, report generated from a database or expert report based on electronic material.

Classification tells us whether a certificate under Section 63 is required and what other proof may be required.

Second: identify the source and control

The court should identify who controlled the relevant device and whether the certifier has sufficient knowledge on that matter. The certificate must disclose the institutional relationship between the certifier and the record.

Third: examine statutory conditions

The court should confirm that the certificate covers regular use, ordinary course input, proper functioning and reproduction or derivation from information supplied to the system. A certificate just says that the printout is 'true and correct' may be insufficient if it fails to cover the statutory requirements.

Fourth: preserve integrity

The court should examine chain-of-custody material, hash values, forensic image, seals, logs and storage records if authenticity is in dispute. Scrutiny should be commensurate with the nature of the dispute and the importance of the record.

Fifth: separate admission from weight

After admitting the record, the court should separately consider questions of authorship, attribution, completeness, context, reliability and probative value.

Sixth: cure defects fairly

Where a defect is curable, the court may allow corrected certificate, recall of witness technical examination provided the opposing party gets adequate notice and opportunity to respond.

RECOMMENDATIONS

First, the judiciary should devise model checklists for electronic evidence, including source identification, the description of the device from which it was obtained, its method of extraction, data metadata, hash values, chain of custody, certification and disclosure to the opposing party.

Second, the Schedule certificate should be accompanied by indicative guidance for different classes of record, including CCTV, call-detail records, social-media material, cloud documents, institutional databases and mobile-phone extractions.

Third, While the judges do not have to become forensic experts, they should understand the difference between original data, forensic images, screenshots, metadata and system-generated reports.

Fourth, investigation agencies, and institutional litigants should retain electronic material in standard forensic formats and keep contemporaneous acquisition logs: certificates generated years later are inherently more likely to be incomplete and controversial.

Fifth, The courts should assess the technical knowledge, methodology and relationship to the record of the expert concerned, and not just rely on his or her occupational qualification.

Sixth, procedural objections should be taken at the first reasonable opportunity. A party should not be allowed to raise an objection to a missing certificate at final argument, if the deficiency could have been raised earlier in the proceedings. Objections at an early stage allow amendment and avoid surprise.

CONCLUSION

Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 offers the main statutory mechanism for admitting electronic records created as computer output. Its efficacy will depend less on the text but the manner in which trial courts apply it. Equally, courts should not refuse reliable evidence because of a curable procedural flaw or the inability to get a certificate from an out-of-reach intermediary over whom they have no control. A good approach would be for courts to classify the record, establish the source, investigate the qualifications of the certifier, check the statutory conditions, determine the chain of custody and separately assess weight.

The Supreme Court's approach to a similar situation under the old law, particularly the distinction between primary and secondary evidence and potential for curing defects before conclusion of trial, provides useful guidance, subject to the wording of the BSA.²³

Ultimately, for section 63 to be a guarantee of reliability, and not an impediment to truth, it will require the co-operation of courts, lawyers, investigators, experts, public institutions and technology providers. Clear certificates, reliable forensic practices, early disclosure and reasoned judicial case management should ensure that digital evidence is both, technologically credible and procedurally fair.

²³ Id. at 25–27, 35–38.