

NOTES

# Admissibility of Electronic Evidence under the Bharatiya Sakshya Adhiniyam(BSA), 2023

Julie Nigam · 14 Oct 2026

---

## Introduction: Admissibility of Electronic Evidence

A WhatsApp message, CCTV clip, email, call-detail record, GPS location, online payment receipt or social-media post may become important in a case. In today's dynamic society, people communicate, shop, work, transfer money and store records digitally every day. A CCTV recording may show who entered a building, while a bank-server record may connect a payment to an account. But a digital file can be edited or copied. The court therefore asks, Is it admissible, and how much should it be trusted?

The **Bharatiya Sakshya Adhiniyam, 2023 (BSA)** responds to this reality. It recognises electronic and digital records as documents and gives them the same legal effect as other documents, subject to statutory safeguards. **Sections 61, 62 and 63**, read with the Schedule, explain how a printout, screenshot, recording, phone extract or cloud record can enter evidence. **Section 63** of **BSA** uses a certificate, device details and a hash value to help the court check the source and integrity of a computer output. This article explains how that mechanism works, how it differs from old **Section 65B** of **Indian Evidence Act, 1860** and how the 2026 Supreme Court ruling has clarified it.

## What counts as electronic evidence?

**Section 2(1)(d)** of **BSA** treats an electronic or digital record broadly. It includes data, records, images or sounds stored, received or sent electronically, including electronic records on computers, smartphones, servers and websites. **Section 2(1)(e)** of **BSA** includes electronic statements as oral evidence and electronic or digital records produced for the court's inspection as documentary evidence.

## Sections 61, 62 and 63

**Section 61** of **BSA** says an electronic or digital record cannot be rejected merely because it is electronic. Subject to **Section 63**, it has the same legal effect, validity and enforceability as another document. **Section 62** of **BSA** states that the contents of electronic records may be proved according to **Section 63** of **BSA**.

**Section 63** of **BSA** deals with admissibility of electronic records produced as computer output. A printout, copy, export, recording or storage output can be treated as a document and admitted without producing the original device if the statutory conditions are satisfied. This is an admissibility rule. It does not finally prove who created the message or whether its contents are true.

## **Admission is not the same as proof**

Evidence is admissible if the court can accept the record and consider it. Proof is concerned with its authenticity, authorship, accuracy, relevance and evidentiary weight. A certified screenshot can be tendered as evidence, but the court may still rule that the sender is not identified or that the content has been tampered with. The other side can challenge the metadata, the chain of custody, the ownership of the device, relevance and the possibility of fabrication.

In the case of ***State of Maharashtra v. Dr Praful B. Desai (2003)***, the Supreme Court accepted computer-generated material as documentary evidence.

## **The Old Regime: Sections 65A and 65B of Indian Evidence Act**

The Information Technology Act, 2000 amended the Indian Evidence Act by inserting **sections 65A** and **65B**. **Section 65A** required the courts to apply the special method found in **section 65B**. **Section 65B** laid down the conditions for admission of computer output as a document and the supply of a certificate.

In ***Anvar P.V. v. P.K. Basheer (2014)*** the Constitution Bench held that secondary electronic evidence must ordinarily satisfy **Section 65B**. In ***Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)*** it was reiterated that the certificate is ordinarily a condition for admissibility and the court can direct the person controlling the device to produce it.

## **The four conditions under old **Section 65B(2)****

The old rule required proof that:

1. the computer was regularly used for the relevant activity,
2. information of that kind was regularly fed into it in the ordinary course,
3. the computer was operating properly, or any defect did not affect the record, and
4. the output reproduced or was derived from information fed into the computer in the ordinary course.

Section 63(2) of BSA substantially retains these conditions.

# Admissibility of Electronic Evidence under the BSA, 2023

## 1 WHAT COUNTS?

Messages, emails, CCTV, call records, GPS data, payment records, social-media posts, phone, server and cloud records.



## 2 KEY SECTIONS

**Section 61:** electronic records cannot be rejected only because they are electronic.

**Section 62:** contents are proved under Section 63.

**Section 63:** printouts, screenshots, copies, exports and recordings may be admitted if the statutory conditions are met.

## 3 SECTION 63: FOUR CONDITIONS



Regularly used system



Information regularly entered



System working properly



Output derived from ordinary-course information

## 4 CERTIFICATE + HASH



**Part A:** source, device and method, signed by the person in charge.

**Part B:** technical source and integrity, signed by a qualified person.



**Hash value:** digital fingerprint that helps show whether the file changed.

## 5 ADMISSIBILITY ≠ PROOF



Admission only lets the court consider the record.

The court still checks relevance, authenticity, authorship, accuracy, tampering and chain of custody.

## 6 2026 RULING



**Pune Bar Association v. Union of India:**

Section 63(4) certificate and hash safeguards are constitutionally valid. Part B is not limited only to a Section 79A-notified expert if the court is satisfied about the person's expertise.

## Section 65B of IEA and Section 63 of BSA compared

The BSA does not discard the old approach. It modernises it in three important ways. First, [Section 63](#) expressly covers communication devices, semiconductor memory and electronic forms, making its language better suited to smartphones, networks and modern storage. Second, [Section 63\(3\)](#) treats computers, systems, networks, computer resources and intermediaries used together as one computer or communication system. Third, [Section 63\(4\)](#) requires a Schedule-based certificate with **Part A**, **Part B** and the hash value.

Under old [Section 65B](#), one responsible person signed the certificate. Under [Section 63](#), **Part A** is signed by the person in charge of the device or relevant activity, and **Part B** is signed by an expert. The certificate must accompany the electronic record each time it is submitted for admission. A certificate referring only to old [Section 65B](#) is not the proper document for evidence governed by the BSA, although the law applicable to a proceeding depends on the date and transitional provisions.

## Section 63 clause by clause

[Section 63\(1\)](#) covers information printed on paper, stored in optical or magnetic media or semiconductor memory, or produced by a computer or communication device. It permits the output without production of the original if Section 63 is satisfied.

[Section 63\(2\)](#) contains the four conditions. [Section 63\(3\)](#) recognises combined devices and intermediaries, such as a phone, cloud server and platform.

[Section 63\(4\)](#) requires a certificate identifying the record, explaining its production, giving device particulars and addressing Section 63(2). It's contents remain open to challenge.

## Part A, Part B and the Hash value

**Part A** is completed by the person in charge of the device or activity. It identifies the source, explains how the record was obtained and states that the device was under lawful control and functioning properly.

**Part B** is completed by an expert. It deals with the technical source and integrity of the record. [Section 39\(1\) BSA](#) recognises opinions of persons with special skill in science or another field. [Section 39\(2\) BSA](#) specifically recognises the opinion of an Examiner of Electronic Evidence

notified under **Section 79A** of the Information Technology Act.

A **hash value** is the digital fingerprint of a file. An algorithm such as SHA-256 converts it into a fixed string. If the file changes, the hash ordinarily changes. The Schedule requires the hash and algorithm so the court can compare the certified record with the record produced at trial.

## The ruling of the Supreme Court in 2026 was

In ***Pune Bar Association v. Union of India*** (22 May 2026) the Supreme Court upheld the constitutional validity of **Section 63(4) BSA** and its Schedule. It held that a requirement for a hash value has a rational connection with authenticity and integrity. Expert certification adds another safeguard and is not manifestly arbitrary.

The Court also clarified the expert issue. It did not hold that Part B can be signed only by an expert notified under **Section 79A** of IT act. Reading **Sections 39(1)** and **39(2)** together, it indicated that a person with special skill in computer science or cyber forensics may be accepted if the court is satisfied about the expertise. However, the Court kept the broader question open and refused to treat the contrary Madras High Court view as binding. The certificate and hash requirements are therefore settled, but the expert category may continue to develop.

## When is a certificate required?

A **Section 63(4)** certificate is normally required for a copy, printout, screenshot, export, pen drive, CD or server extract rather than the original device. The hash and chain of custody should be preserved.

If the original device is produced and a competent witness proves the record directly from it, the special computer-output route may not be necessary. This follows ***Arjun Panditrao***, although relevance, authenticity and foundation must still be shown. Remember, a screenshot is not the original record.

If the person controlling the device refuses to provide a certificate, the party may ask the court to summon that person or direct its production. Certification should not be treated as optional.

## Proving common digital records

For a mobile chat, preserve the phone, export the conversation, record device identifiers and obtain the certificate. For CCTV, identify the DVR or server, show that it functioned properly, preserve the relevant segment and maintain chain of custody. For call-detail, bank, cloud or social-media records, the provider or custodian should identify the system and explain extraction.

An expert may examine metadata, timestamps, device images and hash values. Expert opinion assists the court but does not replace its independent assessment.

## **Practical mistakes and transition issues**

Electronic evidence is often weakened by a blurred screenshot, failure to preserve the source, no certificate, an omitted hash algorithm or an unexplained chain of custody. Deepfakes make verification important.

The governing statute depends on the proceeding's date and transitional rules. Courts should not mechanically apply **Section 63** to every old case. The safest practice is to identify the applicable law, preserve the source, calculate the hash, obtain the Schedule certificate and disclose how the record was collected.

## **Conclusion**

The BSA gives electronic records the same legal status as other documents, but it demands a reliable method of proving computer outputs. For CLAT PG students it is important to remember the sequence of sections i.e. Section 61 recognises electronic records, Section 62 directs proof through Section 63, Section 63(2) retains four reliability conditions, Section 63(3) covers combined devices, and Section 63(4) requires the Schedule certificate, Part A, Part B and hash value.

2026 **Pune Bar Association** ruling upholds constitutionality of these safeguards. Electronic evidence is admissible if it is relevant, properly sourced, preserved and supported by the certificate. Therefore we can say that, admissibility is the door, authenticity and weight is what it proves.