



LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

[ISSN: 2583-7753]

Volume 4 | Issue 3

2026

DOI: <https://doi.org/10.70183/lijdlr.2026.v04.355>

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com

Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)

To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript [Click here](#)

CAN A CERTIFICATE DECIDE THE TRUTH? SECTION 65-B AND THE FUTURE OF ELECTRONIC EVIDENCE AFTER POORANMAL

Aditi Raikwar¹, Himanshu Kamlesh Mishra² and Harsh Chawla³

I. ABSTRACT

Indian courts have spent more than a decade insisting that a printed call record, a chat export or a video file is not evidence until a certificate says it is. The rule, traced to Section 65-B of the Indian Evidence Act 1872 and now carried into Section 63 of the Bharatiya Sakshya Adhiniyam 2023, was restated by the Supreme Court in Pooranmal v State of Rajasthan in March 2026. There, call detail records were excluded and a murder conviction was set aside because the prosecution had not proved the certificate and had relied instead on the oral testimony of telecom nodal officers. This paper uses that decision as a vantage point to ask what the certificate can and cannot do. It argues that the certificate is a gatekeeping device for admissibility and a weak proxy for authenticity, and that Indian law has asked more often whether the paperwork was completed than whether the record can be trusted. Tracing the line of authority from Navjot Sandhu through Anvar, Shafhi Mohammad and Khotkar, the paper examines the legislative reworking of the certificate in the Bharatiya Sakshya Adhiniyam, including the hash value and the expert's declaration, and the decision of the Supreme Court in Pune Bar Association v Union of India upholding that design in May 2026. It then tests the regime against the problems of access, forensic capacity, custody and synthetic media. The paper proposes a calibrated model built around early certification at source, a statutory chain-of-custody code, funded access to expert certification for indigent accused, a preserved judicial power to cure defects, and a clear separation between the certificate as a threshold and authenticity as a question of weight.

¹ 5th year B.Sc. LL.B. (Hons.) [Cyber Security] Student at National Law Institute University, Bhopal (India). Email: aditiraikwar.bscllb@nliu.ac.in

² 5th year B.Sc. LL.B. (Hons.) [Cyber Security] Student at National Law Institute University, Bhopal (India). Email: himanshukamleshmishra.bscllb@nliu.ac.in

³ 5th year BA. LL.B. (Hons.) [Cyber Security] Student at National Law Institute University, Bhopal (India). Email: harshchawla.ballb@nliu.ac.in

II. KEYWORDS

Electronic evidence; Section 65-B; Section 63 Bharatiya Sakshya Adhiniyam; admissibility certificate; Pooranmal.

III. INTRODUCTION

On 10 March 2026 a bench of Vikram Nath, Sandeep Mehta and NV Anjaria JJ of the Supreme Court acquitted a man who had been convicted of a murder committed in 2010 in Rajasthan. The prosecution case against him rested on three circumstances: a blood-stained shirt, a sum of money recovered from his house, and call detail records showing repeated contact with the co-accused around the time of the offence. The Court found both recoveries unreliable and held that the chain of custody of the forensic samples had been broken. On the call detail records it held that, without the certificate required by Section 65-B (4) of the Indian Evidence Act 1872, they were inadmissible, and that the oral evidence of the two telecom nodal officers who had been examined at trial could not stand in for the certificate.⁴

The decision restates settled law and does not break new ground, which is part of its interest. The rule that an electronic record led as secondary evidence must be accompanied by a certificate has been in force since *Anvar PV v PK Basheer* in 2014 and was reaffirmed by a bench of three judges in 2020. It nevertheless continues to decide criminal appeals, and since 1 July 2024 it has had a new statutory home. Section 63 of the Bharatiya Sakshya Adhiniyam 2023 keeps the certificate, requires it in a prescribed form with two parts, and adds a hash value and the declaration of an expert.⁵ In May 2026 the Supreme Court upheld that design against a constitutional challenge brought

⁴*Pooranmal v State of Rajasthan* 2026 INSC 217, 2026 LiveLaw (SC) 227 [26], [49]-[52] https://www.livelaw.in/pdf_upload/2026/04/18/2026-livelaw-sc-227-pooranmal-v-state-of-rajasthan-10-mar-2026-668387.pdf accessed 5 October 2026.

⁵Bharatiya Sakshya Adhiniyam 2023 (Act 47 of 2023), s 63 and the Schedule; Priyanka Agarwal, 'Electronic Evidence under the BSA, 2023' (*iPleaders*, 1 July 2026) <https://blog.ipleaders.in/electronic-evidence-under-the-bsa-2023/> accessed 5 October 2026.

by a bar association.⁶ The certificate has therefore been strengthened by Parliament and endorsed by the Supreme Court twice within a single year.

The title of this paper asks whether a certificate can decide the truth. On a close reading of the statute the answer is that it cannot, and that it was never meant to. A certificate is evidence of the matters stated in it, namely the identity of the record, the manner of its production, the particulars of the device and the working of the system that produced it.⁷ It does not establish that the content of the record is accurate, that the person who appears to have sent a message actually sent it, or that a recording has not been fabricated with tools that leave the hash value of the final file intact. Yet in practice the presence or absence of the certificate decides whether a court looks at the record at all. The distance between what the certificate certifies and what a court needs to know is the subject of this paper.

The question is timely for a second reason. *Pooranmal* arose from a trial held under the Evidence Act and was decided when the Bharatiya Sakshya Adhiniyam had already replaced it. The Court quoted the text of Section 65-B(4) and placed Section 63 of the new Act beside it in square brackets, as though the two were interchangeable.⁸ They are not. The new certificate is longer, is signed by two persons and carries a hash value. How far the case law built around the old provision carries over to the new one is a question that trial courts will now face every day.

The paper proceeds in five substantive parts. Part IV traces the law from the early tape-recording cases to the decision of the Supreme Court in *Arjun Panditrao Khotkar*. Part V examines *Pooranmal* in detail, including what it does not decide. Part VI sets out Section 63 of the Bharatiya Sakshya Adhiniyam, the legislative debate that preceded it and the decision in the *Pune Bar Association*. Part VII offers a critical appraisal of the certificate as an instrument for reaching the truth, and Part VIII proposes a calibrated model for the future. Part IX concludes.

⁶*Pune Bar Association v Union of India* Writ Petition (Civil) No 599 of 2026, 2026 SCC OnLine SC 1297, 2026 LiveLaw (SC) 551 (SC, 22 May 2026) <https://indiankanoon.org/doc/5836207/> accessed 5 October 2026.

⁷Indian Evidence Act 1872, s 65B(4), reproduced in *Pooranmal* (n 4) [49].

⁸*Pooranmal* (n 4) [49]-[52].

A. Research Objectives

This paper pursues the following research objectives:

1. To trace the development of the certificate requirement for electronic evidence in India from the tape-recording cases to *Pooranmal v State of Rajasthan* (2026).
2. To examine the reasoning of *Pooranmal* and to identify the questions it leaves open, particularly on curing a missing certificate and on the relationship between the old and the new law.
3. To evaluate Section 63 of the Bharatiya Sakshya Adhiniyam 2023, including the hash value and the expert's declaration, in light of *Pune Bar Association v Union of India* (2026).
4. To assess whether a certificate-based gate is a sound method of securing the authenticity and reliability of electronic evidence.
5. To propose a workable and fair model for the future regulation of electronic evidence in Indian courts.

B. Research Questions

The paper is guided by the following research questions:

1. How did the certificate under Section 65-B come to be treated as a mandatory condition for the admissibility of electronic records led as secondary evidence?
2. What did the Supreme Court decide in *Pooranmal*, and which questions about electronic evidence does the decision leave unresolved?
3. In what respects does Section 63 of the Bharatiya Sakshya Adhiniyam depart from Section 65-B, and what did the Supreme Court hold in the *Pune Bar Association*?
4. To what extent can a certificate establish the authenticity and reliability of an electronic record, and what does the regime leave to other safeguards?

5. What legal and institutional design should India adopt so that electronic evidence is neither admitted carelessly nor excluded for want of avoidable formalities?

C. Research Methodology

This paper adopts a doctrinal research methodology. It analyses primary legal materials, including the Indian Evidence Act 1872 as amended by the Information Technology Act 2000, the Bharatiya Sakshya Adhiniyam 2023, the Bharatiya Nagarik Suraksha Sanhita 2023, and the decisions of the Supreme Court of India on electronic evidence. The judgments in *Pooranmal*, *Arjun Panditrao Khotkar* and *Pune Bar Association* have been read from published copies of the full text. The doctrinal analysis is supplemented by the report of the Parliamentary Standing Committee on Home Affairs on the Bharatiya Sakshya Bill 2023 and by selected academic and professional commentary.

The paper does not use empirical data. Its conclusions about the practical operation of the certificate rule are drawn from reported decisions and from the structure of the statutory provisions, and should be read with that limit in mind. Reference is made to England and Wales in one place only, in Part VII, because the English experience of replacing a statutory reliability requirement with a presumption that computers work properly offers a useful caution against an overcorrection of the Indian position.

IV. THE ROAD TO A MANDATORY CERTIFICATE

A. Tape Recordings and the Common Law Inheritance

Before Parliament legislated for electronic records, courts treated them as an extension of documentary evidence and tested them for genuineness case by case. In *RM Malkani v State of Maharashtra* the Supreme Court admitted a tape-recorded conversation on the footing that it was relevant, that the voices were identified and that the possibility of erasure, addition or distortion had been excluded.⁹ *Ziyauddin Burhanuddin Bukhari v Brijmohan Ramdass Mehra* treated tape records as documents within the Evidence Act and insisted on proof of accuracy, and *Ram Singh v Col Ram Singh* set out the conditions

⁹*RM Malkani v State of Maharashtra* (1973) 1 SCC 471.

in fuller form, including identification of the voices, audibility, proper custody and the elimination of tampering.¹⁰ The method was functional. The question was whether the record was genuine, and the answer came from witnesses who could be cross-examined on the circumstances in which it was made and kept.

B. The Information Technology Act 2000 and Section 65-B

The Information Technology Act 2000 changed the method. Through its Second Schedule it amended the Evidence Act so that electronic records fell within the definition of evidence and of documents, so that oral admissions about the contents of an electronic record became irrelevant unless the genuineness of the record was in question, so that the contents of electronic records could not be proved by oral evidence, and so that Sections 65A and 65B were added.¹¹ Section 65A directs that the contents of electronic records may be proved only in accordance with Section 65B.

Section 65-B(1) deems information contained in an electronic record, whether printed on paper or stored, recorded or copied in optical or magnetic media produced by a computer, to be a document, and makes it admissible without further proof or production of the original, if the conditions in sub-section (2) are satisfied. Those conditions concern regular use of the computer under lawful control, regular feeding of information of that kind in the ordinary course of activity, proper operation of the computer during the material period, and derivation of the output from information so fed.¹²

Sub-section (4) provides that a certificate identifying the record, describing how it was produced, giving particulars of the device and dealing with the conditions, signed by a person occupying a responsible official position in relation to the device or the relevant activities, is evidence of any matter stated in it, and that it is enough for a matter to be stated to the best of the signatory's knowledge and belief.¹³

¹⁰*Ziyauddin Burhanuddin Bukhari v Brijmohan Ramdass Mehra* (1976) 2 SCC 17; *Ram Singh v Col Ram Singh* 1985 Supp SCC 611.

¹¹Information Technology Act 2000, Second Schedule, amending the Indian Evidence Act 1872, ss 3, 22A, 59, 65A and 65B.

¹²Indian Evidence Act 1872, s 65B(1)-(2).

¹³*ibid* s 65B(4); the text is reproduced in *Pooranmal* (n 4) [49].

C. From Navjot Sandhu to Anvar

The first major test came in *State (NCT of Delhi) v Navjot Sandhu*, arising from the attack on Parliament in 2001. The Court there allowed call records to be proved by secondary evidence under the general provisions of the Evidence Act even though no certificate had been produced.¹⁴ That view stood for nine years. In *Anvar PV v PK Basheer*, a bench of three judges held that Sections 65A and 65B form a special regime that displaces the general law on secondary evidence, that the certificate must accompany the electronic record when it is produced in evidence, and that the Evidence Act does not contemplate or permit proof of an electronic record by oral evidence where Section 65-B is not complied with.¹⁵

The Court explained the purpose of the safeguard as the protection of source and authenticity, since electronic records are more susceptible than paper to tampering, alteration and excision.¹⁶ It added that the genuineness of a record becomes a live question only once the record has been duly produced under Section 65-B, and that it is at that stage that the opinion of the Examiner of Electronic Evidence under Section 45A may be called for.¹⁷ The sequence matters for the argument of this paper. On the *Anvar* reading, the certificate comes first and authenticity comes after it.

D. Sonu, Shafhi Mohammad and the Relaxation of the Rule

Two decisions then loosened the rule. In *Sonu alias Amar v State of Haryana* the Court held that an objection to the mode of proof of call records, taken for the first time on appeal, was too late, which treated non-compliance with Section 65-B as a defect in the mode of proof that a party could waive by failing to object at trial.¹⁸ In *Shafhi Mohammad v State of Himachal Pradesh* a bench of two judges held that the certificate is

¹⁴*State (NCT of Delhi) v Navjot Sandhu alias Afsan Guru* (2005) 11 SCC 600.

¹⁵*Anvar PV v PK Basheer* (2014) 10 SCC 473 [14]-[18], as reproduced in *Pooranmal* (n 4) [50].

¹⁶*Anvar* (n 15) [16].

¹⁷*ibid* [17].

¹⁸*Sonu alias Amar v State of Haryana* (2017) 8 SCC 570; Abhinav Sekhri, 'The Supreme Court, 65-B Certificates, and Electronic Evidence' (*The Criminal Law Blog*, 20 July 2020)

<https://thecriminallawblog.in/2020/07/20/the-supreme-court-65-b-certificates-and-electronic-evidence/> accessed 5 October 2026.

a procedural requirement which may be relaxed where the party relying on the record is not in possession of the device that produced it.¹⁹

The fairness logic was plain enough, since a party should not lose evidence because a stranger to the case declines to sign a form. Taken together with *Sonu*, however, the two decisions meant that electronic evidence could enter the record without a certificate either because the party could not obtain one or because the opponent had not objected in time.

In the same period *Tomaso Bruno v State of UP*, decided by a bench of three judges, accepted proof of the contents of an electronic record through the general provisions on secondary evidence, following *Navjot Sandhu*. That observation was in any event obiter, because the CCTV footage and the call records were never placed on record, and *Khotkar* later held that it was not a correct statement of the law and overruled it.²⁰

E. Arjun Panditrao Khotkar

The conflict between *Anvar* and *Shafhi Mohammad* was referred to a bench of three judges in an election dispute in which video recordings of nomination proceedings were in issue. The decision in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* is the foundation of modern law.²¹ Ramasubramanian J delivered a separate opinion. The Court held that *Anvar* states the law correctly and that *Shafhi Mohammad* and some other decisions do not. Sections 65-A and 65-B are a complete code, and the general provisions on secondary evidence have no application to electronic records. The certificate is mandatory wherever the original device is not itself produced.

A person giving the certificate needs to attest only to the best of his or her knowledge and belief. Where a certificate is demanded and is not given, or is defective, the trial judge must summon the person concerned and require its production, and the requirement can be waived only where the certificate is not forthcoming despite such

¹⁹*Shafhi Mohammad v State of Himachal Pradesh* (2018) 2 SCC 801.

²⁰*Tomaso Bruno v State of UP* (2015) 7 SCC 178 [25]; *Khotkar* (n 21) [34]-[35]; Shobha Gupta, 'Legal Turmoil in Admissibility of Electronic Evidence Due to Interpretation of S 65B by Supreme Court (Part 3)' (*The Leaflet*, 15 October 2020) <https://theleaflet.in/supreme-court/part-3-legal-turmoil-in-admissibility-of-electronic-evidence-due-to-interpretation-of-s-65b-by-supreme-court> accessed 7 October 2026.

²¹*Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.

directions. In criminal cases the certificate should ordinarily be filed at the outset, although a court may permit later filing for good reason.

The Court also issued general directions to cellular companies and internet service providers to maintain call detail records and other relevant records for the concerned period, in tune with Section 39 of the Evidence Act, in a segregated and secure manner where such a record is seized during an investigation, those directions to hold until directions are issued under the applicable licences or under Section 67C of the Information Technology Act 2000. The licence conditions the Court noted required retention for one year only, and the Unified Licence was amended on 21 December 2021 to require archiving for at least two years.²²

The decision also confirms an exception that matters more in theory than in practice. Section 65-B regulates the computer output, which is a copy of the information. Where the original electronic record itself is produced, by bringing to court the device on which the information was first stored and proving it through its owner or operator, the record is primary evidence and no certificate is required.²³

The exception is rarely available in the cases where electronic evidence matters most. A call detail record sits on the servers of a service provider and cannot be carried into a courtroom, and a complainant's phone is often needed by its owner or held by the police. For records of this kind, which form a large part of the electronic evidence in criminal trials, the certificate is the only practicable route.

The Court's own formulation, as it was later quoted in *Pooranmal*, was that the certificate is a condition precedent to the admissibility of evidence by way of electronic record, and that oral evidence in its place cannot suffice because the requirement is mandatory.²⁴ By 2020, then, the doctrine had three features. The certificate was mandatory for secondary electronic evidence. A defect could be cured by court direction. And an oral substitute was unavailable. The second feature will become

²²*Khotkar* (n 21) [20] and [23]

²³*Khotkar* (n 21) [31]-[32].

²⁴*Khotkar* (n 21) [61], as quoted in *Pooranmal* (n 4) [51].

important in the discussion of *Pooranmal*, because the Court in that case applied the first and third without reference to the second.

V. POORANMAL: FACTS, HOLDING AND LIMITS

A. The Case Before the Court

The deceased was found dead in her husband's house, within the jurisdiction of Police Station Bijolia in Rajasthan, on the night of 2 and 3 March 2010. The husband, Ladu Lal, lodged the first report, but suspicion soon turned on him, and a disclosure statement made by him led the police to the appellant, Pooranmal. The investigating officer recovered a blood-stained shirt and a sum of Rs 46,000 on the strength of disclosures said to have been made by the appellant, and collected the call details of the mobile numbers of the two accused, from which the prosecution inferred continuous contact between them near the time of the incident.²⁵

The Additional Sessions Judge at Bhilwara convicted both accused under Sections 302 read with 34 and Section 201 of the Indian Penal Code on 8 February 2012, and the High Court of Rajasthan dismissed their appeal on 16 March 2018. The co-convict's special leave petition was dismissed in 2022. The appellant, who had not been able to appeal earlier because of poverty and lack of legal assistance, approached the Supreme Court through legal aid after a delay of 2749 days, which the Court condoned. The Court noted that the case against him differed from the case against the co-convict, who faced a reverse burden under Section 106 of the Evidence Act, because the case against the appellant rested purely on recoveries and call detail records.²⁶

B. The Three Circumstances

The Court began from the principles governing convictions on circumstantial evidence laid down in *Sharad Birdhichand Sarda v State of Maharashtra*, under which the circumstances must be fully established, must be consistent only with the guilt of the

²⁵*Pooranmal* (n 4) [8]-[11].

²⁶*ibid* [3]-[6].

accused and must form a chain so complete as to leave no reasonable ground for a conclusion consistent with innocence.²⁷ It then took the three circumstances in turn.

On the money, the Court observed that the packet was recorded as containing Rs 46,000 but that Rs 46,145 was counted in court, so that the very fact of the recovery was under a cloud, and that in any event recovery of currency without a proven nexus to the crime is not incriminating.²⁸ On the shirt, it found it improbable that a person at liberty for days would conceal a blood-stained shirt in an iron box when he could have burnt or washed it, and it held that the forensic report was worthless because the prosecution had not proved an unbroken chain of custody. The malkhana register and the testimony of the malkhana in-charge and the carrier constable were irreconcilable on when the samples had been sent to the laboratory and returned, and no reason for the return was given.²⁹

C. The Call Detail Records

The call detail records were the last of the three. The State argued that they had been proved by the nodal officers of the two service providers, who were examined as prosecution witnesses 23 and 24, and that the non-production of the certificate was therefore of no consequence.³⁰ The Court rejected the submission. It set out the text of Section 65-B(4), quoted the passages of *Anvar* that require the certificate to accompany the record and exclude oral proof, and quoted the passage of *Khotkar* describing the certificate as a condition precedent.

It then recorded that, admittedly, the certificate had not been proved by the prosecution, and held that in its absence the call detail records were inadmissible and could not be used to support the prosecution case.³¹ Having found none of the three circumstances established, the Court held that the prosecution had failed to prove a complete chain and acquitted the appellant.³²

²⁷*Sharad Birdhichand Sarda v State of Maharashtra* (1984) 4 SCC 116, applied in *Pooranmal* (n 4) [27]-[28].

²⁸*Pooranmal* (n 4) [29]-[33].

²⁹*ibid* [34]-[47]; *Karandeep Sharma alias Razia alias Raju v State of Uttarakhand* 2025 SCC OnLine SC 773.

³⁰*Pooranmal* (n 4) [22].

³¹*ibid* [49]-[52].

³²*ibid* [53]-[55].

D. What Pooranmal Decides and What It Leaves Open

The decision is clear on one point. Oral evidence of the employees of the custodian of the record, however senior and however familiar with the system, does not substitute for the certificate. That is the position taken in *Anvar* and *Khotkar*, and *Pooranmal* applies it to the most common kind of electronic evidence in Indian criminal trials, the call detail record.

On several other points the judgment is silent. First, it does not record whether the defence objected to the call detail records before the Sessions Court, nor whether the prosecution was asked to produce the certificate. The only contention noted on this point is that of counsel for the appellant before the Supreme Court.³³ The *Sonu* question, whether a late objection to the mode of proof is available, is therefore left where *Khotkar* left it. Sekhri has observed that *Khotkar* did not resolve it.³⁴ Secondly, the judgment does not discuss the curative route recognised in *Khotkar*, under which a trial judge who learns that a certificate has not been produced must summon the person concerned and require it.

Whether such a direction should have been given, or could still have been given, is not addressed. Thirdly, the judgment does not consider what the certificate would have shown. The call detail records were used only to show contact between two persons, and the appellant does not appear to have disputed their accuracy. The case therefore shows the certificate operating purely as a threshold.

Fourthly, the judgment is a decision on the old law. The Court notes the equivalent provisions of the new Act in square brackets throughout, and when it reproduces the text of Section 65-B(4) it pairs it with Section 63(4) of the Bharatiya Sakshya Adhiniyam.³⁵ The two provisions are not identical. The statutory certificate under Section 63(4) must be in the form prescribed in the Schedule and must be signed by an expert as well as by the person in charge of the device. The bracketed references

³³*ibid* [17].

³⁴Sekhri (n 18).

³⁵*Pooranmal* (n 4) [49].

are a convenience for the reader, and they should not be read as a holding that the cases decided under Section 65-B apply without adjustment to the new provision.

E. The Two Pooranmals

The title of this paper refers to a decision of 2026, but the name is not new in the law of evidence. In *Pooran Mal v Director of Inspection (Investigation) of Income Tax, New Delhi* the Court declined to import into Indian law an exclusionary rule of the kind associated with American constitutional practice, and treated the relevance and genuineness of the evidence as the governing question even where the search that yielded it was said to have been irregular.³⁶

The manner of collection went, at most, to weight. In the later decision, evidence that was relevant and, so far as the report shows, genuine was excluded for want of a statutory form. The contrast is not a contradiction. The earlier case, decided in December 1973 and reported in 1974, concerned the absence of a constitutional exclusionary rule, while Section 65-B is a specific statutory condition. But the two together show how unusual the certificate is within Indian evidence law, which has otherwise preferred to ask whether evidence is relevant and to leave questions of reliability to weight.

VI. SECTION 63 OF THE BHARATIYA SAKSHYA ADHINIYAM AND THE JUDICIAL ENDORSEMENT OF 2026

A. The Legislative Journey

The Bharatiya Sakshya Bill 2023 was introduced in the Lok Sabha on 11 August 2023 and referred to the Parliamentary Standing Committee on Home Affairs, which presented its 248th Report on 10 November 2023.³⁷ The first Bill was withdrawn and replaced by the Bharatiya Sakshya (Second) Bill 2023, which became the Act. The Act

³⁶*Pooran Mal v Director of Inspection (Investigation) of Income Tax, New Delhi* (1974) 1 SCC 345 (SC, 14 December 1973).

³⁷PRS Legislative Research, 'The Bharatiya Sakshya Bill, 2023' <https://prsindia.org/billtrack/the-bharatiya-sakshya-bill-2023> accessed 5 October 2026.

received the assent of the President on 25 December 2023 and was brought into force on 1 July 2024.³⁸

The Committee's report is relevant here because it identified the problems that the certificate was meant to address. It stressed that electronic and digital records are prone to tampering and recommended that records collected during investigation be handled through a proper chain of custody, a matter on which the Bill was silent.³⁹ It noted that the Bill treated electronic records produced from proper custody as primary evidence while retaining the certificate provision, and recommended that electronic records be proved in accordance with the certificate provision.⁴⁰

It also found that the draft certificate, as filled in by the person in charge of the device and by an expert, did not meet all the requirements of the admissibility provision, and recommended that the form be improved.⁴¹ A later PRS brief on the Second Bill observed that, although the Bill provided for admissibility, it contained no safeguards against tampering and contamination during the investigation process.⁴² The certificate in the Act as passed appears to reflect the Committee's concern with integrity, but the custody concern was left to other instruments.

B. The Structure of Sections 61 to 63

Section 61 of the Adhiniyam provides that nothing in the Act is to be applied so as to deny admissibility to an electronic or digital record on the ground that it is such a record, and that such a record has the same legal effect, validity and enforceability as any other document. Section 62 provides that the contents of electronic records may be proved in accordance with Section 63. Section 63 carries forward the architecture

³⁸PRS Legislative Research, 'Legislative Brief: The Bharatiya Sakshya (Second) Bill, 2023' [https://prsindia.org/files/bills_acts/bills_parliament/2023/Legislative_Brief_The_Bharatiya_Sakshya_\(Second\)_Bill_2023.pdf](https://prsindia.org/files/bills_acts/bills_parliament/2023/Legislative_Brief_The_Bharatiya_Sakshya_(Second)_Bill_2023.pdf) accessed 5 October 2026.

³⁹Department-Related Parliamentary Standing Committee on Home Affairs, *Two Hundred and Forty-Eighth Report: The Bharatiya Sakshya Bill, 2023* (Rajya Sabha Secretariat, November 2023) https://prsindia.org/files/bills_acts/bills_parliament/2023/SC_Report_Bharatiya_Sakshya_Bill_2023.pdf accessed 5 October 2026.

⁴⁰*ibid* para 4.8.1; PRS Legislative Research, 'Standing Committee Report Summary: The Bharatiya Sakshya Bill, 2023' (10 November 2023) <https://prsindia.org/billtrack/prs-products/standing-committee-report-summary-4276> accessed 5 October 2026.

⁴¹PRS, 'Standing Committee Report Summary' (n 40).

⁴²PRS, 'Legislative Brief: The Bharatiya Sakshya (Second) Bill, 2023' (n 38).

of Section 65-B with several changes.⁴³ The scope of the provision is widened to cover information stored in semiconductor memory and produced by any communication device as well as by a computer, which answers the old argument about whether a smartphone is a computer. The certificate must be in the form specified in the Schedule, and must be submitted at each instance where the record is submitted for admission. The certificate must be signed by the person in charge of the computer or communication device or the management of the relevant activities and also by an expert.⁴⁴

The Schedule is divided into two parts. Part A is to be completed by the party or the person in charge of the device and carries the identification of the record, the manner of its production, the particulars of the device, the statement on the conditions in Section 63(2), and the hash value of the record with the algorithm used. Part B is to be completed by the expert, who records the examination of the record and the matching hash value.⁴⁵ The hash value is a fixed-length string produced by passing a file through a mathematical function, and it changes if the file is altered in any respect. Its inclusion in the certificate gives the court a way of checking whether the file before it is the file that was certified.

C. Pune Bar Association v Union of India

A bar association challenged the constitutional validity of Section 63(4) and the Schedule, arguing that the requirements of a hash value in Part A and an expert's signature in Part B placed an undue burden on ordinary litigants. It also relied on a decision of the Madras High Court in *R v B & Anr* holding that Part B must be completed by an Examiner of Electronic Evidence notified under Section 79A of the Information Technology Act 2000. A bench of Surya Kant CJI, Joymalya Bagchi and Vipul M Pancholi JJ rejected the challenge on 22 May 2026, disposing of the petition at the admission stage and without issuing notice to the Union of India.⁴⁶

⁴³Bharatiya Sakshya Adhiniyam 2023, ss 61-63.

⁴⁴*ibid* s 63(4) and Schedule.

⁴⁵*ibid* Schedule, Parts A and B; Agarwal (n 5).

⁴⁶*Pune Bar Association* (n 6) <https://www.livelaw.in/pdf_upload/2026/05/27/pune-bar-association-v-union-of-india-676590.pdf> accessed 5 October 2026; *R v B & Anr* 2024 SCC OnLine Mad 6084.

The Court held that the requirements had a rational nexus with the object of the law. It described the hash value as an electronic fingerprint of the data and treated expert certification as an additional layer of assurance for secondary electronic evidence.⁴⁷ On the question of who may sign Part B, the Court read Section 39(1) and Section 39(2) of the Adhiniyam together. Section 39(2) makes the opinion of the Examiner of Electronic Evidence a relevant fact, but, unlike Section 63(4) and the old Section 65-B, it is not prefaced by a non obstante clause that would exclude the operation of Section 39(1) in the field of electronic records.

The Court observed that, on a harmonious reading of the two sub-sections, it is possible to hold that where a court is satisfied on the basis of unimpeachable material that a person has special skill and expertise in computer science and cyber forensics, the opinion of that person may be relevant as that of an expert and he may sign Part B. Because it was not inclined to admit the matter or to issue notice to the Union of India, the Court refrained from giving any conclusive opinion and expressly kept the question of law open. What it decided was that Section 63(4) is valid and that the Madras High Court's contrary finding on Part B is not to be treated as binding precedent.⁴⁸

Two features of the decision deserve notice. The first is that the Court treated the certificate regime as a legitimate legislative choice in the interest of authenticity, and was not inclined to dilute it because of its cost. The second is that the standard it suggested for experts, unimpeachable material of special skill and expertise, is open-textured and will be applied by trial courts in different ways. Because the petition was disposed of at the admission stage, without notice to the Union, and the question was expressly left open, the decision is a persuasive signal in favour of a wider pool of persons who may sign Part B rather than a ruling that widens it, and it says nothing about how a court is to verify their credentials.

⁴⁷ibid.

⁴⁸ibid [7].

D. The Transition Between Two Regimes

Section 170 of the Adhiniyam repeals the Evidence Act of 1872 subject to savings.⁴⁹ The decisions on Section 65-B continue to govern proceedings and steps taken under the old law, as *Pooranmal* itself shows. How the savings apply to electronic records tendered after 1 July 2024 in a trial that began earlier, and whether a certificate in the old form can suffice in such a case, are questions that will have to be decided by courts. Until then, a careful advocate will prepare a certificate in the prescribed Schedule form for any record tendered after the commencement date, whatever the age of the proceeding.

E. Reading the Two Decisions of 2026 Together

Pooranmal and *Pune Bar Association* were decided about ten weeks apart and point in the same direction. The first shows what follows when the certificate is not proved. The second shows that the Court regards the burden of the new, heavier certificate as justified by the need to guard against fabricated and altered records. A trial court reading the two together will take the message that the certificate is not negotiable and that its design is legitimate.

Neither decision, however, answers the questions that arise next. It is not clear whether a certificate that carries Part A but lacks Part B is a defective certificate that may be cured by a direction, or no certificate at all. It is not clear whether the timing rule in *Khotkar*, which allowed the certificate to be produced later in the trial with the leave of the court, survives the statutory requirement that the certificate be submitted at each instance where the record is submitted for admission.

And it is not clear how a party is to proceed where the record is held by a third party who will neither sign Part A nor allow an expert to examine the source. These questions will be decided in trial courts and High Courts over the coming years, and the answers will determine whether the new regime is workable or only strict.

⁴⁹Bharatiya Sakshya Adhiniyam 2023, s 170.

VII. CAN A CERTIFICATE DECIDE THE TRUTH? A CRITICAL APPRAISAL

A. What the Certificate Certifies

The text of the provision answers the question in the title. The certificate under Section 65-B(4) is evidence of the matters stated in it, and the matters it may state are the identity of the electronic record, the manner of its production, the particulars of the device and the conditions in sub-section (2).⁵⁰ Those conditions go to the regular operation of the system. They do not go to the accuracy of the information that was fed into it. A certificate may truthfully state that a server was working properly and that a chat export was produced from a given phone, and the chat may still be a record of a conversation in which a participant lied or in which the account was used by someone else.

The Court in *Anvar* saw this when it said that the genuineness of an electronic record is a question that arises once the record has been duly produced.⁵¹ The statute then supplies the further tools of opinion evidence and cross-examination. The practical difficulty is that the doctrine has come to concentrate attention on the first step. In *Pooranmal* the call detail records were excluded because the certificate was missing, and the judgment does not reveal any dispute about whether the records were accurate. The certificate did its work as a threshold, and there was no occasion to test what lay beyond it.

There is a related oddity in the way the rule treats witnesses. The nodal officers examined in *Pooranmal* could have been cross-examined on the very matters that a certificate would recite, namely how the records were generated, whether the system was working and whether the printout matched the source.⁵² The certificate is a written statement made without cross-examination. In preferring the document to the witness, the law prefers the less testable form of proof. Sekhri has argued that the text of Section 65-B supports a reading under which a party may either call a witness or

⁵⁰Indian Evidence Act 1872, s 65B(4); *Pooranmal* (n 4) [49].

⁵¹*Anvar* (n 15) [17].

⁵²*Pooranmal* (n 4) [22].

furnish a certificate, and that *Anvar* and *Khotkar* turned a rule about the kind of material covered by the provision into a rule about how its conditions must be proved.⁵³ The Supreme Court has not accepted that reading, and *Pooranmal* shows no sign of reconsidering it. The better view of the settled law is that it rests on the principle that where a statute prescribes a manner of proof, proof must be given in that manner or not at all, which *Khotkar* drew from an old English authority.⁵⁴ The principle explains the rule. It does not show that the rule serves truth-finding well.

The defence of the certificate deserves to be stated fairly. It fixes responsibility on a named person at an early stage. It gives the opposing party notice of the basis on which the record is tendered. It saves trial time that would otherwise be spent examining custodians on routine matters. And in a system in which police stations and trial courts handle large volumes of electronic material with variable care, a formal gate is a blunt but administrable tool. These are real advantages. They justify a certificate as a threshold, but they do not justify treating it as a proof of reliability.

B. The Hash Value, the Expert and the Meaning of Integrity

The Bharatiya Sakshya Adhiniyam strengthens the threshold by requiring a hash value and an expert. The strengthening is real, and *Pune Bar Association* is right that a hash value is an effective way of showing that a file has not changed since it was hashed. But the property it proves is narrow. A hash shows that the file in court is identical to the file that was hashed.

It says nothing about whether the file was authentic when it was hashed. A fabricated message thread, exported and hashed at the moment of fabrication, produces a perfectly consistent hash. The same is true of a synthetic audio recording. The hash anchors the record from the point of collection forward, and everything before that point depends on how the device was seized, handled and examined.⁵⁵

The same logic explains why the Court in *Pooranmal* was so exacting about custody of the physical samples. It held that the forensic report on the shirt was a worthless piece

⁵³Sekhri (n 18).

⁵⁴*Khotkar* (n 21) [61], as quoted in *Pooranmal* (n 4) [51].

⁵⁵See generally Stephen Mason and Daniel Seng (eds), *Electronic Evidence and Electronic Signatures* (5th edn, University of London Press 2021).

of paper because the prosecution could not account for the movement of the sealed articles between the police station and the laboratory.⁵⁶ The concern is the same as the concern that the hash value addresses for digital records: whether the thing examined is the thing seized. The difference is that for physical samples Indian courts have long asked for custody evidence, whereas for electronic records the law has asked for a certificate and has said much less about custody before the point of certification. The Standing Committee drew attention to this gap.⁵⁷

The expert's role raises a different problem. Part B is meant to add independent assurance, but the assurance is only as good as the expert's competence and independence. *Pune Bar Association* suggests that persons other than the notified examiners may sign, but leaves the question open, and the Court's reference to unimpeachable material as the test of competence leaves the practical content of the standard to individual courts. Without a published method for assessing credentials, there is a risk that Part B becomes a signature that can be bought rather than a check that can be trusted.

C. Access, Cost and Equality of Arms

The certificate rule has an uneven effect on the parties to a criminal case. In *Pooranmal* it benefited the accused, because the prosecution carried the burden of proving the records and could not do so. The appellant was poor, was unable to appeal for years and reached the Supreme Court through legal aid.⁵⁸ But the same rule can work against an accused who seeks to rely on electronic material, such as CCTV footage held by a third party, messages on a device the police have seized, or records held by a platform that will not respond to a private request.

The State can compel a telecom operator to produce records and can retain forensic experts. The accused usually cannot. Under *Khotkar*, a court may require the person in control of the record to supply the certificate, and the Bharatiya Nagarik Suraksha

⁵⁶*Pooranmal* (n 4) [36]-[44].

⁵⁷*Two Hundred and Forty-Eighth Report* (n 39); PRS, 'Legislative Brief: The Bharatiya Sakshya (Second) Bill, 2023' (n 38).

⁵⁸*Pooranmal* (n 4) [5]-[6].

Sanhita contains a power to order production of documents and other things.⁵⁹ The power is useful, but it presupposes a lawyer who knows how to invoke it and a court willing to stop the trial and use it.

The requirement of an expert's certificate in Part B adds cost. The Supreme Court has long held that legal aid is part of the guarantee of a fair procedure under Article 21 of the Constitution, and Article 39A directs the State to secure equal justice through free legal aid, an obligation the State cannot avoid by pleading financial or administrative inability.⁶⁰ If expert certification is a condition of admissibility, the State's obligation logically extends to making such certification available to those who cannot afford it. The present framework says nothing on the point.

D. The Timing Problem

A final difficulty is timing. In *Pooranmal* the missing certificate decided an appeal fourteen years after the judgment of the trial court. Whatever the explanation, the case illustrates the cost of discovering a defect in the proof of electronic evidence at the last stage of the process. *Khotkar* anticipated the difficulty by advising that in criminal cases the certificate should ordinarily be filed at the outset, and by requiring trial courts to take steps to obtain a certificate that has been demanded and not supplied.

The Adhiniyam adds that the certificate is to be submitted at each instance where a record is submitted for admission. If those instructions were followed consistently, defects would be found when they can still be cured. The facts of *Pooranmal* suggest that they were not followed, or that the point was not taken, at the trial.

E. Matching Formality to Dispute

A further feature of the rule is that it applies whether or not anyone disputes the record. In many criminal cases the accused has no quarrel with the fact that a call was made or a message was sent, and the contest lies elsewhere, in what the call or message meant. The Code of Criminal Procedure provides a procedure under which the

⁵⁹*Khotkar* (n 21) [43] and [50]; Bharatiya Nagarik Suraksha Sanhita 2023, s 94, corresponding to the Code of Criminal Procedure 1973, s 91.

⁶⁰*Hussainara Khatoon (IV) v Home Secretary, State of Bihar* (1980) 1 SCC 98; *MH Hoskot v State of Maharashtra* (1978) 3 SCC 544; *Khatris v State of Bihar* (1981) 1 SCC 627; Constitution of India, arts 21 and 39A.

genuineness of a document that is not disputed may be admitted and the document read in evidence without formal proof, and the Bharatiya Nagarik Suraksha Sanhita carries the procedure forward.⁶¹ Whether that procedure can be used for electronic records, and how it fits with the statement in *Khotkar* that the certificate is a condition precedent, has not been settled by the Supreme Court in the decisions discussed in this paper.

There is a case for allowing it, on conditions. Where integrity is not in dispute, insisting on a certificate with two signatures and a hash value adds cost and delay and tests nothing. The conditions would need to be strict, since an admission made carelessly by a lawyer at an early stage can prejudice an accused who understood neither the record nor its significance. An admission of that kind should be expressed, recorded and made with the assistance of counsel, and the court should retain the power to require a certificate where it has reason to doubt the record. The point is offered as a matter for consideration. It shows that the certificate is a rule of proof and that rules of proof can reasonably be matched to the real scope of the dispute.

F. A Cautionary Comparison

The English experience supplies a caution against overcorrecting. For some years the law of England and Wales required a statutory showing, in criminal proceedings, that a computer was operating properly before its output could be admitted. That requirement was repealed by an Act of 1999, on the recommendation of a report of the Law Commission published in 1997, the repeal coming into force on 14 April 2000, and the courts now proceed on a presumption that a computer was working properly unless there is evidence to the contrary.⁶²

The presumption has been criticised, and the Post Office Horizon litigation showed how a system with serious defects could be treated as reliable in prosecutions for years. In the civil proceedings that exposed the problem the court found that the

⁶¹Code of Criminal Procedure 1973, s 294; Bharatiya Nagarik Suraksha Sanhita 2023, s 330.

⁶²Youth Justice and Criminal Evidence Act 1999, s 60, repealing the Police and Criminal Evidence Act 1984, s 69; Youth Justice and Criminal Evidence Act 1999 (Commencement No 2) Order 2000, SI 2000/1034, art 2(a); Law Commission, *Evidence in Criminal Proceedings: Hearsay and Related Topics* (Law Com No 245, 1997).

system contained bugs, errors and defects, and the Court of Appeal later quashed the convictions of a number of sub-postmasters.⁶³

The lesson for India is not that the certificate should be abandoned. A rule that presumes reliability puts the burden of proving unreliability on the party who has the least access to the system. The Indian certificate at least compels the party relying on a record to identify the source and to state how the record was produced. The lesson is rather that neither a presumption nor a certificate is a substitute for adversarial testing of the system. Where the reliability of a computer system is in real dispute, the court needs access to the system itself, to its logs and to a competent expert, and a certificate signed by the system's operator is unlikely to resolve the matter.

VIII. TOWARDS A CALIBRATED MODEL FOR ELECTRONIC EVIDENCE

The analysis above points away from two tempting responses to *Pooranmal*. One is to treat the certificate as a proof of reliability and to extend it further, adding more signatures and more particulars. The other is to dismiss it as a technicality and return to the permissive position of *Navjot Sandhu* or *Shafhi Mohammad*. The evidence supports a more modest model, built around six choices.

The first is to keep the certificate as a threshold and to say so. Courts and practitioners should treat compliance with Section 63 as the condition on which a record is admitted, and should treat authenticity and weight as separate questions to be decided on the whole of the evidence. This is already the logic of *Anvar*, which puts the genuineness inquiry after the production of the record. It would help if courts, when admitting a certified record, recorded in terms that its admission does not establish its authenticity, and if the Adhiniyam were applied so that a record admitted on a certificate can still be challenged by cross-examination of the person who signed it and by opinion evidence on the device.

⁶³*Bates v Post Office Ltd (No 6: Horizon Issues)* [2019] EWHC 3408 (QB); *Hamilton v Post Office Ltd* [2021] EWCA Crim 577; Paul Marshall and others, 'Recommendations for the Probity of Computer Evidence' (2021) 18 Digital Evidence and Electronic Signature Law Review 18.

The second is to move certification to the source and to the beginning of the case. *Khotkar* advised that the certificate should ordinarily be filed at the outset of a criminal case. The Bharatiya Nagarik Suraksha Sanhita already requires the documents on which the prosecution relies to accompany the police report and to be supplied to the accused, and these provisions are the natural place to require that every electronic record relied on is accompanied by a certificate in the prescribed form.⁶⁴ In *Pooranmal* the investigating officer himself collected the call details from the service providers.⁶⁵ A standing protocol under which service providers return call detail records to investigating agencies with the Part A certificate and the hash value already attached would have avoided the failure in that case at almost no cost.

The third is a statutory chain-of-custody code for electronic records. The Standing Committee asked for one, and the later PRS brief on the Second Bill noted that the Bill contained no safeguards of this kind against tampering during investigation.⁶⁶ The Bharatiya Nagarik Suraksha Sanhita provides for audio-video recording of search and seizure and for the involvement of forensic experts in the investigation of serious offences, and these provisions could be used to build a protocol in which a device is seized, imaged and hashed on camera, with the hash value recorded in the seizure memorandum.⁶⁷ Such a protocol would address what the certificate cannot, namely the history of the record before it is certified, and it would apply to electronic records the same insistence on custody that *Pooranmal* applied to the blood-stained shirt.

The fourth is to build forensic capacity and to fund access to it. *Pune Bar Association* points towards a wider pool of experts who may sign Part B but leaves the question open, and a pool without a method of accreditation would in any event be no solution. States should maintain registers of accredited forensic examiners, with published criteria, so that courts can apply the standard of unimpeachable material consistently. For accused persons who cannot afford an expert, the cost of Part B and of any

⁶⁴Bharatiya Nagarik Suraksha Sanhita 2023, ss 193 and 230, corresponding to the Code of Criminal Procedure 1973, ss 173 and 207.

⁶⁵*Pooranmal* (n 4) [11].

⁶⁶*Two Hundred and Forty-Eighth Report* (n 39); PRS, 'Legislative Brief: The Bharatiya Sakshya (Second) Bill, 2023' (n 38).

⁶⁷Bharatiya Nagarik Suraksha Sanhita 2023, ss 105 and 176(3).

independent examination should be met under the legal aid framework, which follows from the constitutional position on fair procedure.

The fifth is to preserve the curative power, to use it early, and to match formality to the real dispute. The route recognised in *Khotkar*, under which a court summons the person in control of the record and requires the certificate, should be treated as continuing under Section 63. The corollary is that the court should decide the admissibility of an electronic record when it is tendered, and should not leave the point to be discovered on appeal.

A rule that objections to the certificate must be taken and decided at the stage of tendering, while leaving room for the court to relieve a party where a fair trial requires it, would resolve the uncertainty left by *Sonu* and would avoid acquittals such as that in *Pooranmal* resting on a defect that could have been remedied years earlier. Where the genuineness of a record is expressly admitted by an accused with the assistance of counsel, the court should consider whether the existing procedure for admitting undisputed documents can be used, so that formal certification is reserved for records whose integrity is actually in question.

The sixth is to prepare for synthetic media. The hash value and the expert's declaration were designed for a world in which the main risk is tampering with an existing file. They are less useful where the risk is the creation of a new and convincing record from nothing.

For audio and video evidence in particular, courts will need to ask about provenance, such as the source device, the metadata, the corresponding server-side records and the circumstances of recording, and not only about the certificate. This is a matter for judicial training and for rules of court more than for legislation, and the law should remain open to revision as the technology and the evidence of its effects develop. The Adhiniyam also treats electronic records produced from proper custody as primary evidence in certain circumstances, which sits uneasily with a certificate rule meant to apply to secondary evidence, and the relationship between the two should be clarified by the courts or by the Standing Committee when it next reviews the Act.

Table 1 summarises the model, setting each problem identified in this paper against the present position and the proposed response.

Table 1: Summary of the proposed model

Problem	Present position	Proposed response
Certificate treated as proof of reliability	A threshold of admissibility. Authenticity is a separate question (<i>Anvar</i>), but attention concentrates on the threshold.	Record that admission does not establish authenticity and keep cross-examination and expert opinion open.
Missing certificates discovered late	Filing at the outset is advised in criminal cases. In <i>Pooranmal</i> the defect decided an appeal fourteen years after the trial judgment.	Certify at source, file with the police report and decide admissibility when the record is tendered.
Custody before certification	Not covered by Section 63. The Standing Committee's concern was left to other instruments.	A custody protocol, with the hash value recorded at seizure on camera.
Expert capacity	Open question, with a persuasive signal that a person with special skill may sign Part B on unimpeachable material (<i>Pune Bar Association</i>).	State registers of accredited examiners with published criteria.

Problem	Present position	Proposed response
Access for indigent accused	No provision for the cost of Part B or independent examination.	Legal aid funding for expert certification and examination.
Synthetic media	Hash value and expert declaration are designed for tampering with an existing file.	A provenance inquiry developed through rules of court and judicial training.

IX. CONCLUSION

The Supreme Court's decision in *Pooranmal* confirms that a certificate under Section 65-B remains the price of admission for electronic records led as secondary evidence, and that oral testimony from the custodian will not do in its place. The decision is correct on the settled law and is consistent with *Anvar* and *Khotkar*. Its significance lies less in what it decides than in what it shows about the rule. The certificate was missing, the records were excluded, and a conviction that depended on them fell. At no point did the Court need to ask whether the records were true.

That is both the strength and the limit of the certificate. It gives the courts a clear and administrable threshold, it fixes responsibility on a named person, and it has now been strengthened by Parliament through the hash value and the expert's declaration and upheld by the Supreme Court in *Pune Bar Association*. But it certifies the manner in which a record was produced and not the truth of what the record says. A court that mistakes the one for the other risks admitting a well-certified falsehood, or excluding a true record because a form was not completed in time.

The model proposed in this paper keeps the certificate and puts it in its place. It would make the certificate a threshold and keep authenticity open, move certification to the source and to the start of the case, supply a custody code for the period before certification, pay for forensic capacity and for access to it, cure defects early, and

prepare for synthetic media. None of these steps requires a new statute of any length. Most can be taken through rules of court, investigative protocols and sustained judicial attention. The test of the regime in the years ahead will be whether the certificate helps courts to reach the truth, or only to decide which records they may look at.

X. BIBLIOGRAPHY

A. Primary Legislation

1. Bharatiya Nagarik Suraksha Sanhita 2023
2. Bharatiya Sakshya Adhiniyam 2023 (Act 47 of 2023)
3. Code of Criminal Procedure 1973
4. Constitution of India 1950
5. Indian Evidence Act 1872
6. Information Technology Act 2000
7. Police and Criminal Evidence Act 1984 (UK)
8. Youth Justice and Criminal Evidence Act 1999 (UK)
9. Youth Justice and Criminal Evidence Act 1999 (Commencement No 2) Order 2000, SI 2000/1034 (UK)

B. Cases

1. *Anvar PV v PK Basheer* (2014) 10 SCC 473
2. *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1
3. *Bates v Post Office Ltd (No 6: Horizon Issues)* [2019] EWHC 3408 (QB)
4. *Hamilton v Post Office Ltd* [2021] EWCA Crim 577
5. *Hussainara Khatoon (IV) v Home Secretary, State of Bihar* (1980) 1 SCC 98
6. *Karandeep Sharma alias Razia alias Raju v State of Uttarakhand* 2025 SCC OnLine SC 773
7. *Khatri v State of Bihar* (1981) 1 SCC 627

8. *MH Hoskot v State of Maharashtra* (1978) 3 SCC 544
9. *Pooran Mal v Director of Inspection (Investigation) of Income Tax, New Delhi* (1974) 1 SCC 345 (SC, 14 December 1973)
10. *Pooranmal v State of Rajasthan* 2026 INSC 217 (SC, 10 March 2026)
11. *Pune Bar Association v Union of India* Writ Petition (Civil) No 599 of 2026, 2026 SCC OnLine SC 1297, 2026 LiveLaw (SC) 551 (SC, 22 May 2026)
12. *R v B & Anr* 2024 SCC OnLine Mad 6084 (Mad)
13. *Ram Singh v Col Ram Singh* 1985 Supp SCC 611
14. *RM Malkani v State of Maharashtra* (1973) 1 SCC 471
15. *Shafhi Mohammad v State of Himachal Pradesh* (2018) 2 SCC 801
16. *Sharad Birdhichand Sarda v State of Maharashtra* (1984) 4 SCC 116
17. *Sonu alias Amar v State of Haryana* (2017) 8 SCC 570
18. *State (NCT of Delhi) v Navjot Sandhu alias Afsan Guru* (2005) 11 SCC 600
19. *Tomaso Bruno v State of UP* (2015) 7 SCC 178
20. *Ziyouddin Burhanuddin Bukhari v Brijmohan Ramdass Mehra* (1976) 2 SCC 17

C. Reports and Official Materials

1. Department of Telecommunications, Amendments to the Unified Licence and Other Licence Agreements (No 20-271/2010-AS-I (Vol III), 21 December 2021)
2. Department-Related Parliamentary Standing Committee on Home Affairs, *Two Hundred and Forty-Eighth Report: The Bharatiya Sakshya Bill, 2023* (Rajya Sabha Secretariat, November 2023)
3. Law Commission, *Evidence in Criminal Proceedings: Hearsay and Related Topics* (Law Com No 245, 1997)
4. PRS Legislative Research, 'Legislative Brief: The Bharatiya Sakshya (Second) Bill, 2023'
https://prsindia.org/files/bills_acts/bills_parliament/2023/Legislative

[Brief_The_Bharatiya_Sakshya_\(Second\)_Bill_2023.pdf](#) accessed 5 October 2026

5. PRS Legislative Research, 'Standing Committee Report Summary: The Bharatiya Sakshya Bill, 2023' (10 November 2023) <https://prsindia.org/billtrack/prs-products/standing-committee-report-summary-4276> accessed 5 October 2026
6. PRS Legislative Research, 'The Bharatiya Sakshya Bill, 2023' <https://prsindia.org/billtrack/the-bharatiya-sakshya-bill-2023> accessed 5 October 2026

D. Books, Articles and Secondary Sources

1. Agarwal P, 'Electronic Evidence under the BSA, 2023' (*iPleaders*, 1 July 2026) <https://blog.ipleaders.in/electronic-evidence-under-the-bsa-2023/>
2. Gupta S, 'Legal Turmoil in Admissibility of Electronic Evidence Due to Interpretation of S 65B by Supreme Court (Part 3)' (*The Leaflet*, 15 October 2020) <https://theleaflet.in/supreme-court/part-3-legal-turmoil-in-admissibility-of-electronic-evidence-due-to-interpretation-of-s-65b-by-supreme-court> accessed 7 October 2026
3. Marshall P and others, 'Recommendations for the Probity of Computer Evidence' (2021) 18 *Digital Evidence and Electronic Signature Law Review* 18
4. Mason S and Seng D (eds), *Electronic Evidence and Electronic Signatures* (5th edn, University of London Press 2021)
5. Sekhri A, 'The Supreme Court, 65-B Certificates, and Electronic Evidence' (*The Criminal Law Blog*, 20 July 2020) <https://thecriminallawblog.in/2020/07/20/the-supreme-court-65-b-certificates-and-electronic-evidence/>