
WHO CAN CERTIFY ELECTRONIC EVIDENCE? THE SUPREME COURT'S UNFINISHED INTERPRETATION OF SECTION 63(4) OF THE BHARATIYA SAKSHYA ADHINIYAM, 2023

Rajdeep Malik, Bareilly College, Bareilly, Affiliated to Mahatma Jyotiba Phule
Rohilkhand University, Bareilly, Uttar Pradesh, India

ABSTRACT

Section 63(4) of the Bharatiya Sakshya Adhiniyam, 2023 conditions the admissibility of secondary electronic evidence on a standard-form certificate whose Schedule is split into Part A, signed by the party, and Part B, signed by an unspecified "expert." This bifurcation raised a question the statute left unanswered: who is competent to sign Part B? A Madras High Court view confined that role to Examiners of Electronic Evidence notified under Section 79A of the Information Technology Act, 2000, threatening to route all digital evidence through a handful of forensic laboratories. In *Pune Bar Association v. Union of India* (2026), the Supreme Court upheld the constitutional validity of Section 63(4), treating the hash-value and expert requirements as bearing a rational nexus to authenticity and integrity, and read Sections 39(1) and 39(2) of the BSA harmoniously to permit court-satisfied private cyber-forensics experts to sign Part B. Yet the Court declined notice and kept the question of law open, producing an authoritative signal without a binding rule. This article traces the evolution from Section 65B, dissects the Court's reasoning, distinguishes admissibility from authenticity and weight, compares United States and English approaches, and argues that India's certification model remains clarified in direction but unfinished in doctrine.

Keywords: electronic evidence; Section 63(4) Bharatiya Sakshya Adhiniyam 2023; Part B certificate; Examiner of Electronic Evidence; Section 79A IT Act; hash value; admissibility; deepfakes.

I. Introduction: A Narrow Order With a Wide Shadow

When the Supreme Court disposed of *Pune Bar Association v. Union of India* on 22 May 2026, it did so without issuing notice to the Union of India and in a short signed order¹. Yet the order has generated attention out of all proportion to its length, because it touched the most practically consequential question in the new law of electronic evidence: when a party places a digital record before an Indian court, who must sign the certificate that renders that record admissible?

The controversy is precise. Section 63(4) of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) requires that every computer output offered as secondary electronic evidence be accompanied by a certificate in the form prescribed in the Schedule to the Act². That Schedule splits the certificate into two parts: Part A, "to be filled by the Party," and Part B, "to be filled by the Expert³." The Act does not define who counts as an "expert" for the purposes of Part B. A single line of reasoning in a Madras High Court matrimonial judgment had suggested that only a government-notified Examiner of Electronic Evidence under Section 79A of the Information Technology Act, 2000 could sign that part⁴. If correct, that reading would have made the admissibility of digital evidence hostage to a tiny roster of accredited forensic laboratories⁵. The Pune Bar Association argued that the entire scheme was manifestly arbitrary, and asked the Court to strike it down⁶.

The Supreme Court refused to strike it down, upheld the provision's rationality, and read the "expert" requirement broadly⁷. But it expressly declined to render a "conclusive opinion" and kept "the question of law open⁸." The result is an authoritative signal without a binding rule – an interpretation that is, in a real sense, unfinished. This article maps that unfinished interpretation, situates it in the arc of Indian electronic-evidence jurisprudence, and asks what remains to be

¹ *Pune Bar Association v. Union of India*, W.P. (C) No. 599 of 2026, ¶ 7 (S.C. May 22, 2026) (declining to admit the matter or issue notice and disposing of the petition by signed order), <https://www.casemine.com/judgement/in/6a1d30370f59796491c16219>; see also JSA, *JSA Prism | Dispute Resolution* (June 2026) (recording decision date as May 22, 2026), <https://www.jsalaw.com/newsletters-and-updates/jsa-prism-dispute-resolution-june-2026-2/>.

² Bharatiya Sakshya Adhiniyam, 2023, § 63(4), <https://indiankanoon.org/doc/125020475/>.

³ The Schedule to the Bharatiya Sakshya Adhiniyam, 2023 [See § 63(4)(c)], India Code, https://upload.indiacode.nic.in/schedulefile?aid=AC_CEN_5_23_00049_2023-47_1719292804654&rid=1163.

⁴ *Pune Bar Association*, *supra* note 1, 5–6 (referring to *R. v. B & Anr.*, 2024 SCC OnLine Mad 6084), <https://www.casemine.com/judgement/in/6a1d30370f59796491c16219>.

⁵ JSA, *supra* note 1 (noting the "limited number of Examiners notified under Section 79A" and consequent practical difficulty), <https://www.jsalaw.com/newsletters-and-updates/jsa-prism-dispute-resolution-june-2026-2/>.

⁶ *Pune Bar Association*, *supra* note 1, ¶ 1 (petitioner's contention that the provision is "manifestly arbitrary and unjust"), <https://www.casemine.com/judgement/in/6a1d30370f59796491c16219>.

⁷ *Id.* ¶¶ 4, 7.

⁸ *Id.* ¶ 7 ("we refrain from giving any conclusive opinion on this issue and keep the question of law open").

settled.

The stakes are not academic. Digital records now saturate litigation of every kind, from the WhatsApp message in a matrimonial dispute to the CCTV clip in a murder trial and the server log in a commercial fraud. The rule that decides who may vouch for such a record decides, in practice, whether a vast quantity of everyday evidence ever reaches a judge's eyes. A restrictive rule protects against fabrication but risks paralysing ordinary litigation; a permissive one eases access but dilutes the very safeguard the certificate was meant to supply. The Court in *Pune Bar Association* felt the pull of both concerns and, characteristically for a disposal without notice, resolved the tension only partially. Understanding exactly how far it went and where it stopped is therefore essential for anyone who will place a digital record before an Indian court in the years ahead.

II. From Section 65B to Section 63: An Evolving Certificate

Indian law began treating computer output as a distinct evidentiary species in 2000, when the Information Technology Act inserted Sections 65A and 65B into the Indian Evidence Act, 1872⁹. Section 65B made secondary electronic evidence admissible only on conditions, chief among them a certificate under Section 65B(4)¹⁰.

The judicial interpretation of that certificate swung between rigour and pragmatism. In *Anvar P.V. v. P.K. Basheer*, a three-judge Bench held in 2014 that a Section 65B(4) certificate was a condition precedent to the admissibility of secondary electronic evidence, and that oral evidence could not substitute for it¹¹. A two-judge Bench diluted this in *Shafhi Mohammad v. State of Himachal Pradesh* (2018), reasoning that the certificate requirement was "procedural" and could be relaxed where the party tendering the record was not in possession of the device¹².

⁹ *Admissibility of Electronic Evidence Under the Indian Evidence Act, 1872*, Mondaq (Sections 65A and 65B inserted by the IT Act, 2000), <https://www.mondaq.com/india/disclosure-amp-electronic-discovery-amp-privilege/715108/admissibility-of-electronic-evidence-under-the-indian-evidence-act-1872>.

¹⁰ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, judgment PDF (§ 65B(4) certificate a "sine qua non" for admissibility of secondary electronic evidence), https://aphc.gov.in/docs/imp_judgements/Arjun%20Panditrao%20Khotkar%20_%20Kailash%20Kushanrao%20Gorantyal%20And%20Ors._1701334263.pdf.

¹¹ *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473, as discussed in Mondaq, *supra* note 9 (three-judge Bench; secondary electronic evidence requires § 65B procedure), <https://www.mondaq.com/india/disclosure-amp-electronic-discovery-amp-privilege/715108/admissibility-of-electronic-evidence-under-the-indian-evidence-act-1872>.

¹² *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801, ¶ 30, as reproduced at CaseMine ("The applicability of requirement of certificate being procedural can be relaxed by Court wherever interest of justice so justifies."), <https://www.casemine.com/judgement/in/5ac9bf344a9326331c621b67>.

That relaxation proved short-lived. In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), a three-judge Bench reaffirmed *Anvar*, overruled *Shafhi Mohammad*, and held that a written certificate under Section 65B(4) is a *sine qua non* for the admissibility of information contained in electronic records by way of secondary evidence¹³. It clarified that no certificate is needed where the original device itself is produced by its owner, and it laid down a procedure for parties who cannot secure a certificate, permitting them to apply to the trial judge to summon the person or authority holding it¹⁴.

The BSA, which replaced the Evidence Act in 2023, carried this architecture forward but tightened it. Section 63 of the BSA reproduces the conditions of the old Section 65B almost verbatim¹⁵, but Section 63(4) now insists on a certificate "in the form" specified in the Schedule "at each instance where it is being submitted for admission¹⁶." The Supreme Court itself described the shift succinctly: the BSA "improved upon the certificate envisaged under the old law by mandating the issuance of a standard-form certificate," adding two new elements disclosure of the hash value of the record and a further certification by an expert¹⁷.

III. The Architecture of Section 63, the Schedule, and Section 79A

Section 63(1) deems any computer output to be a document admissible without production of the original if the statutory conditions are met¹⁸. Section 63(2) restates the familiar reliability conditions regular use of the device, ordinary-course feeding of information, proper operation, and faithful reproduction¹⁹. Section 63(3) treats a network of devices as a single computer²⁰. Section 63(4) is the operative gateway: it requires a certificate identifying the record, describing how it was produced, giving particulars of the device, and dealing with the subsection (2) conditions, "purporting to be signed by a person in charge of the computer or communication device or the management of the relevant activities (whichever is appropriate)

¹³ Aishwarya Agrawal, *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, LawBhoomi (July 19, 2024) (2020 decision reaffirming *Anvar* and overruling *Shafhi Mohammad*; § 65B(4) certificate mandatory), <https://lawbhoomi.com/arjun-panditrao-khotkar-v-kailash-kushanrao-gorantyal/>; see also *Arjun Panditrao judgment PDF*, *supra* note 10 (Nariman & Ramasubramanian, JJ.).

¹⁴ LawBhoomi, *supra* note 13 (no certificate where original device produced by owner; application to judge available where certificate cannot be obtained), <https://lawbhoomi.com/arjun-panditrao-khotkar-v-kailash-kushanrao-gorantyal/>.

¹⁵ Bharatiya Sakshya Adhiniyam, 2023, § 63(2)(a)–(d), <https://indiankanoon.org/doc/125020475/>.

¹⁶ *Id.* § 63(4).

¹⁷ *Pune Bar Association*, *supra* note 1, ¶ 4, <https://www.casemine.com/judgement/in/6a1d30370f59796491c16219>.

¹⁸ Bharatiya Sakshya Adhiniyam, 2023, § 63(1), <https://indiankanoon.org/doc/125020475/>.

¹⁹ *Id.* § 63(2).

²⁰ *Id.* § 63(3).

and an expert²¹."

The Schedule, headed "[See section 63(4)(c)]," splits that signature obligation. Part A is completed by the party, who identifies the device or source (computer, DVR, mobile, flash drive, CD/DVD, server, cloud, or other), attests to the device's lawful control and proper functioning, and states the hash value obtained through a named algorithm such as SHA1, SHA256, or MD5, with a hash report enclosed²². Part B is completed by "the Expert," who separately identifies the source, restates the hash value, and signs with name, designation, and signature²³. The two innovations over Section 65B are therefore visible on the face of the form: the compulsory hash value in Part A, and the compulsory expert signature in Part B.

The drafting choice to bifurcate the certificate is significant in itself. Under the old Section 65B, a single custodian's certificate sufficed; the person in charge of the device attested to both operation and content, and no separate expert imprimatur was required. By adding Part B, the BSA converts what was once a self-certified custodian's statement into a dual-signature instrument that pairs the party's factual attestation with an independent technical endorsement. This is a deliberate raising of the evidentiary threshold, and it explains why the identity of the Part B signatory became the fulcrum of the litigation: the more demanding the expert requirement, the harder it becomes to bring routine digital evidence to court at all.

Who that expert is depends on a provision outside the BSA. Section 79A of the IT Act empowers the Central Government to "notify" as an "Examiner of Electronic Evidence" any "Department, body or agency of the Central Government or a State Government" that provides expert opinion on electronic-form evidence²⁴. Two features of Section 79A matter for the present controversy. First, it is enabling and institutional: the Ministry of Electronics and Information Technology's scheme states expressly that it is "not for individual expert to be notified as Expert Examiners rather for labs to be notified²⁵." Second, the pool is small and slow-growing. As of mid-2026, roughly two dozen laboratories had been notified, with six

²¹ *Id.* § 63(4)(a)–(c).

²² The Schedule, Part A, *supra* note 3, https://upload.indiacode.nic.in/schedulefile?aid=AC_CEN_5_23_00049_2023-47_1719292804654&rid=1163.

²³ *Id.* Part B ("To be filled by the Expert"; "Name, designation and signature").

²⁴ Information Technology Act, 2000, § 79A, India Code, https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.

²⁵ Ministry of Electronics & Information Technology, *Scheme for Notifying Examiner of Electronic Evidence Under Section 79A* ("Scheme is not for individual expert to be notified as Expert Examiners rather for labs to be notified"), <https://www.meity.gov.in/static/uploads/2025/11/67f1ee29ffea0e76a3e5b5fee9883711.pdf>.

additional institutions gazetted only on 13 July 2026²⁶. Inside the BSA, Section 39(2) links to this framework by treating the opinion of a Section 79A Examiner as that of an expert; Section 39(1) more generally makes relevant the opinion of any person "having special skill" in science or "any other field"²⁷.

IV. Pune Bar Association v. Union of India: Facts, Questions, and Holding

The petitioner, the Pune Bar Association, invoked Article 32 to challenge Section 63(4) read with the Schedule as unconstitutional, contending that the requirement to disclose a hash value in Part A and to obtain an expert's signature in Part B imposed an "extremely onerous obligation" on ordinary litigants and rendered the provision "manifestly arbitrary and unjust"²⁸. A Bench of Chief Justice Surya Kant, Justice Joymalya Bagchi, and Justice Vipul M. Pancholi heard the matter and disposed of it by a signed order on 22 May 2026, without admitting the petition or issuing notice to the Union²⁹.

Two questions were embedded in the challenge. The first was whether the hash-value and expert-certification requirements were constitutionally arbitrary. The second, raised through reliance on the Madras High Court's decision in *R. v. B*, was whether Part B could be signed only by a Section 79A-notified Examiner, given that "only a handful of entities" are so authorised³⁰.

On the first question, the Court upheld the provision. It observed that an electronic record is "a unique species of evidence which is liable to continuous mutation and modification affecting its authenticity, integrity and intrinsic evidentiary value," and that these challenges are "accentuated with the advent of artificial intelligence and deepfake technology"³¹. A hash value, the Court reasoned, "is synonymous with an electronic fingerprint and provides a sure

²⁶ *India Bolsters Digital Forensics Capabilities with Six New Institutions*, Ministry of Cyber Affairs (July 14, 2026) (six institutions gazetted July 13, 2026, in addition to existing labs), <https://ministryofcyberaffairs.com/news/india-bolsters-digital-forensics-capabilities-with-six-new-institutions-for-electronic-evidence-examination-1f6606f8-ba8a-4432-ba2d-2e3d0511582a>.

²⁷ *Pune Bar Association*, *supra* note 1, ¶ 6 (describing § 39(1) and § 39(2) of the BSA), <https://www.casemine.com/judgement/in/6a1d30370f59796491c16219>.

²⁸ *Id.* ¶ 1.

²⁹ *Id.* (coram: Surya Kant, C.J., Joymalya Bagchi & Vipul M. Pancholi, JJ.; order dated May 22, 2026); *Supreme Court Rejects Challenge To S.63(4) BSA*, Live Law (May 28, 2026) (confirming bench and Article 32 petition), <https://www.livelaw.in/top-stories/supreme-court-rejects-challenge-to-s634-bsa-mandating-hash-value-disclosure-for-electronic-evidence-535950>.

³⁰ *Pune Bar Association*, *supra* note 1, ¶ 5, <https://www.casemine.com/judgement/in/6a1d30370f59796491c16219>.

³¹ *Id.* ¶ 3.

way of identifying and verifying digital data," so its disclosure "cannot be said to lack a rational nexus with the object of the Act³²." Expert certification in Part B "provides an additional layer of authenticity³³." Accordingly, the requirements bore "a clear and rational nexus with the object of the law" and did not suffer from "the vice of manifest arbitrariness³⁴."

On the second question, the Court parted company with the Madras High Court. It noted that the High Court had, in a matrimonial case instituted in 2019 governed by the old Evidence Act, held that the Part B expert must be a Section 79A Examiner, but had reached that view by referring only to Section 39(2) of the BSA "and not sub-section (1)³⁵." Reading the two sub-sections "harmoniously," the Court held that in addition to notified Examiners, "if the Court is satisfied, on the basis of unimpeachable material, that any other person has special skill and expertise in computer science and cyber forensics," that person's opinion "may be held relevant as an expert" and "such person may sign Part B of the Schedule as an expert.³⁶" The Court was "fortified" in this reading because Section 39(2), "unlike 63(4) and erstwhile 65B," is "not prefaced by a non-obstante clause" and so does not exclude the operation of Section 39(1)³⁷.

V. What the Court Decided and What It Left Open

It is essential to separate the two strands of the order, because they have different legal weight. The first strand – the constitutional validity of Section 63(4) and its hash-value and expert requirements – was a considered adjudication that upheld the provision as neither arbitrary nor unreasonable³⁸. The second strand – the identity of the Part B expert – was deliberately provisional. Having declined to admit the matter or issue notice to the Union, the Court "refrain[ed] from giving any conclusive opinion on this issue" and kept "the question of law open³⁹." Its operative direction was negative rather than positive: it held only that the Madras High Court's finding "that Part B must be filled up by an expert notified under Section 79A of the IT Act shall not be treated as a binding precedent⁴⁰."

The consequence is a precedential asymmetry that practitioners must handle carefully. The

³² *Id.* ¶ 4.

³⁴ https://word-edit.officeapps.live.com/we/*Id.*

³⁵ *Id.* ¶ 6.

³⁶ *Id.* ¶ 7.

³⁷ https://word-edit.officeapps.live.com/we/*Id.*

³⁸ *Id.* ¶ 4.

³⁹ *Id.* ¶ 7.

⁴⁰ https://word-edit.officeapps.live.com/we/*Id.*

restrictive Madras view is now disapproved and denuded of binding force; the broader view that an independent cyber-forensics expert may sign Part B is strongly indicated but not settled as ratio, because the Court itself framed it as an observation on an open question decided without contest. A candid reading is that the door has been widened, but not bolted open. Until a Bench decides the point after full argument or the legislature clarifies it a subordinate court retains room to demand a notified Examiner in a case where it is not satisfied by "unimpeachable material" about a private expert's credentials⁴¹.

VI. Untangling Six Distinct Legal Ideas

Much of the confusion in this field flows from collapsing analytically distinct concepts. Section 63(4) engages at least six.

Production concerns whether the original device or a copy is placed before the court; *Arjun Panditrao* fixed that primary evidence produced by the device's owner needs no certificate, while secondary evidence does⁴². *Admissibility* is the threshold legal question of whether the record may enter the record at all; under Section 63(4) the certificate is the key to that door⁴³. *Authenticity* asks whether the record is genuinely what it purports to be the function the Court assigned to the hash value as an "electronic fingerprint"⁴⁴. *Integrity* asks whether the record has been altered since capture; a matching hash across time is the technical proof of non-alteration⁴⁵. *Probative weight* is a later, separate inquiry into how much the admitted record proves and here the Court's clarification is telling: even where a private expert signs Part B, "the discretion to admit electronic documents based on the certificates provided by such experts still rests with the courts"⁴⁶. *Expert opinion*, finally, is the appreciation under Section 39 of whether the certifier possesses the "special skill" the record's evaluation demands⁴⁷. The Part B controversy is, at bottom, an argument about the last of these the qualification of the opinion-giver masquerading as an argument about admissibility.

⁴¹ *Id.* (private expert admissible only where court is satisfied "on the basis of unimpeachable material").

⁴² LawBhoomi, *supra* note 13, <https://lawbhoomi.com/arjun-panditrao-khotkar-v-kailash-kushanrao-gorantyal/>.

⁴³ Bharatiya Sakshya Adhiniyam, 2023, § 63(4), <https://indiankanoon.org/doc/125020475/>

⁴⁴ *Pune Bar Association*, *supra* note 1, ¶ 4,

<https://www.casemine.com/judgement/in/6a1d30370f59796491c16219>.

⁴⁵ *Id.* (hash value ensures "authenticity and integrity").

⁴⁶ JSA, *supra* note 1 (courts retain discretion to admit despite private-expert certificate),

<https://www.jsalaw.com/newsletters-and-updates/jsa-prism-dispute-resolution-june-2026-2/>.

⁴⁷ *Pune Bar Association*, *supra* note 1, ¶ 6 (§ 39 on opinions of experts),

<https://www.casemine.com/judgement/in/6a1d30370f59796491c16219>.

VII. Who Signs Part A, Who Signs Part B, and Why It Matters

The Schedule allocates the two signatures to different actors for different reasons. Part A is the party's or custodian's declaration: the person "in charge" of the device or "the management of the relevant activities" attests to lawful control, ordinary-course operation, and the computed hash value⁴⁸. This mirrors the traditional Section 65B custodian's certificate and is, in principle, within the reach of any ordinary litigant who controls the source.

Part B is where the interpretive fault line runs. On the restrictive reading, advanced by the Madras High Court and pressed by the petitioner, the expert must be a Section 79A-notified Examiner, because Section 39(2) elevates such an Examiner's opinion to expert status for electronic records⁴⁹. On the expansive reading adopted by the Supreme Court, Section 39(1) independently makes relevant the opinion of any person with special skill in "science" or "any other field," and since Section 39(2) carries no non-obstante clause, it supplements rather than supplants Section 39(1); a court-satisfied private cyber-forensics expert may therefore sign⁵⁰.

The practical stakes are considerable. There is only a small set of notified laboratories, and channelling every certificate through them would create backlogs and delay litigation, as commentary on the judgment observed⁵¹. The expansive reading relieves that bottleneck. But it transfers a gatekeeping burden to trial judges, who must now assess, on "unimpeachable material," whether a proffered private expert genuinely possesses the requisite skill a task for which many courts are under-equipped, and which reintroduces the very case-by-case uncertainty that a standard-form certificate was meant to eliminate⁵².

There is also a subtler point about the relationship between the two parts. Part A is not dispensable merely because a well-qualified expert signs Part B; the party's own attestation of lawful control and ordinary-course operation remains a distinct requirement rooted in the Section 63(2) conditions. Nor does an expert's Part B signature convert an otherwise

⁴⁸ The Schedule, Part A, *supra* note 3, https://upload.indiacode.nic.in/schedulefile?aid=AC_CEN_5_23_00049_2023-47_1719292804654&rid=1163; Bharatiya Sakshya Adhiniyam, 2023, § 63(4)(c) (person "in charge" or of "the management of the relevant activities").

⁴⁹ *Pune Bar Association*, *supra* note 1, ¶¶ 5–6, <https://www.casemine.com/judgement/in/6a1d30370f59796491c16219>.

⁵⁰ *Id.* ¶ 7.

⁵¹ JSA, *supra* note 1, <https://www.jsalaw.com/newsletters-and-updates/jsa-prism-dispute-resolution-june-2026-2/>.

⁵² *Pune Bar Association*, *supra* note 1, ¶ 7 (court-satisfaction requirement), <https://www.casemine.com/judgement/in/6a1d30370f59796491c16219>.

inadmissible record into conclusive proof. As the post-judgment commentary stresses, the trial court's discretion to weigh and even to decline to admit a record certified by a private expert survives intact. The certificate, in other words, is a gate, not a guarantee; passing through it secures a hearing on the merits, not a verdict on authenticity.

VIII. Special Challenges: CCTV, Phones, Social Media, Cloud, and Synthetic Media

The generic certificate confronts very different technical realities. CCTV and DVR footage is expressly contemplated in the Schedule's device list, yet such systems frequently overwrite storage and lack a clear custodian able to attest to continuous proper operation⁵³. Mobile phones raise the *Arjun Panditrao* problem acutely: the owner can produce the handset and avoid a certificate, but records extracted from a seized phone by investigators are secondary evidence needing Part B certification, and the extraction process itself must preserve the hash⁵⁴. Social-media and cloud records, both listed in the Schedule, are typically held by intermediaries abroad; the party seeking to rely on them rarely has "lawful control," and the hash of a downloaded copy proves only the integrity of that copy, not of the server-side original⁵⁵.

Synthetic media is the challenge the Court itself foregrounded. It observed that authenticity concerns are "accentuated with the advent of artificial intelligence and deepfake technology," and treated the hash-plus-expert regime as a rational response⁵⁶. But a hash value certifies only that a file has not changed since it was hashed; it says nothing about whether the file was fabricated by generative AI before hashing. This is precisely the gap that reform proposals abroad target: draft amendments to the U.S. Federal Rules of Evidence would shift a heightened authenticity burden onto the proponent once a challenger shows a record may be AI-fabricated⁵⁷. India's certificate framework, focused on integrity rather than provenance, does not yet close that gap—a limitation the Court's own reasoning implicitly concedes but does not resolve.

⁵³ The Schedule, Part A (device list includes DVR, Cloud, Server), *supra* note 3, https://upload.indiacode.nic.in/schedulefile?aid=AC_CEN_5_23_00049_2023-47_1719292804654&rid=1163

⁵⁴ LawBhoomi, *supra* note 13 (owner may produce device to avoid certificate; extracted secondary evidence needs certification), <https://lawbhoomi.com/arjun-panditrao-khotkar-v-kailash-kushanrao-gorantyal/>.

⁵⁵ The Schedule, Part A (Cloud and Server sources; "lawful control" attestation), *supra* note 3, https://upload.indiacode.nic.in/schedulefile?aid=AC_CEN_5_23_00049_2023-47_1719292804654&rid=1163.

⁵⁶ *Pune Bar Association*, *supra* note 1, ¶ 3, <https://www.casemine.com/judgement/in/6a1d30370f59796491c16219>.

⁵⁷ *Deepfakes on Trial: How Judges Are Navigating AI Evidence*, Thomson Reuters Institute (May 8, 2025), <https://www.thomsonreuters.com/en-us/posts/ai-in-courts/deepfakes-evidence-authentication/>.

IX. Constitutional and Fair-Trial Implications

For the prosecution, the strict certificate regime is a discipline: without a compliant Part A and Part B, a digital record "does not enter the court's record, regardless of how authentic or relevant it may be," so investigators must build hash and chain-of-custody practices into every seizure⁵⁸. For the accused, the same rigour is a shield against fabricated or tampered digital evidence, consistent with the fair-trial guarantee read into Article 21; but the accused may also be disadvantaged where exculpatory digital material sits in a third party's control and no expert is readily available to certify it. *Arjun Panditrao's* summoning mechanism partly addresses this by allowing a party who cannot obtain a certificate to seek the court's help⁵⁹. For civil litigants, the expert-signature requirement raises access-to-justice concerns: the Pune Bar Association's core grievance was that ordinary litigants would be burdened by a scarce and costly expert pool⁶⁰. The Supreme Court's expansive reading of "expert" was, in substance, a proportionality-driven mitigation of that burden preserving the safeguard while widening the class of persons who can satisfy it⁶¹.

X. Comparative Perspectives: The United States and England and Wales

Two mature systems illustrate divergent design choices, and the comparison should be kept proportionate to India's statutory model.

The United States moved toward certification, not away from it. Federal Rules of Evidence 902(13) and 902(14), effective December 2017, make certain electronic records self-authenticating on a written "certification of a qualified person," subject to advance notice to the adverse party Rule 902(13) for records "generated by an electronic process or system" and Rule 902(14) for "data copied from an electronic device, storage medium, or file" authenticated by "a process of digital identification⁶²." This resembles the Indian approach in spirit: a qualified person's certificate, keyed to a digital-identification process such as hashing, substitutes for live foundational testimony. The difference is that U.S. self-authentication only removes the authentication hurdle; the opponent may still contest weight, and reform debates

⁵⁸ *Pune Bar Association*, *supra* note 1, ¶ 4 (certificate a condition of admissibility); *see also* JSA, *supra* note 1, <https://www.jsalaw.com/newsletters-and-updates/jsa-prism-dispute-resolution-june-2026-2/>.

⁵⁹ LawBhoomi, *supra* note 13, <https://lawbhoomi.com/arjun-panditrao-khotkar-v-kailash-kushanrao-gorantyal/>.

⁶⁰ *Pune Bar Association*, *supra* note 1, ¶ 1, <https://www.casemine.com/judgement/in/6a1d30370f59796491c16219>.

⁶¹ *Id.* ¶ 7.

⁶² Fed. R. Evid. 902(13)–(14), Legal Information Institute, https://www.law.cornell.edu/rules/fre/rule_902.

now focus on deepfake-specific burden-shifting⁶³.

England and Wales chose the opposite pole. Section 69 of the Police and Criminal Evidence Act 1984, which had required proof that a computer was operating properly, was repealed in 2000 following a Law Commission recommendation, leaving a common-law rebuttable presumption that a computer was "working correctly at the material time" unless contrary evidence is adduced⁶⁴. The *Bates v Post Office Horizon* litigation exposed the danger of that presumption, with the court accepting that software errors could have produced apparent accounting shortfalls, and prompting a government call for evidence on reform in 2025⁶⁵. The contrast is instructive: India's Section 63(4) places the evidential onus of authenticity on the proponent through a mandatory certificate and hash, whereas England presumes reliability and puts the challenger to proof an allocation the Horizon scandal has shown can be unjust. India's front-loaded, proponent-borne model looks the safer of the two, provided the expert bottleneck is solved.

XI. Implementation Gaps

Several gaps remain even after *Pune Bar Association*. The identity of the Part B expert is legally unsettled, since the Court kept the question open⁶⁶. The Section 79A pool remains institutional and thin, and the MeitY scheme notifies laboratories, not individuals, leaving unclear how a private "person" with "special skill" is to be objectively qualified in practice⁶⁷. There is no uniform standard for what "unimpeachable material" a court must see before accepting a private expert, no prescribed accreditation for individual cyber-forensics practitioners, and no statutory guidance on provenance testing for AI-generated media as opposed to integrity testing by hash⁶⁸. Finally, chain-of-custody, metadata preservation, and

⁶³ Thomson Reuters Institute, *supra* note 57, <https://www.thomsonreuters.com/en-us/posts/ai-in-courts/deepfakes-evidence-authentication/>.

⁶⁴ *The Presumption That Computers Are Reliable*, Counsel Magazine (July 10, 2024) (PACE 1984 § 69 repealed; common-law rebuttable presumption), <https://www.counselmagazine.co.uk/articles/the-presumption-that-computers-are-reliable>; Youth Justice and Criminal Evidence Act 1999, § 60, Explanatory Notes, <https://www.legislation.gov.uk/ukpga/1999/23/notes/division/4/2/6/3>.

⁶⁵ Counsel Magazine, *supra* note 64 (*Bates v The Post Office Ltd (No. 6: Horizon Issues)* [2019] EWHC 3408 (QB)), <https://www.counselmagazine.co.uk/articles/the-presumption-that-computers-are-reliable>; *Use of Computer Evidence in Court to Be Interrogated*, GOV.UK (Jan. 21, 2025), <https://www.gov.uk/government/news/use-of-computer-evidence-in-court-to-be-interrogated>.

⁶⁶ *Pune Bar Association*, *supra* note 1, ¶ 7, <https://www.casemine.com/judgement/in/6a1d30370f59796491c16219>.

⁶⁷ MeitY Scheme, *supra* note 25, <https://www.meity.gov.in/static/uploads/2025/11/67f1ee29ffea0e76a3e5b5fee9883711.pdf>.

⁶⁸ *Pune Bar Association*, *supra* note 1, ¶ 7 (no defined standard for "unimpeachable material"), <https://www.casemine.com/judgement/in/6a1d30370f59796491c16219>.

retention duties which *Arjun Panditrao* urged be codified through rules under the IT Act remain incompletely implemented⁶⁹.

XII. Recommendations

Legislative. Parliament or the rule-making authority should define "expert" for Part B, either by amending the Schedule or by framing rules that recognise both Section 79A-notified laboratories and individually accredited cyber-forensics professionals, with objective eligibility criteria. Given that Section 39(2) lacks a non-obstante clause the very point on which the Court relied a clarificatory proviso would settle the question the Court left open⁷⁰.

Judicial. Pending legislative clarity, an appropriately constituted Bench should decide the open question after full argument and notice to the Union, so that the expansive reading acquires the status of binding ratio rather than tentative observation. Courts should also develop a checklist for assessing private experts' credentials to give content to the "unimpeachable material" threshold.

Administrative. The Government should expand and decentralise the Section 79A pool the July 2026 notification of six more laboratories is a step in this direction and create an accreditation register for individual examiners⁷¹. Investigating agencies should adopt standardised hashing and chain-of-custody protocols aligned with ISO/IEC 17025 and 27037, which already underpin the MeitY notification scheme⁷². Finally, rule-makers should consider a provenance-focused safeguard for suspected synthetic media, drawing on the burden-shifting model under discussion abroad⁷³.

XIII. Conclusion

Pune Bar Association v. Union of India settled that Section 63(4) of the BSA is constitutionally

⁶⁹ LawBhoomi, *supra* note 13 (*Arjun Panditrao* directions on CDR retention, chain of custody, and IT Act rule-making), <https://lawbhoomi.com/arjun-panditrao-khotkar-v-kailash-kushanrao-gorantyal/>.

⁷⁰ *Pune Bar Association*, *supra* note 1, ¶ 7 (reliance on the absence of a non-obstante clause in § 39(2)), <https://www.casemine.com/judgement/in/6a1d30370f59796491c16219>.

⁷¹ Ministry of Cyber Affairs, *supra* note 26, <https://ministryofcyberaffairs.com/news/india-bolsters-digital-forensics-capabilities-with-six-new-institutions-for-electronic-evidence-examination-1f6606f8-ba8a-4432-ba2d-2e3d0511582a>.

⁷² MeitY Scheme, *supra* note 25 (ISO/IEC 17025 and 27037 compliance), <https://www.meity.gov.in/static/uploads/2025/11/67f1ee29ffea0e76a3e5b5fee9883711.pdf>.

⁷³ Thomson Reuters Institute, *supra* note 57, <https://www.thomsonreuters.com/en-us/posts/ai-in-courts/deepfakes-evidence-authentication/>.

sound: the hash value and the expert signature bear a rational nexus to the object of ensuring the authenticity and integrity of a uniquely mutable species of evidence. It strongly signalled that the Part B "expert" is not confined to Section 79A Examiners, reading Sections 39(1) and 39(2) harmoniously to admit court-satisfied private cyber-forensics experts. But by declining notice and keeping the question of law open, the Court left the central practical question who can certify electronic evidence authoritatively indicated yet formally unresolved. The interpretation is, for now, unfinished. Until a Bench decides the point on contest or the legislature defines the expert, litigants operate in the space between a disapproved narrow rule and an un-ratified broad one. The candid conclusion is that the law of electronic-evidence certification in India has been clarified in direction but not yet fixed in doctrine.

REFERENCES:**Primary Sources**

- Bharatiya Sakshya Adhiniyam, 2023, § 63, <https://indiankanoon.org/doc/125020475/>.
- The Schedule to the Bharatiya Sakshya Adhiniyam, 2023 [See § 63(4)(c)], India Code, https://upload.indiacode.nic.in/schedulefile?aid=AC_CEN_5_23_00049_2023-47_1719292804654&rid=1163.
- Information Technology Act, 2000, § 79A, India Code, https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.
- *Pune Bar Association v. Union of India*, W.P. (C) No. 599 of 2026 (S.C. May 22, 2026), full order text at CaseMine, <https://www.casemine.com/judgement/in/6a1d30370f59796491c16219>.
- Fed. R. Evid. 902(13)–(14), Legal Information Institute, https://www.law.cornell.edu/rules/fre/rule_902.
- Youth Justice and Criminal Evidence Act 1999, § 60 (repealing PACE 1984, § 69), Explanatory Notes, <https://www.legislation.gov.uk/ukpga/1999/23/notes/division/4/2/6/3>.

Secondary Sources

- *Supreme Court Rejects Challenge To S.63(4) BSA Mandating Hash Value Disclosure For Electronic Evidence*, Live Law (May 28, 2026), <https://www.livelaw.in/top-stories/supreme-court-rejects-challenge-to-s634-bsa-mandating-hash-value-disclosure-for-electronic-evidence-535950>.
- JSA, *JSA Prism | Dispute Resolution* (June 2026), <https://www.jsalaw.com/newsletters-and-updates/jsa-prism-dispute-resolution-june-2026-2/>.
- Ministry of Electronics & Information Technology, *Scheme for Notifying Examiner of Electronic Evidence Under Section 79A*,

<https://www.meity.gov.in/static/uploads/2025/11/67f1ee29ffea0e76a3e5b5fee9883711.pdf>.

- *India Bolsters Digital Forensics Capabilities with Six New Institutions*, Ministry of Cyber Affairs (July 14, 2026), <https://ministryofcyberaffairs.com/news/india-bolsters-digital-forensics-capabilities-with-six-new-institutions-for-electronic-evidence-examination-1f6606f8-ba8a-4432-ba2d-2e3d0511582a>.
- Aishwarya Agrawal, *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, LawBhoomi (July 19, 2024), <https://lawbhoomi.com/arjun-panditrao-khotkar-v-kailash-kushanrao-gorantyal/>.
- *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, judgment PDF, A.P. High Court repository, https://aphc.gov.in/docs/imp_judgements/Arjun%20Panditrao%20Khotkar%20_%20Kailash%20Kushanrao%20Gorantyal%20And%20Ors._1701334263.pdf.
- *Admissibility of Electronic Evidence Under the Indian Evidence Act, 1872*, Mondaq, <https://www.mondaq.com/india/disclosure-amp-electronic-discovery-amp-privilege/715108/admissibility-of-electronic-evidence-under-the-indian-evidence-act-1872>.
- *Shafhi Mohammad v. State of Himachal Pradesh*, CaseMine, <https://www.casemine.com/judgement/in/5ac9bf344a9326331c621b67>.
- *The Presumption That Computers Are Reliable*, Counsel Magazine (July 10, 2024), <https://www.counselmagazine.co.uk/articles/the-presumption-that-computers-are-reliable>.
- *Deepfakes on Trial: How Judges Are Navigating AI Evidence*, Thomson Reuters Institute (May 8, 2025), <https://www.thomsonreuters.com/en-us/posts/ai-in-courts/deepfakes-evidence-authentication/>.