CRYPTOGRAPHIC INTEGRITY VS. PROCEDURAL ACCESSIBILITY: ANALYZING SECTION 63(4) OF THE BHARATIYA SAKSHYA ADHINIYAM, 2023 IN THE WAKE OF PUNE BAR ASSOCIATION V. UNION OF INDIA

Rudra Prasad Rimal, LLM (Criminal Law), Faculty of Law,
ICFAI University, Gangtok, Sikkim.

ABSTRACT

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) introduced an elevated standard for the admissibility of secondary electronic evidence. Section 63(4) read with the Schedule of the BSA, requires the litigants to submit a Part A certificate disclosing the cryptographic hash value and Part B certificate requires expert certification. The Supreme Court in *Pune Bar Association v. Union of India & Ors.* (2026), while upholding the constitutional validity of this framework, reasoned that the hash values act as vital "digital fingerprints" necessary in order to combat the digital tampering, deepfakes, and Artificial Intelligence driven manipulation of evidence. The Court's decision by harmoniously interpreting Section 39(1) and 39(2) provides much-needed flexibility to expand the pool of eligible forensic experts beyond Section 79A of the IT Act. However, critical technical and practical ambiguities remained unaddressed. This article will examine the operational complexities arising due to mandatory hash value disclosure, particularly due to the fragility of digital metadata, the lack of standardized hashing algorithms (e.g., SHA-256 vs. MD5), and the procedural burden on ordinary, non-technical litigants. This article will compare the BSA's cryptographic mandates with international electronic evidence standards, viz; US Federal Rule of Evidence 902 and other international rules. Finally, this article in order to balance evidentiary integrity with constitutional access to justice will propose regulatory guidelines, algorithm standardization, and accessible forensic tooling.

Keywords: Bharatiya Sakshya Adhiniyam (BSA), Electronic Evidence, Hash Value, Cyber Forensics, Section 63(4), Deepfakes, Pune Bar Association, Digital Integrity.

1. Introduction & Background

a. The Shift to Digital Evidence and the Genesis of Section 63(4) BSA

In the era of the digital world, electronic records have evolved as a primary instrument of proof in courtrooms.[1] At the outset by introducing Section 65B into the Indian Evidence Act, 1872 (IEA) by amending the Information Technology Act, 2000 the Indian legal framework responded to much required digital shift.[2] Under section 65B secondary electronic evidence, requires a compliance certificate to verify the authenticity and proper operation of the computer system involved.[3][4] However, for more than two decades the judicial interpretation of Section 65B remained inconsistent. It see-saw from strict mandatory compliance in *Anvar P.V. v. P.K. Basheer* (2014)[5] to temporary relaxations in *Tomaso Bruno v. State of U.P.* (2015)[6] and *Shafhi Mohammad v. State of H.P.* (2018)[7], before ultimately getting stabilized under the Constitution Bench ruling in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020).[8] The vulnerabilities of Section 65B get exposed with the proliferation of advanced technologies like Artificial Intelligence, automated editing tools and deepfake generation. Rather than intrinsic verification of the digital file itself, the framework relied heavily on declarations of system integrity. The Indian Parliament repealed the Indian Evidence Act (IEA) and enacted Bharatiya Sakshya Adhiniyam, 2023 (BSA) recognizing that electronic records are a "unique species of evidence" inherently prone to subtle, non-evident mutation.

b. The New Statutory Mandate: Section 63(4) and the Schedule

Through Section 63(4) the BSA modernized the rules governing secondary electronic evidence.[9] Section 63(4) replaced the discretionary format under Section 65B with a mandatory, two-part standard-form certificate set out in the Schedule to the Act while retaining

[1] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (Academic Press, 4th edn., 2020) 15–34.
[2] Information Technology Act, 2000, No. 21 of 2000, s. 92 (inserting ss. 65A and 65B into the Indian Evidence Act, 1872).
[3] Justice Yatindra Singh, *Electronic Evidence* (Universal Law Publishing Co., 6th edn., 2023) 81–98.
[4] Avtar Singh, *Law of Evidence* (Central Law Publications, 25th edn., 2023) 563–570.
[5] (2014) 10 SCC 473
[6] (2015) 7 SCC 178
[7] (2018) 2 SCC 801
[8] (2020) 7 SCC 1
[9] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, s. 63(4).

the core requirement of a certification process :[10]

i) **Part A (Litigant Declaration & Hash Value):** It requires that the party generating the electronic record provide standard ownership/operational declarations, accompanied by the explicit disclosure of the record's hash value.[11]

ii) **Part B (Expert Certification):** It requires an additional declaration signed by an expert to validate the integrity and source of the electronic record.[12]

The main statutory objective while incorporating the hash value as described by the judiciary as a "digital fingerprint" is to establish a verifiable standard (mathematically) of the integrity of file from the moment it is extracted to its production in Court.[13]

Table 1: Evolution of Admissibility of Secondary Electronic Evidence under the Indian Evidence Act, 1872 and the Bharatiya Sakshya Adhiniyam, 2023[14]

EVOLUTION OF ADMISSIBILITY	
Indian Evidence Act, 1872 (Section 65B)	**BSA, 2023 (Section 63(4))**
Discretionary certificate structure	Mandatory statutory Schedule
Focus on system operational integrity	Focus on digital record integrity (Hash Value)
No cryptographic mandate	Part A: Hash disclosure
No explicit expert co-signature requirement	Part B: Expert signature

[10] Bharatiya Sakshya Adhiniyam, 2023, Sch. (Certificate under s. 63(4))
[11] Ministry of Home Affairs, Government of India, *The Bharatiya Sakshya Adhiniyam, 2023* (Act No. 47 of 2023), Schedule, Part A.
[12] Ministry of Home Affairs, Government of India, *The Bharatiya Sakshya Adhiniyam, 2023* (Act No. 47 of 2023), Schedule, Part B.
[13] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, Sch., Part A (requiring disclosure of the hash value in the certificate under s. 63(4)).
[14] Information Technology Act, 2000, No. 21 of 2000, s. 92 (inserting ss. 65A and 65B into the Indian Evidence Act, 1872); Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, s. 63(4) and Sch.; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1; Justice Yatindra Singh, *Electronic Evidence* (Universal Law Publishing Co., 6th edn., 2023) 215–230.

c. Constitutional Challenge and the Pune Bar Association Ruling

Enforcing Section 63(4) prompted widespread skepticism within legal circles regarding its accessibility for ordinary litigants.[15] In *Pune Bar Association v. Union of India & Ors.* (Writ Petition (Civil) No. 599 of 2026), the petitioner challenged Section 63(4) and its Schedule as unconstitutional, arguing that mandatory hash value generation (Part A) and expert verification (Part B) imposed an unduly onerous, arbitrary, and unjust burden on ordinary citizens.[16] While disposing of the petition on May 22, 2026, a Supreme Court Bench upheld the provision's validity, observing that the cryptographic hashing has a rational nexus with the legislative objective of preventing digital tampering in an era of sophisticated deepfakes. The Court adopted a harmonious construction of Section 39 of the BSA to prevent administrative bottlenecks regarding expert certification and clarify that Part B need not be restricted solely to government-notified examiners. While the ruling settled the question of constitutional validity, it opened up critical questions regarding cryptographic standards, forensic procedure, and evidentiary accessibility, the central themes analyzed in this paper.

2. Deconstructing the Supreme Court Order

a. The Constitutional Threshold & Manifest Arbitrariness

In *Pune Bar Association v. Union of India*, the petitioner challenged the new requirements primarily on the ground of manifest arbitrariness under Article 14 of the Constitution of India. According to the petitioner, requiring ordinary litigants to generate cryptographic hash values (Part A) and obtain expert co-signatures (Part B) placed an excessive and, in many cases, unrealistic burden on individuals seeking to rely on electronic evidence. This, it was argued, effectively restricted access to justice by making it difficult for litigants to present crucial digital evidence before the courts. The Supreme Court, however, rejected this argument. In its reasoning, the Court highlighted the changing nature of digital forensics and the growing risks associated with electronic evidence. It observed that electronic records constitute a "unique species of evidence" because they are inherently vulnerable to continuous

[15] *Pune Bar Association v. Union of India & Ors.*, Writ Petition (Civil) No. 599 of 2026, order dated 22 May 2026 (SC) (observing the challenge to the practical implementation of s. 63(4) of the Bharatiya Sakshya Adhiniyam, 2023).

[16] *Pune Bar Association v. Union of India & Ors.*, Writ Petition (Civil) No. 599 of 2026, order dated 22 May 2026 (SC), paras 1 & 4 (recording the petitioner's contention that mandatory disclosure of the hash value under Part A and expert certification under Part B imposed an onerous burden, and upholding the provision as having a rational nexus with the object of ensuring authenticity and integrity of electronic records).

and often undetectable alteration. Referring to the rapid advancement of artificial intelligence (AI) and deepfake technologies, the Bench further observed:

"*Such fast and varied transformation in technology necessitated reviewing the erstwhile Evidence Act... Hash value of an electronic data is synonymous with an electronic fingerprint and provides a sure way of identifying and verifying digital data. The necessity of incorporating the hash value... cannot be said to lack a rational nexus with the object of the Act.*"

The Court held that the requirement of furnishing hash values under Section 63(4) is directly connected to the legitimate objective of safeguarding the integrity and authenticity of electronic evidence, particularly in light of the increasing risks posed by AI-driven manipulation. Since the provision bears a clear and rational nexus to the objectives of the Bharatiya Sakshya Adhiniyam (BSA), it does not satisfy the stringent standard required to establish manifest arbitrariness under Article 14.

b. The Expert Dilemma: Resolving R. v. B & Anr. via Harmonious Construction

The petitioner also identified a significant practical obstacle in the requirement under Part B of the Schedule, which mandates that the secondary evidence certificate be signed by an expert. In support of this argument, the petitioner relied on the *R. v. B & Anr.* (2024) decision of the Madras High Court, which held that Part B could be completed only by an Examiner of Electronic Evidence formally notified under Section 79A of the Information Technology Act, 2000.[17] The petitioner argued that this interpretation created a serious practical difficulty. Since only a handful of government agencies across India have been notified as Section 79A Examiners of Electronic Evidence, insisting that only such authorities could sign Part B of the certificate would have led to significant institutional delays and made compliance with Section 63(4) virtually impossible in many cases. The Supreme Court resolved this issue by identifying a key flaw in the Madras High Court's interpretation. It observed that the High Court had confined its analysis to Section 39(2) of the Bharatiya Sakshya Adhiniyam (BSA), which expressly refers to Examiners of Electronic Evidence notified under Section 79A of the

[17] *R. v. B*, 2024:MHC:5028 (Mad), CRP (MD) No. 2362 of 2024, decided on 30 October 2024, paras 5–6 (holding that Part B of the certificate under s. 63(4) of the Bharatiya Sakshya Adhiniyam, 2023 must be completed by an Examiner of Electronic Evidence notified under s. 79A of the Information Technology Act, 2000).

Information Technology Act, 2000, while overlooking the broader language of Section 39(1). Reading Sections 39(1) and 39(2) together, the Supreme Court clarified that:

i) **Section 39(1)** is a general provision admitting the opinions of any individuals possessing "special skill" in relevant fields, including computer science and cyber forensics.

ii) **Section 39(2)** is an enabling provision granting automatic relevance to opinions from Section 79A notified examiners, but it lacks a non-obstante clause that would otherwise exclude the application of sub-section (1).

Consequently, the Court held that any private practitioner, forensic consultant, or computer expert who demonstrates "special skill and expertise" to the court's satisfaction based on "unimpeachable material" can sign Part B of the Schedule. The finding in R. v. B & Anr., was explicitly declared to have no binding precedential value.

c. The Unanswered Legal Questions

Although the Supreme Court successfully defused the immediate administrative bottleneck, its procedural solution does not conclusively settle the underlying legal and technical complexities, leaving substantial questions for future judicial consideration:

i) **Unsettled Precedent:** Since the Bench neither issued notice to the Union of India nor delivered a final constitutional ruling, it deliberately left the central question of law unresolved. As a result, trial courts must determine the qualifications and competence of experts under Section 39(1) on a case-by-case basis, without the benefit of uniform statutory or judicial guidelines. This lack of standardized criteria creates uncertainty in the application of the provision and leaves considerable discretion in the hands of individual courts.

ii) **Judicial Discretion versus Technical Rigor:** By shifting the standard for determining who qualifies as an "expert" under Part B from government-accredited Examiners of Electronic Evidence under Section 79A of the Information Technology Act to experts whose credentials satisfy the court on the basis of "unimpeachable material," the Supreme Court has introduced a significant element of judicial discretion into the assessment of cyber forensic expertise. While this

approach enhances procedural flexibility, it also raises concerns about the absence of uniform standards for evaluating technical qualifications. This uncertainty forms the foundation of the technical and procedural critiques examined in the subsequent sections of this study.

3. Cryptographic Mechanics & Operational Hardships

a. Hashing Mechanics and the Illusion of Immutability

Cryptographic hash functions are deterministic algorithms designed to take an input of arbitrary size such as a PDF, JPEG image, or MP4 video and transform it into a fixed-size string of characters.[18] In theory, a cryptographic hash acts as an unforgeable "digital fingerprint".[19] If even a single bit of data within a file is modified, the hash output changes completely (a phenomenon known as the *avalanche effect*).[20] While the Supreme Court in *Pune Bar Association* rightly recognized the theoretical strength of hash values in identifying deepfakes and manipulated records,[21] the practical realities of handling digital files introduce significant friction.[22] Digital evidence is volatile. Everyday interactions, such as sending a media file over instant messaging platforms like WhatsApp, attaching an audio recording to an email, or simply opening a file in a different operating system, routinely alter file metadata (e.g., *Date Modified*, *Last Accessed*, or EXIF tags).[23][24] Although the core visual or auditory content of the file remains identical, these background metadata shifts produce a completely different hash value. Under a rigid interpretation of Section 63(4) BSA, a litigant who generates a hash value at the point of receipt and another at the time of submission in court may face rejection of secondary evidence due to an apparent "hash mismatch," even where no substantive

[18] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (Academic Press, 4th edn., 2020) 168–175.
[19] Jason Sachowski (ed.), *Implementing Digital Forensic Readiness: From Reactive to Proactive Process* (Syngress, 2016) 48–55.
[20] National Institute of Standards and Technology (NIST), *Secure Hash Standard (SHS)*, FIPS PUB 180-4 (U.S. Department of Commerce, August 2015) 1–7.
[21] *Pune Bar Association v. Union of India & Ors.*, Writ Petition (Civil) No. 599 of 2026, order dated 22 May 2026 (SC), para 4.
[22] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (Academic Press, 4th edn., 2020) 67–85.
[23] Brian Carrier, *File System Forensic Analysis* (Addison-Wesley Professional, 2005) 15–39.
[24] Jason Sachowski (ed.), *Implementing Digital Forensic Readiness: From Reactive to Proactive Process* (Syngress, 2016) 72–91.

tampering has occurred.[25]

b. Legislative Ambiguity: The Missing Algorithm Standard

A significant technical limitation within Section 63(4) of the BSA and Part A of its Schedule is the absence of any express specification regarding the cryptographic hash algorithm that must be used for generating hash values. While the provision requires parties to disclose the hash value of electronic evidence, it remains silent on the underlying technical standard or methodology to be adopted. This lack of clarity creates uncertainty because not all hashing algorithms provide the same level of security or reliability. Older algorithms, such as MD5 and SHA-1, have known vulnerabilities and are no longer considered suitable for ensuring the integrity of digital evidence, whereas modern algorithms such as SHA-256 and SHA-3 offer significantly stronger protection against manipulation. Without a legally prescribed standard, different courts and litigants may rely on varying levels of cryptographic assurance, potentially leading to inconsistent forensic practices and uncertainty in the assessment of electronic evidence. Establishing clear algorithmic standards is therefore essential to ensure that the requirement of hash disclosure achieves its intended purpose of protecting evidentiary integrity rather than becoming a merely formal compliance exercise.

[25] International Organization for Standardization (ISO), *ISO/IEC 27037:2012—Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence* (ISO, 2012) 14–24.

Table 2: Comparative Assessment of Common Hashing Algorithms for Electronic Evidence Authentication

Hashing Algorithm	Output Length	Cryptographic Status	Risk in Evidentiary Context
MD5[26]	128 bits	Cryptographically Broken	Highly susceptible to collision attacks (different files generating the same hash).
SHA-1[27]	160 bits	Deprecated / Vulnerable	Demonstrated collision vulnerabilities; unsafe for legal proof.
SHA-256 (SHA-2)[28]	256 bits	Industry Standard	Highly secure; computationally infeasible to forge or collide.
SHA-3[29]	Variable	Advanced Standard	Next-generation security; less commonly implemented in consumer software.

Without a statutory baseline (such as mandating SHA-256 or higher), parties in litigation may submit hash values generated via legacy algorithms like MD5 or SHA-1.[30][31] Opposing parties can exploit known collision vulnerabilities to challenge the evidentiary integrity of such records.[32] Conversely, if opposing parties use different algorithms for the same underlying file, trial courts will lack a unified benchmark to compare the submitted outputs.[33]

[26] Ronald L. Rivest, *The MD5 Message-Digest Algorithm*, RFC 1321 (Internet Engineering Task Force, April 1992).
[27] National Institute of Standards and Technology (NIST), *Secure Hash Standard (SHS)*, FIPS PUB 180-4 (U.S. Department of Commerce, August 2015); Marc Stevens, Pierre Karpman and Thomas Peyrin, 'Freestart Collision for Full SHA-1' in *Advances in Cryptology – EUROCRYPT 2016* (Springer, 2016) 459–483.
[28] National Institute of Standards and Technology (NIST), *Secure Hash Standard (SHS)*, FIPS PUB 180-4 (U.S. Department of Commerce, August 2015)
[29] National Institute of Standards and Technology (NIST), *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, FIPS PUB 202 (U.S. Department of Commerce, August 2015).
[30] National Security Agency (NSA), *Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ* (National Security Agency, 2022) (recommending the use of SHA-256 and stronger hash algorithms for security-sensitive applications).
[31] International Organization for Standardization, *ISO/IEC 10118-3:2018—Information Technology—Security Techniques—Hash Functions—Part 3: Dedicated Hash Functions* (ISO, 2018).
[32] Xiaoyun Wang and Hongbo Yu, 'How to Break MD5 and Other Hash Functions' in Ronald Cramer (ed.), *Advances in Cryptology – EUROCRYPT 2005* (Springer, 2005) 19–35.
[33] National Institute of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders* (2nd edn., U.S. Department of Justice, 2008) 24–27 (emphasizing the importance of using consistent forensic methodologies, including hash verification, to preserve the integrity of digital evidence).

c. Litigation Hardships & Access to Justice

While expert forensic examiners possess write-blockers, hash-calculating software, and sterile lab environments, ordinary citizens and non-technical litigants do not.[34] The procedural imposition under Section 63(4) Part A creates several practical hurdles:

i) **The Non-Technical Litigant Barrier:** An ordinary litigant seeking to produce routine digital evidence such as SMS threads, call recordings, or bank statements rarely possesses the technical knowledge to calculate cryptographic hashes without specialized software.[35]

ii) **Chain-of-Custody Inadvertent Breaches:** Attempting to extract a hash without proper forensic write-blocking software can inadvertently modify access timestamps or other metadata and, if the file is altered during handling, compromise the integrity of the evidence and the reliability of any subsequently generated hash value.[36][37]

iii) **Economic Cost of Part B Compliance:** Even with the Supreme Court expanding the expert pool under Section 39(1) BSA, requiring a private cyber forensic expert to sign Part B for routine litigation imposes disproportionate financial burdens, disproportionately impacting self-represented or low-income litigants.

Far from being a mere procedural checklist, mandatory hash disclosure risks becoming a technological barrier to court access unless complemented by standardized software tools and judicial guidelines.

4. Comparative Global Frameworks

To assess the practical effectiveness of Section 63(4) of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), it is useful to examine how other jurisdictions reconcile the need to preserve the integrity of electronic evidence with the goal of ensuring procedural accessibility. Although many foreign legal systems also rely on cryptographic hashing to establish the

[34] Darren R. Hayes, *A Practical Guide to Computer Forensics Investigations* (Pearson Education, 2nd edn., 2015) 27–46
[35] George L. Paul, *Foundations of Digital Evidence* (American Bar Association, 2nd edn., 2017) 103–118.
[36] Kruse II Warren G. and Jay G. Heiser, *Computer Forensics: Incident Response Essentials* (Addison-Wesley Professional, 2nd edn., 2002) 73–90.
[37] Harlan Carvey, *Windows Forensic Analysis Toolkit* (Syngress, 4th edn., 2014) 35–56.

authenticity and integrity of digital records, they generally do not treat the generation of hash values as a mandatory or inflexible precondition for admissibility. Instead, they adopt more flexible approaches that balance technical reliability with the practical realities of litigation.

a. United States: Flexible Self-Authentication under FRE 902(13) and 902(14)

In the United States federal legal system, the authentication of digital evidence underwent significant modernization through the addition of Rules 902(13) and 902(14) to the Federal Rules of Evidence (FRE).[38]

- **Rule 902(13):**The provision applies to records produced by an electronic process or system and allows them to be self-authenticated through a written certification by a qualified person, thereby dispensing with the requirement of live courtroom testimony to establish their authenticity. [39]

- **Rule 902(14):** The provision specifically applies to digital copies extracted from electronic devices or storage media. It permits these copies to be self-authenticated when they are verified through a recognized process of digital identification, expressly including the use of cryptographic hash values such as SHA-256 to establish their authenticity and integrity. [40]

Key Differences from BSA Section 63(4):

i) **Self-Authentication as an Option, Not a Bar:** Under FRE 902, providing a cryptographic hash certification is a permissive mechanism to streamline authentication. If a party fails to generate a hash, the evidence is not automatically excluded. The proponent can still authenticate the evidence through traditional circumstantial methods under FRE 901 (such as witness testimony or system logs).[41] In

[38] Federal Rules of Evidence, Rules 902(13) & 902(14), as amended with effect from 1 December 2017.
[39] Advisory Committee on Evidence Rules, *Report of the Advisory Committee on Evidence Rules* (Judicial Conference of the United States, 5 May 2016) 13–21 (explaining the rationale for Rule 902(13) and the concept of certification by a qualified person).
[40] Advisory Committee Notes to the 2017 Amendment to Rule 902, Federal Rules of Evidence (recognising that digital identification by comparison of hash values permits self-authentication of electronic evidence); Christopher B. Mueller and Laird C. Kirkpatrick, *Federal Evidence* (4th edn., Wolters Kluwer, 2018) Vol. 5, §§ 9:66–9:68.
[41] Federal Rules of Evidence, r. 901(a); Edward J. Imwinkelried, *Evidentiary Foundations* (LexisNexis, 10th edn., 2018) 233–255.

contrast, BSA Section 63(4) operates as an exclusionary gateway for secondary electronic records.[42]

ii) **Standardized Hash Recognition:** The US Advisory Committee Notes expressly acknowledge the use of modern cryptographic standards, including algorithms such as SHA-256, while also recognizing that older algorithms like MD5 and SHA-1 have been deprecated due to their reduced reliability for forensic verification. This distinction, which reflects the evolving nature of digital forensic practices, is notably absent from the Schedule to the BSA.[43]

b. United Kingdom: Chain-of-Custody and Evidentiary Weight

In the United Kingdom, the admissibility of electronic evidence across civil and criminal proceedings is governed by a combination of statutory rules and established forensic practice guides:[44]

i) **ACPO / NPCC Good Practice Guide for Digital Evidence:** Principle 1 mandates that no action taken by law enforcement or forensic examiners should change data held on a device. Principle 3 requires an audit trail allowing an independent expert to re-examine the process and achieve identical results.[45]

ii) **Criminal Procedure Rules & PACE 1984:** Under Section 78 of the Police and Criminal Evidence Act 1984 (PACE), UK courts retain discretion to exclude evidence if its admission would adversely affect the fairness of proceedings.[46]

iii) **Civil Procedure Rules (CPR Part 31):** Electronic disclosure mandates establishing a documented, verifiable chain of custody.[47]

[42] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, s. 63(4) read with the Schedule.

[43] Advisory Committee on Evidence Rules, *Federal Rule of Evidence 902(14) Advisory Committee Note*, 2017, available at United States Courts, https://www.uscourts.gov/rules-policies/archives/rules-evidence (last visited 27 July 2026).

[44] Paul Roberts and Adrian Zuckerman, *Criminal Evidence* (3rd edn., Oxford University Press, 2023) 1083–1118.

[45] National Police Chiefs' Council (NPCC), *Good Practice Guide for Digital Evidence* (Version 7.0, 2020) Principles 1 & 3.

[46] Police and Criminal Evidence Act 1984, c. 60, s. 78; Criminal Procedure Rules 2020, SI 2020/759.

[47] Civil Procedure Rules 1998, Pt. 31; Sir Geoffrey Vos (ed.), *Disclosure* (White Book Service, Sweet & Maxwell, 2024).

Key Differences from BSA Section 63(4):

Unlike the mandatory dual certification mandated by the BSA Schedule, UK courts differentiate between the admissibility of a digital record and its probative weight.[48] Hashing is treated as standard forensic best practice during data acquisition and preservation of digital evidence.[49] However, if an ordinary litigant produces an un-hashed digital document or media file, UK courts evaluate its authenticity by examining the overall chain of custody and surrounding circumstances, rather than barring the evidence at the threshold for procedural non-compliance.[50]

c) Key Policy Takeaways for Indian Jurisprudence

Comparative analysis reveals that mature common-law jurisdictions treat cryptographic hashing as a trusted tool for self-authentication rather than an inflexible procedural barrier:

i) **Separating Integrity Verification from Admissibility Requirements:** Although providing cryptographic hash values is an effective way to ensure that electronic evidence has not been altered, making it a mandatory requirement in every case may create unnecessary barriers. Such a rigid approach could prevent courts from considering genuine and untampered secondary evidence, particularly when it is presented by ordinary litigants who may lack technical expertise or access to specialized forensic resources.

ii) **Need for Statutory Flexibility:** India's evidentiary framework could benefit from adopting a more flexible approach similar to the model under **FRE 902(14)** in the United States, where hash verification serves as a convenient and reliable method for establishing the authenticity of electronic records when available, while other forms of authentication remain permissible where strict technical compliance is impractical or impossible. This approach would preserve evidentiary integrity without creating unnecessary barriers for litigants seeking to rely on genuine digital evidence.

[48] Colin Tapper, *Cross and Tapper on Evidence* (13th edn., Oxford University Press, 2018) 136–145.
[49] Forensic Science Regulator, *Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System* (Version 2, 2023) Pt. FSA 1000 (Digital Forensics).
[50] Stephen Mason and Daniel Seng (eds.), *Electronic Evidence and Electronic Signatures* (7th edn., Institute of Advanced Legal Studies, School of Advanced Study, University of London, 2024) Chs. 4 & 5.

5. Reform Recommendations & Conclusion

a. Pragmatic Recommendations for Reform

To bridge the gap between the cryptographic objectives of Section 63(4) of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) and ground-level litigation realities, targeted legislative amendments, administrative frameworks, and judicial guidelines are necessary:

i) Statutory Specification of Cryptographic Standards: Parliament or the Ministry of Electronics and Information Technology (MeitY) should consider issuing standardized guidelines specifying the cryptographic hash algorithms that may be relied upon for evidentiary purposes. Older algorithms such as MD5 and SHA-1, which are vulnerable to collision attacks and are no longer considered suitable for forensic verification, should be expressly excluded. Establishing a uniform requirement based on secure algorithms such as SHA-256 or stronger standards would reduce uncertainty, promote consistency in forensic practices, and ensure a more reliable approach to the evaluation of electronic evidence across Indian courts.

ii) Provision of Publicly Accessible Hashing Tools: To reduce the practical burden on ordinary litigants, state governments and the e-Courts initiative should consider incorporating standardized, user-friendly hash generation and verification tools into official court portals. Providing secure and open-source utilities would allow self-represented and non-technical litigants to generate and verify hash values accurately without the risk of unintentionally altering electronic files or bearing the additional costs associated with professional forensic services. Such measures would improve accessibility while preserving the integrity requirements of electronic evidence.

iii) Standardized Judicial Guidelines for Expert Credentials under Section 39(1): Following the Supreme Court's harmonious interpretation of Sections 39(1) and 39(2) of the BSA in *Pune Bar Association*, trial courts require clear and objective criteria for assessing the competence of private experts. High Courts, exercising their rulemaking powers, should consider prescribing minimum qualifications and professional standards for experts authorized to sign Part B of the Schedule. These standards may include relevant educational qualifications, recognized certifications such as Certified Cybersecurity Expert (CCE) or Computer Hacking Forensic Investigator (CHFI), or postgraduate qualifications

in cyber forensics and related disciplines. Establishing such benchmarks would promote consistency, reduce uncertainty, and ensure that expert certification is based on demonstrable technical competence.[51]

iv) Legislative Carve-Out for Primary Electronic Evidence and Low-Value Litigation: To avoid unnecessary procedural burdens, Section 63(4) should be clarified to provide that where primary electronic evidence is produced directly from an original device that has not been tampered with, or in summary and small-claims proceedings, the requirement of dual certification and mandatory hash disclosure may be relaxed at the discretion of the court. Such relaxation should remain subject to the condition that the opposing party has not specifically disputed the authenticity or integrity of the electronic record. This approach would maintain evidentiary safeguards while preventing procedural requirements from becoming disproportionate barriers to access to justice.

5.2 Conclusion

The Supreme Court's decision in *Pune Bar Association v. Union of India* represents a significant development in Indian evidence law. By upholding the constitutional validity of Section 63(4) and the accompanying Schedule of the BSA, the Court recognized that, in an era increasingly shaped by AI-generated deepfakes and the continuous vulnerability of digital records to alteration, conventional evidentiary safeguards may no longer be sufficient. Cryptographic hash values function as essential "digital fingerprints," providing a reliable mechanism to preserve the integrity and authenticity of secondary electronic evidence. The Court's pragmatic interpretation of Sections 39(1) and 39(2) further prevented a potential administrative deadlock that could have arisen if expert certification had been limited exclusively to entities accredited under Section 79A of the Information Technology Act.

However, the effectiveness of statutory safeguards ultimately depends on their practical accessibility. As this study demonstrates, mandatory cryptographic requirements, if implemented without adequate support mechanisms, may unintentionally create procedural barriers for non-technical litigants. To ensure that technological rigor does not undermine access to justice, the framework requires complementary measures such as clear standards for

[51] International Association of Computer Investigative Specialists (IACIS), *Certified Forensic Computer Examiner (CFCE) Certification Program* (describing the competency-based certification process and core digital forensic competencies expected of certified examiners).

permissible cryptographic algorithms, publicly accessible verification tools, and consistent judicial guidelines for assessing expert competence. With these reforms, the Indian evidentiary system can achieve a sustainable balance between maintaining the integrity of digital evidence and preserving the constitutional commitment to fair and accessible justice.