ADMISSIBILITY OF ELECTRONIC RECORD AND THE DUAL-CERTIFICATION REGIME UNDER BSA, 2023

Mridul Bhatt, LL.M. (Cyber and Security Law),
ICFAI University Dehradun, Uttarakhand, India[1]

ABSTRACT

The Bharatiya Sakshya Adhiniyam, 2023 marks a foundational shift in the law of electronic evidence in India by elevating admissibility from a question of mere relevance to one of demonstrable process integrity. Under Section 63(2), the legislature has substantially retained the four-fold conditions established under the earlier Section 65B of the Indian Evidence Act, namely, regular use of the device, feeding of information in the ordinary course, proper functioning of the system during the material period, and faithful reproduction of the original record. These conditions are not procedural ornaments; they are substantive filters designed to ensure that what enters the judicial record as a digital output is, in fact, a reliable representation of an underlying truth. Section 63(4) reinforces this framework by mandating a certificate as a condition precedent to admissibility. The Supreme Court's reasoning in Anvar P.V. v. P.K. Basheer and the further clarification in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal established that certification cannot be treated as an optional or dispensable formality. The BSA deepens this requirement through the Schedule, which bifurcates the certificate into Part A, to be furnished by the party in possession of the device or data, and Part B, to be endorsed by a qualified expert. This dual-certification model reflects a deliberate legislative choice to strengthen the authentication chain.

However, the architecture creates a jurisprudential tension between formal compliance and substantive justice. Where delayed expert endorsement or cloud-based storage makes strict compliance difficult without prejudice, courts must adopt a purposive construction, treating incurable absence of the certificate as fatal while permitting curable delays on demonstrable and recorded grounds, so that process integrity and fair trial are protected simultaneously.

Keywords: Electronic records; Section 63, BSA 2023; Admissibility of digital evidence; Mandatory certificate; Dual-certification regime; Forensic authentication

[1] LL.M. Cyber and Security Law, ICFAI University Dehradun, Uttarakhand, India

1.1. The Mechanics of Admissibility: Conditions under Section 63(2)

The operationalization of the *Bharatiya Sakshya Adhiniyam (BSA), 2023*, hinges fundamentally on the precise mechanics of admissibility codified under Section 63[2]. This provision serves as the new statutory "gatekeeper," regulating the entry of electronic records into the judicial domain. In the transition from the *Indian Evidence Act (IEA)* to the BSA, the legislature has attempted to move beyond the rigid, hardware-centric view of the past to a more process-oriented approach. While Section 57 creates the potential for digital files to be classified as "Primary Evidence," Section 63(2) establishes the substantive physiological conditions that transform a mere digital output into admissible evidence.

The admissibility of electronic records is no longer a matter of mere production; it is a question of process integrity. Under Section 63(2), the law stipulates a quartet of conditions that mirror, yet refine, the erstwhile requirements of Section 65B (2) of the IEA. These conditions mandate that the computer output must be produced by a device used regularly to store or process information for lawful activities; that the information must be fed into the computer in the ordinary course of those activities; that the computer must be operating properly during the material period; and that the output must be a faithful reproduction of the electronic record[3].

However, in the "post-BSA era" of 2026, the interpretation of these conditions has evolved significantly. The judicial focus has shifted from the mere regularity of use—a concept suited for mainframes and office desktops—to the "sanctity of the bitstream" processed by decentralized networks. The condition requiring the computer to be "operating properly" is particularly litigious in the age of malware and remote hacking. Courts are now increasingly tasked with verifying not just the device's history, but the integrity of the automated process itself. The defence bar in 2026 frequently argues that a device infected with malware, even if functioning "properly" in its mechanical sense, fails the condition of reliability under Section 63(2). Thus, Section 63(2) acts not merely as a checklist but as a robust forensic filter, intended to prevent data contamination from entering the evidentiary record before it even reaches the stage of certification.

Furthermore, the "lawful control" requirement under this section creates a complex friction when applied to cloud-based evidence. When data resides on a third-party server (e.g., AWS or

[2] The Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India), Section 63
[3] The Bharatiya Sakshya Adhiniyam, 2023, Section 63(2)

Google Cloud), the user may have "lawful access," but arguably not "lawful control" over the physical hardware. This distinction creates a jurisprudential gap where the mechanical conditions of admissibility—drafted with physical devices in mind—struggle to encompass virtualized storage environments. Consequently, Section 63(2) requires a purposive interpretation, where "control" is read as control over the *data credentials* rather than the *silicon chips*.

1.2. The Mandatory Certificate: Critical Analysis of Section 63(4)

If Section 63(2) provides the mechanical prerequisites, Section 63(4) imposes the procedural mandate. This subsection stipulates that any electronic record sought to be used as evidence "shall" be accompanied by a certificate signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities[4]. The use of the mandatory auxiliary "shall," reinforced by the Supreme Court's foundational precedent in *Anvar P.V. v. P.K. Basheer* (2014)[5], cements the certificate as a non-negotiable condition precedent for admissibility.

The jurisprudential journey to this mandatory requirement has been tumultuous. The "Liberal Era," characterized by *State (NCT of Delhi) v. Navjot Sandhu* (2005)[6], allowed for the bypassing of this certificate if the evidence appeared authentic. This approach, while pragmatic, was deemed legally unsound as it allowed secondary evidence to bypass the special safeguards created for digital fragility. The BSA 2023 firmly rejects the *Navjot Sandhu* logic. By codifying the mandatory nature of the certificate in Section 63(4), the legislature has signalled that in the digital domain, "procedure is the handmaiden of justice" only when that procedure ensures the veracity of the evidence.

However, the BSA introduces a critical, and perhaps controversial, evolution in this mandate. Unlike the singular certification of the past (under Section 65B of the IEA), Section 63(4) structures a more rigorous validation protocol intended to curb the submission of manipulated data. This legislative intent, while noble, has drawn sharp criticism for creating a "procedural rigidity" that may prioritize form over substance. Legal scholars argue that this strict adherence risks creating a "Trial by Certificate" In this scenario, substantive justice is held hostage to the

[4]The Bharatiya Sakshya Adhiniyam, 2023, Section 63(4)
[5] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473
[6] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600

technical availability of a certification document. If a prosecutor possesses a video clearly depicting a homicide, but lacks the Section 63(4) certificate due to a bureaucratic delay, the evidence is inadmissible. This creates a paradox where the "truth" is visible to the court but legally invisible to the judgment.

Moreover, the "Mandatory Certificate" regime assumes a chain of custody that is unbroken and documented. In reality, investigating agencies often seize devices in a haphazard manner. The certificate is often drafted *post-facto*, months after the seizure, by an officer who may not recall the specific state of the device. This turns the certification process into a "performative ritual" rather than a genuine guarantee of integrity. The critique in 2026 is that Section 63(4) has become a check-box exercise that validates the *file format* but fails to interrogate the *content veracity*, leaving the system vulnerable to the "Liar's Dividend" where formal compliance masks substantive fabrication.

1.3. The Dual-Signature Requirement: Roles of the Custodian vs. the Forensic Expert

The most contentious innovation of the BSA framework, and the focal point of current litigation, is the introduction of the "Dual-Certification" or "Two-Part Certificate" regime. Section 63(4) explicitly bifurcates the responsibility of authentication, requiring signatures from two distinct entities: the "Custodian" (the user/owner of the device) and the "Forensic Expert"[7].

This dual-signature requirement was introduced to add a layer of expert verification to the user's affirmation. Theoretically, this acts as a "double-lock" on the evidence: the user confirms the source, and the expert confirms the technical integrity. However, in practice, this requirement has created a significant "Expert Bottleneck" within the criminal justice system.

The Custodian: The first signatory is the person in charge of the computer system (the Custodian). Their role is to attest that the device was under their lawful control and that the data was generated during the ordinary course of business. This is a continuation of the old Section 65B (4) requirement.

The Forensic Expert: The second signatory creates the bottleneck. The BSA mandates that the certificate must also be signed by an expert, specifically one notified under Section 79A of

[7] The Bharatiya Sakshya Adhiniyam, 2023, Section 63(4)

the *Information Technology Act, 2000*. This provision has disastrous logistical implications. As noted in recent judicial trends, specifically, there is a chronic and severe deficit of notified forensic experts across India.

This shortage creates an "Administrative Bottleneck" where the legal process is effectively paused, waiting for an expert signature. Investigating officers are finding themselves in a queue, sometimes lasting months, to get a Section 63(4) countersignature from a Central Forensic Science Laboratory (CFSL) or State Forensic Science Laboratory (SFSL).

Furthermore, this regime introduces a profound legal liability paradox. The expert is required to sign a certificate vouching for the integrity of data on a device they did not personally seize or maintain in the chain of custody. They are essentially certifying a "black box" based on a hash value generated at the lab. If it is later revealed that the device was tampered with *during transit* between the police station and the lab, the expert who signed the certificate faces potential cross-examination and liability for certifying a compromised device. This "remote certification" dilemma makes experts hesitant to sign, further exacerbating the bottleneck.

Consequently, the dual-signature requirement, intended to be a shield against tampering, has become a sword that cuts into the efficiency of the trial process. It forces the defence to attack the *absence* of the second signature rather than the content of the evidence, leading to acquittals based on technical non-compliance rather than innocence.

1.4. The Timing of Filing: Admissibility at the stage of Charge Sheet vs. Trial

The procedural ambiguity regarding *when* this certificate must be filed has been a subject of intense judicial scrutiny in the post-BSA era. Drawing from the *Arjun Panditrao* synthesis[8], the settled position in 2026 is that the certificate should ideally accompany the electronic record when produced in court, typically at the stage of filing the charge sheet.

The rationale for this timing is grounded in the principle of "fair trial" and "disclosure." The accused has a right to know the full extent of the evidence against them at the earliest stage. If the prosecution holds back the certificate until the final arguments, the defence is denied the opportunity to challenge the certificate's validity or cross-examine the signatories. Therefore,

[8] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1

the general rule is "filing at first instance."

However, the rigidity of this timeline is often tested by the forensic realities of the BSA regime. Given the "Administrative Bottleneck" caused by the shortage of experts, investigating agencies frequently struggle to procure the expert signature by the time the statutory period for filing the charge sheet (60 or 90 days) expires. Consequently, courts are frequently petitioned to condone delays.

This creates a friction between the accused's right to a speedy trial and the prosecution's need for procedural compliance. The judiciary is forced to balance the strict mandate against the pragmatic necessity of justice. Emerging jurisprudence suggests that while the certificate *must* exist to make the evidence admissible, its production can be delayed if the prosecution can demonstrate "sufficient cause." Courts are distinguishing between a "fatal defect" (non-existence of the certificate) and a "curable defect" (delayed production). Yet, this flexibility is a double-edged sword; it allows the prosecution to patch up investigations retrospectively, potentially undermining the rigorous standards the BSA sought to impose.

1.5. Judicial Discretion: Can the Court dispense with the Certificate in 2026?

A critical question facing the judiciary in the BSA era is the extent of judicial discretion to dispense with the Section 63(4) certificate entirely. While *Anvar P.V.* seemingly closed the door on non-certified evidence, the *Arjun Panditrao* judgment left a specific window open: the doctrine of "impossibility of performance" (*lex non cogit ad impossibilia*)[9].

In 2026, this doctrine is invoked more frequently than anticipated. The question arises: If a party has done everything possible to obtain a certificate—specifically the expert signature required by the dual-certification regime—but fails due to the systemic shortage of experts or the refusal of a third-party service provider (like WhatsApp or Google) to cooperate, does the law demand the impossible?

Recent trends suggest that courts, facing the "Section 79A shortage", may be moving towards a doctrine of "substantial compliance." In cases where the "Expert Bottleneck" makes strict compliance impossible, courts are beginning to ask if the authenticity of the data can be

[9] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (referencing the maxim lex non cogit ad impossibilia)

established through other corroborative means, such as hash value matching or oral testimony of the seizure officer.

This represents a potential return to a "modified *Navjot Sandhu*" approach, albeit under a different guise. If the judiciary allows the dispensing of the certificate due to administrative failure, it effectively nullifies the legislative intent of Section 63(4). Conversely, if they strictly enforce it, thousands of cases may collapse. Thus, judicial discretion in 2026 is a volatile battleground, balancing the "Best Evidence Rule" against the pragmatic collapse of forensic infrastructure. The current consensus is that while the court *can* dispense with the certificate in rare cases of "impossibility," this discretion must be exercised sparingly to prevent the exception from swallowing the rule.

Conclusion

Section 63 of the BSA, 2023 represents a serious legislative attempt to ensure that electronic records enter the evidentiary record only when their source, method, and integrity are properly established. The dual-certification structure has the potential to strengthen confidence in digital proof, yet an overly mechanical application may shift litigation from the truth of the record to the technical sufficiency of the certificate. The preferable judicial approach is one that remains strict about authenticity, but measured about timing and curability where the statutory safeguard is ultimately satisfied without prejudice to the accused or the opposite party.

Suggestion

Having examined the structural design and operational difficulties of the dual-certification regime under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, the author respectfully offers the following suggestions for legislative, institutional, and judicial consideration.

First, the legislature or the competent rule-making authority ought to prescribe clear and uniform criteria defining who qualifies as an "expert" for the purpose of Part B of the Schedule. At present, the absence of a precise threshold creates interpretive inconsistency across forums. It is further submitted that any such definition must address whether the standard of expertise must remain identical across civil and criminal proceedings, or whether the gravity of criminal consequences warrants a more exacting qualification.

Second, investigating agencies must be trained and institutionally directed to generate hash

values, preserve metadata, and maintain a contemporaneous chain-of-custody record from the moment of seizure. The certificate under Section 63(4) must reflect a genuine evidentiary safeguard and not degenerate into a post-facto clerical endorsement drafted long after the device has changed hands.

Third, as a matter of sound procedural policy, the Section 63 certificate should ordinarily accompany the electronic record at the first stage of its production before the court. Any departure from this rule must be permitted only on narrowly defined, judicially recorded grounds, so that the accused's right to disclosure is not undermined.

Fourth, courts are urged to adopt a purposive interpretive approach when adjudicating the admissibility of cloud-based or platform-hosted records. The test of "lawful control" should be read as control over data credentials and reproducibility, rather than physical dominion over the underlying hardware infrastructure.

Fifth and finally, the State must invest meaningfully in expanding institutional forensic capacity. The dual-certification model can fulfil its protective purpose only if qualified experts are accessible without systemic delay. Unless the infrastructure matches the legislative ambition, the certification requirement risks becoming an instrument of procedural delay rather than a guarantor of evidentiary reliability.