Page 1055 - 1068 **DOI:** *https://doij.org/10.10000/IJLMH.1110518*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 4

2025

Undefined and Unqualified: A Critique on the Absence of Expert Standards in India's Digital Evidence Framework

HELAN JESUS MARY L[1] AND NALLAMUNIAPPAN N[2]

ABSTRACT

In the era of rapid digital transformation, electronic evidence plays a pivotal role in civil and criminal trials. However, the credibility and admissibility of such evidence often hinge on expert interpretation. Despite this, Indian law continues to lack a clear statutory framework for recognizing and regulating electronic experts. It continues to recognize only traditional expert categories, such as handwriting or medical experts, and omits any mention of electronic or digital experts, despite the rising significance of technology in modern legal disputes. While the Bharatiya Sakshya Adhiniya, 2023 recognizes expert opinions in areas like handwriting and fingerprint analysis, and courts have a long-standing tradition of relying on such expertise with established interpretative standards, the same cannot be said for electronic or digital experts. Handwriting experts, for instance, benefit from decades of judicial interpretation, clear training protocols, and institutional recognition through forensic science laboratories. This legislative silence creates ambiguity, inconsistent judicial practices, and the risk of admitting evidence based on unverified or unqualified opinions, ultimately undermining the fairness of trial and the rule of law. The absence of statutory recognition for electronic experts also opens the door to misuse, manipulation, and challenges to evidentiary integrity. In this context, there is an urgent need for comprehensive legal reform to define electronic experts, establish qualification standards, and create a regulatory mechanism that ensures only competent and credible professionals assist the courts in interpreting electronic evidence.

This article critically examines the legislative gap concerning the definition, qualification, and recognition of electronic experts in India. The paper also reviews judicial trends, comparative international frameworks, and proposes legal reforms. These include the introduction of a statutory definition, accreditation criteria, training mechanisms, and regulatory oversight to ensure consistency and reliability in expert testimony on electronic records.

Keywords: *Digital transformation, electronic evidence, hash value, electronic expert, qualification*

[1] Author is an Assistant professor of Law at the Central Law college, Salem, India.
[2] Author is an Assistant professor of Law at the Central Law college, Salem, India.

 [ISSN 2581-5369]

I. INTRODUCTION

The evolution of technology has transformed the legal landscape, particularly in the realm of evidence. Electronic evidence, encompassing digital records, emails, audio-visual files, and more, has become a cornerstone in judicial proceedings. With the rapid digitalization of communication, surveillance, and commerce, electronic records such as emails, chat logs, metadata, and cloud-stored data have become central to both civil and criminal trials in India. Electronic evidence has become indispensable in the digital age, playing a critical role in both civil and criminal litigation. From call detail records and CCTV footage to emails, WhatsApp messages, and social media activity, vast amounts of data generated through electronic means are now frequently relied upon to prove or disprove facts in court. While the Indian Evidence Act, 1872, was amended to accommodate electronic evidence, and the Information Technology Act, 2000, introduced provisions for its legal recognition, gaps remain in regulating electronic experts. The Bhartiya Sakshya Adhiniyam (BSA), 2023, further expanded the scope of electronic evidence but failed to address the qualifications and regulation of electronic experts. The *Bharatiya Sakshya Adhiniyam, 2023* has replaced the colonial-era *Indian Evidence Act* with a modernized approach to digital evidence, particularly that mandate expert-backed certification of electronic records. However, while these provisions emphasize the importance of digital authenticity, they fail to define who qualifies as an "electronic expert" or stipulate the procedures and standards for verifying such records. This ambiguity has led to confusion among investigative agencies, prosecutors, and the judiciary, resulting in a fragmented and inconsistent evidentiary regime.

Yet, as this paper critically highlights, even this amendment falls short by **failing to define electronic experts**, thereby creating ambiguity in who is qualified to certify or interpret such vital forms of evidence.

II. LEGAL DEFINITIONS OF UNDER INDIAN LAW

This section discusses various definitions relevant to the topic of this paper, providing a foundational understanding for the content that follows.

A. Information Technology Act 2000

1. Electronic record

"Electronic record"[3] *means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer-generated micro fiche."*

[3]The Information Technology Act, 2000, § 2 (1) (t).

 [ISSN 2581-5369]

Electronic records are treated the same as other types of records. In simple terms, an electronic record is any information created or received on a computer during the start, progress, or end of a task by a person or organization.

The Hon'ble Supreme Court has consistently affirmed the importance of electronic evidence in criminal trials. The Court emphasized that non-production of electronic evidence such as CCTV footage or mobile data amounts to withholding the best evidence[4].

Similarly, internet transaction transcripts were key in proving the accused's guilt[5]. Phone call transcripts linked terrorists to the masterminds[6].

These cases highlight the critical evidentiary role that electronic records now play in contemporary legal proceedings.

2. Computer[7]

It means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network;

3. Computer network[8]

It means the inter-connection of one or more computers or computer systems or communication device through, the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and terminals or a complex consisting of two or more interconnected computers or communication device whether or not the inter-connection is continuously maintained.

4. Computer resource[9]

It means computer, computer system, computer network, data, computer data base or software.

5. Computer system[10]

It means a device or collection of devices, including input and output support devices and

[4] Tomaso Bruno & Anr. v. State of U.P.,2015 Cri. L.J. 1690.
[5] Ajmal Amir Kasab v. State of Maharashtra ,2012 9 SCC 1.
[6] State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru ,2005 11 SCC 600.
[7]The Information Technology Act, 2000, § 2 (1) (i).
[8] The Information Technology Act, 2000, § 2 (1) (j).
[9] The Information Technology Act, 2000, § 2 (1) (k).
[10] The Information Technology Act, 2000, § 2 (1) (l).

 [ISSN 2581-5369]

excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions.

The broader term encompasses computers, systems, networks, data, and software. While these definitions establish the legal basis for recognizing and processing electronic and digital evidence, they fall short of identifying the human expertise required to validate such records.

6. Data"[11]

It means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer."

This definition is technologically neutral, covering both the process and the medium—whether the data is currently being processed, has already been processed, or is intended to be processed. It includes various forms of data storage such as computer printouts, magnetic or optical storage devices, punched cards or tapes, and even data stored internally in computer memory. This broad interpretation ensures that both **active and stored electronic information** fall within the scope of legal protection under the Act.

As per the **Proviso to Section 79A of the IT Act, 2000**,[12] "electronic form evidence" includes any probative information stored or transmitted electronically, such as computer records, digital audio/video, mobile phone data, and faxes.

B. Bharatiya Sakshya Adhiniyam, 2023 (BSA)

1. Evidence[13]

It includes all statements including statements given electronically which the Court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry and such statements are called oral evidence; and all documents including electronic or digital records produced for the inspection of the Court and such documents are called documentary evidence.

Previously, the Indian Evidence Act, 1872 defined oral evidence as statements permitted or

[11] The Information Technology Act,2000, § 2 (1) (o).
[12] The Information Technology Act, 2000, § 79A.
[13] Bharatiya Sakshya Adhiniyam, 2023, § 2(e).

 [ISSN 2581-5369]

required to be made before the court by witnesses. However, it did not expressly include electronically recorded or transmitted statements within its scope. In contrast, Section 2(e) of the Bharatiya Sakshya Adhiniyam, 2023 brings a significant change by explicitly defining oral evidence to include not only statements made in person but also those given electronically. This marks a progressive shift by formally recognizing electronic modes of testimony, such as video conferencing or virtual hearings, as valid forms of oral evidence, which were previously not codified under the 1872 Act.

2. Documents

Both electronic and digital records are included under the definition of "documents"[14] in, and are admissible as evidence.

P. Gopalkrishnan v. State of Kerala,[15] The video footage/clipping contained in such memory card/pen drive being an electronic record as envisaged by Section 2(1)(t) of the 2000 Act, is a "document" and cannot be regarded as a material object.

3. Opinions of experts[16]

When the Court has to form an opinion upon a point of foreign law or of science or art, or any **other field**, or as to identity of handwriting or finger impressions, the opinions upon that point of persons especially skilled in such foreign law, science or art, or any other field, or in questions as to identity of handwriting or finger impressions are relevant facts and such persons are called experts.

For example, in a murder case in Chennai, businessman Mr. Rajan was found dead in his home, and police suspected poisoning. To confirm the cause of death, the prosecution called Dr. Ananya, a forensic toxicology expert. She testified that the symptoms and chemical findings in Mr. Rajan's body matched a specific poison. Under Section 39 of the Bharatiya Sakshya Adhiniyam, her expert opinion was treated as a relevant fact to help the court determine the cause of death.

Just as a **forensic toxicologist** is recognized as a scientific expert who analyzes bodily fluids and tissues to detect poisons or drugs and assists the court in determining causes like poisoning or overdose, an **electronic expert** plays a similarly critical role in the digital domain. An electronic expert examines digital records, system logs, and device data to authenticate, recover, and interpret electronic evidence. Therefore, to ensure consistency,

[14] Bharatiya Sakshya Adhiniyam, 2023, § 2(d)
[15] P. Gopalkrishnan v. State of Kerala, 2019 SCC On Line SC 1532.
[16] Bharatiya Shakshya Adhiniyam 2023, § 39 (1).

 [ISSN 2581-5369]

admissibility, and reliability of digital evidence, there is need to **separately define "electronic expert"** under Indian law.

When in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000, is a relevant fact. And also, in explanation describes, for the purposes of this sub-section, an Examiner of Electronic Evidence shall be an expert.[17]

Merely labelling someone as an "expert" without defined parameters risks inconsistency and weakens the reliability of electronic evidence in judicial proceedings. A uniform, transparent framework is essential for upholding both **technical accuracy** and **judicial fairness**.

III. Difference between Electronic and Digital Records[18]

Section 2(d) of the Bharatiya Sakshya Adhiniyam, 2023 defines the term *document* to include both electronic records and digital records. Although these terms sound similar, they are slightly different in how they are created, stored, and used.

Aspect	Electronic Records	Digital Records
Definition	Data created/stored/transmitted via electronic systems; part of a broader communication platform.	Files in digital form, either originally digital or digitized from physical sources.
Origin	Born digital, existing only within electronic systems.	Can be born digital or digitized.
System Dependency	Platform-dependent (e.g., email servers, apps).	Platform-independent; accessible via common software.
Examples	Emails, SMS, web pages, Excel linked to systems.	PDFs, scanned images, MP3/MP4, Word files.
Legal Relevance	Complex to authenticate; metadata is key in trials.	Easier to present as evidence; integrity essential.

[17] Bharatiya Shakshya Adhiniyam 2023, § 39 (2).
[18] Smt. Sk. Shireen, V Additional Civil Judge (Junior Division) Cum V Additional Judicial Magistrate of First class, Kakinada -ELECTRONIC EVIDENCE.

 [ISSN 2581-5369]

Aspect	Electronic Records	Digital Records
Challenges	Needs expert verification, metadata preservation.	Simpler validation but less contextual info.
Status under BSA, 2023	Recognized under Sec. 2(d); admissible with proof of authenticity.	Also recognized; commonly used as exhibits.

IV. PROCEDURE FOR ADMISSIBILITY OF ELECTRONIC RECORDS

The word 'admissible' means the evidence which can be admitted in court and taken on record. The concept of admissibility is completely different from concept of relevancy and probative value of the evidence adduced. Section 63 makes electronic evidence admissible; it does not dispense with the relevancy and probative value. Section 62 and Section 63 of Bhartiya Sakshya Adhiniyam, 2023 (BSA) lays down rules regarding admissibility of electronic records.

A. Comprehensive framework for the admissibility of electronic records as documentary evidence

Any information contained in an electronic record which is printed on paper, stored, recorded or copied in optical or magnetic media or semiconductor memory which is produced by a computer or any communication device or otherwise stored, recorded or copied in any electronic form (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible.

As per Sub-section (1), any information that is stored, recorded, printed, or copied in an electronic or digital format whether on paper, optical or magnetic media, or in semiconductor memory shall be deemed a document, provided that the conditions laid down in Sub-section (2) are fulfilled. Once these conditions are satisfied, such electronic records are admissible in legal proceedings without the need for producing the original physical document or any further proof.[19]

This provision marks a progressive shift by replacing the earlier reference to only a "computer" under Section 65B of the Indian Evidence Act, 1872, with the broader phrase

[19] BSA 2023, § 63(1).

"computer or any communication device", thereby aligning the law with modern technologies such as smartphones, tablets, and networked devices. It also affirms that where the required certification is in place, the judiciary is bound to accept such computer-generated outputs unless serious doubts are raised regarding the authenticity or procedural compliance of the certification.

B. Essential conditions for admissibility of electronic evidences

The mandatory conditions that must be fulfilled for an electronic record (or computer output) to be deemed admissible as evidence:

- **Regular Use**: The electronic record must have been generated during a period when the computer or communication device was regularly used by a person lawfully controlling it for legitimate activities.
- **Regular Feeding of Data**: Information must have been regularly entered into the device in the ordinary course of those activities.
- **Proper Functioning**: The device must have been operating properly during the relevant time. If it malfunctioned, such disruption must not have affected the accuracy or reliability of the data.
- **Data Accuracy**: The electronic record must accurately reproduce or be derived from the original inputted data during normal operations.[20]

These conditions ensure that electronic records are not only legally valid but also reliable, provided they are generated and maintained under ordinary business or lawful activity. However, my paper critically highlights, even though the law specifies how such data should be authenticated, it fails to define who qualifies as a competent expert to verify this process resulting in ambiguity and inconsistency in courtrooms. This legal vacuum undermines the uniform admissibility of electronic evidence across jurisdictions.

C. Legal recognition of interconnected digital systems as a single source

If, during a certain period, information was regularly created, stored, or processed using one or more computers or devices whether they were used alone, as part of a computer system, connected in a network, used for creating or storing information, or through an intermediary all of those computers or devices will be considered as one single unit for the purposes of this section.[21]

[20] Bharatiya Sakshya Adhiniyam, 2023, § 63(2).
[21] Bharatiya Sakshya Adhiniyam, 2023, § 63(3).

 [ISSN 2581-5369]

D. Certification requirement for admissibility of electronic records

To admit an electronic record in evidence under Section 63, a certificate must be submitted at each instance of its use. This certificate must:

1. Identify the Record: Clearly describe the electronic record and the process by which it was produced.
2. Detail the Device Used: Specify the computer or communication device involved in generating the record, as per the modes described in Section 63(3).
3. Address Admissibility Conditions: Affirm that the record meets the conditions under Section 63(2), and
4. Be Signed by a Competent Authority: It must be signed either by the person managing the device or activity, or an *expert*. The statement may be made to the best of the person's knowledge and belief.[22]

Furthermore, Section 63(5) clarifies that:

- Information is considered "supplied" to a computer/device whether directly or through equipment with or without human intervention.
- A "computer output" is valid regardless of how it was produced, so long as it results from electronic processes mentioned under Section 63(3).[23]

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)[24]: The Supreme Court reaffirmed that a certificate under Section 65B (4)[25] of the Indian Evidence Act is mandatory for the admissibility of electronic records. The Court clarified that oral evidence cannot substitute the requirement of this certificate, emphasizing the need to ensure the authenticity and reliability of electronic evidence.

---

[22] Bharatiya Sakshya Adhiniyam, 2023, § 63 (4).
[23] Bharatiya Sakshya Adhiniyam, 2023, § 63 (5).
[24] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020),AIR 2020 SUPREME COURT 4908, AIRONLINE 2020 SC 641
[25] In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,
(a) identifying the electronic record containing the statement and describing the manner in which it was produced;
(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,
and purporting to be 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 (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this subsection, it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.(Substituted by BSA 2023)

 [ISSN 2581-5369]

State of Karnataka v. M.R. Hiremath (2019)[26] The Supreme Court held that electronic evidence without a certificate under Section 65B (4) is inadmissible. The Court reiterated that the certificate is a condition precedent to the admissibility of electronic records, ensuring their authenticity and reliability.

Shafhi Mohammad v. State of H.P. The requirement of the certificate under Section 65B of the Evidence Act as per the judgment of Anvar (supra) is not required in the following two cases:

- A party who is not in possession of device from which the document is produced cannot be required to produce certificate.[27]
- The applicability of requirement of certificate being procedural can be relaxed by the court wherever interest of justice so justifies.[28]

The Supreme Court observed that the requirement of a certificate under Section 65B (4) is procedural and can be relaxed in the interest of justice, especially when the party seeking to produce electronic evidence is not in possession of the device from which the document is produced. However, this position was later overruled by the decision in Arjun Panditrao Khotkar, reinstating the mandatory nature of the certificate.

V. CERTIFICATE PROCESS FOR ELECTRONIC EVIDENCE[29]

The legal framework for the **admissibility of electronic records** in Indian, it mandates the submission of a **certificate** as part of the evidentiary process to establish the authenticity, origin, and integrity of electronic data. The structure and content of this certificate are detailed in the Schedule to Section 63(4) (c), divided into Part A (to be filled by the party) and Part B (to be filled by the expert).

A. Part A- declaration by the party submitting the evidence

In Part A, the person (party) presenting the electronic record must:

- **Identify the source of the electronic record**, whether it is a computer, mobile phone, DVR, server, cloud storage, flash drive, etc.
- **Provide details** of the device, such as make, model, serial number, and unique identifiers like IMEI, MAC address, or Cloud ID.

[26] State of Karnataka v. M.R. Hiremath, (2019) 7 SCC 515.
[27] Indian Evidence Act, § Section 65 B (4).
[28] (2018) 2 SCC 801.
[29] BSA, 2023, § 63(4) (c).

- **Declare the lawful control and proper functioning** of the device during the relevant period of data creation or processing.
- **Affirm the integrity of the data**, including a declaration that the information was regularly fed into the device in the normal course of activity and that any device malfunction did not affect data accuracy.
- **Generate and state hash values** (SHA-1, SHA-256, MD5, etc.) to prove the authenticity and unaltered status of the data.[30]

B. Part B – Verification by the Expert

Part B is to be completed by an **electronic expert**, who verifies:

- The **technical accuracy and source** of the electronic record.
- The **hash values and digital fingerprint** of the file or record submitted.
- That the evidence was generated by or derived from an appropriate device using an accepted methodology.

This expert must sign and certify the record, lending technical credibility to its admissibility.

While the process outlined in Section 63(4) seems thorough on paper, it suffers from a serious **structural and legal shortcoming the lack of a statutory definition of who qualifies as an electronic expert**.[31]

The failure to produce a certificate under Section 65B (4) of the Evidence Act at the stage when the **charge-sheet is filed is not fatal to the prosecution**. The need for production of such a certificate would arise when the electronic record is sought to be produced in evidence at the trial. It is at that stage that the necessity of the production of the certificate would arise. **This case explains the stage of filing the certificate.[32]**

Anvar P.V v. P.K Basheer[33]: Overrules Navjyot Sandhu, Electronic record by way of secondary evidence shall not be admitted in evidence unless the requirements under Section 65B are satisfied. Since 65A and 65B are special provisions, they will be given precedence over general laws in Sections 63 and 65 (Generalia specialibus non derogant)[34]. Notwithstanding Sections 59, 65A and 65B of the Evidence Act, an electronic record used as primary evidence under Section 62 is admissible in evidence, without complying Section 65B

[30]Schedule to § 63(4) (c), Part A BSA, 2023.
[31] Schedule to § 63(4) (c), Part B BSA, 2023.
[32] State by Karnataka Lokayukta, Police Station, Bengaluru v. M.R. Hiremath (2019) 7 SCC 515.
[33]Anvar P.V v. P.K Basheer (2014) 10 SCC473.
[34]Bhanvi Juvekar, https://blog.ipleaders.in/generalis-specialibus-non-derogant-know-all-about-it/

 [ISSN 2581-5369]

of the Evidence Act.

It is also pertinent to bear in mind that non-production of certificate at an earlier stage is not fatal, it is a curable defect. The Hon'ble Supereme Court, in Union of India & Ors v/s CDR Ravindra Vs Desai[35] has held as follow: Learned counsel for the appellants rightly argued that non-production of the certificate under Section 65-B of the Indian Evidence Act, 1872 on an earlier occasion was a curable defect which stood cured"

Regarding the proof and admissibility of mobile phone call records, it needs to be proved by producing certificate under Section 65-B of Evidence Act. It has been held in Para 36 **that absence of certificate would render the CDR inadmissible in law. Being inadmissible it cannot be considered**[36].

However, the accused side raised a submission that no reliance can be placed on the mobile phone call records , because the prosecution has failed to produce the relevant certificate under section 65-B of the Evidence Act, The Supreme Court has concluded that a cross examination of the competent witness acquainted with the functioning of the computer during the relevant point of time and the manner in **which the printouts of the call records were taken was sufficient to prove the call records**[37]**.**

In Sonu Vs State of Haryana,[38] it has been held in Para 32 by the Supreme Court that an objection that **CDRs are unreliable due to violation of procedure prescribed in section 65-B (4)** cannot be permitted to be raised at the appellate stage as the objection relates to the mode or method of proof.

Since mobile phone is computer, the print out taken is a computer output, it requires certificate under section 65-B of the Evidence Act. However, in Aryan Shah Rukh Khan Vs Union of India[39], it has been held that such a certificate is not necessary in the stage of investigation.

Section 88-A [40]of the Evidence Act provides for a presumption about electronic messages. It is necessary to understand that the presumption merely states that the message received by the addressee is the same, which was fed into the originator's computer for transmission.

[35] Ravindra Vs Desai (2018 Law Suit (SC) 358).
[36]Bala Saheb Gurling Todkari Vs. State of Maharastra (2015 SCC Online Bom 3360).
[37] State of NCT of Delhi Vs Navjot Sadhu, AIR 2005 SC 3820.
[38] Sonu Vs State of Haryana, (2017)8 SCC 517.
[39] ADPS BAIL APPLICATION NO 2571 of 2021 dated 20.10.2021.
[40] The Court may presume that an electronic message, forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

As held by Madras High Court, in S. Karunakaran Vs Srileka[41], the court shall not make any presumption as to the person by whom such message was sent. Therefore, it is clear that mere filing of email does not give raise a presumption that it is sent by the originator. Similarly, the High Court of Punjab and Haryana, in Nidhi Kakka vs Munish Kakkar[42], that the correctness and exact reproduction in print out version of the mail could still be issues in the cross examination and the court will have to consider whether the text could have been altered or morphed.

So finally, this paper concludes, in the digital era, the admissibility of **electronic and digital evidence** has become central to both criminal and civil adjudication. While Section 63 of the **Bharatiya Sakshya Adhiniyam, 2023** attempts to codify the procedure for admitting electronic records through a certificate system, it leaves a glaring legal vacuum regarding the definition, qualification, and accountability of the **electronic expert** who plays a vital role in certifying such evidence.

The Schedule to Section 63(4) provides a dual certification process—Part A by the party submitting the evidence and Part B by the expert. While this mechanism appears comprehensive, its practical utility is diluted by the absence of any statutory definition for an "electronic expert" or "digital forensic expert." Section 39(2) of BSA refers to the Examiner of Electronic Evidence under Section 79A of the IT Act, but this designation too lacks clear eligibility criteria, qualifications, or a national registry of certified professionals.

Further complicating matters is the **judicial uncertainty** about the stage at which this certificate must be produced. Although landmark rulings (e.g., *Anvar P.V. v. P.K. Basheer*, *Sonu v. State of Haryana*, *Aryan Khan v. Union of India*) have clarified the importance of such certification under **Section 65B of the Evidence Act**, courts remain divided on whether non-production at the investigation or bail stage is fatal. This inconsistency weakens procedural fairness and creates challenges for both prosecution and defense side.

VI. WAY FORWARD

1. The application of universal jurisdiction **Statutory Definition of Electronic Expert**

There must be a clear legal definition of who qualifies as an "electronic expert" or "digital forensic expert," ideally incorporated in both the **BSA** and **IT Act**.

[41]S. Karunakaran Vs Srileka, 2019 SCC Online Mad 1402.
[42] Nidhi Kakka vs Munish Kakkar ,2011 SCC On line P&H 2599 has held in Para 6.

2. **Standard qualifications and experience**

The legislature must prescribe minimum educational qualifications (e.g., B.Tech in Computer Science, Cyber Forensics Certification), and work experience criteria for such experts.

3. **Accrediting authority**

An independent body, possibly under the **Ministry of Electronics and Information Technology**, should be authorized to train, certify, and maintain a national registry of qualified electronic experts.

4. **Judicial training and guidelines**

Special training programs must be organized for judges, magistrates, and public prosecutors on evaluating electronic evidence, with clear **guidelines on the admissibility stages**.

5. **Uniform certificate procedures**

A standardized protocol must be issued for when and how certification under Section 63 should be submitted whether at the FIR stage, charge-sheet, bail hearing, or during trial.

VII. CONCLUSION

While Bharatiya Sakshya Adhiniyam, 2023 has modernized the evidentiary framework by recognizing electronic records and setting certification procedures, it stops short of establishing the human infrastructure necessary to implement it effectively. The inclusion of a certificate mechanism under Section 63(4) of the BSA is a progressive and necessary tool for authenticating digital evidence. However, without a clear statutory framework defining electronic experts and their qualifications, the implementation of this provision remains incomplete and vulnerable to misuse. The lack of a defined, regulated, and trained class of electronic experts threatens the integrity, reliability, and uniformity of electronic evidence in Indian courts. Unless this gap is urgently filled through legislative reform and institutional support, the credibility of digital justice will remain vulnerable to procedural ambiguity and technical incompetence. This article highlights the gaps in the current legal framework and emphasizes the need for regulatory provisions for electronic experts. It is tailored for publication to spark discussions on improving the legal treatment of electronic evidence.

Judicial reliance on unverified or underqualified "experts" may jeopardize the reliability of digital evidence, thus defeating the very purpose of this legal reform. Filling this definitional vacuum is essential for preserving the fairness and uniformity of justice in the digital age.

*****

 [ISSN 2581-5369]