LEGAL STANDARDS FOR ADMITTING DIGITAL EVIDENCE IN COURT

Dr. Nainy Singh, Principal, Dr. Ambedkar Government Law College, Puducherry

ABSTRACT

The admission of digital evidence in court has become extremely pertinent, keeping in mind the paradigm shift in the legal diaspora. There is a paradigm shift in the notion of evidence due to the proliferation of cybercrime. The present research paper examines the legal standards governing the admissibility of digital evidence as per the law of the land. By virtue of its unique traits, the electronic evidence is susceptible to misuse and tampering which results in the abuse of justice. Delving into the Sections 65A and 65B, of Indian Evidence Act, introduced through Indian Evidence Act (Amendment) in 2000 under the aegis of Information Technology Act, 2000. These newly introduced provisions establish the legal presumption that electronic evidence is admissible in court subject to stringent conditions ensuring authenticity and integrity. The paper traces the evolution of admissibility standards, examines the pivotal role of forensic analysis, and considers the impact of recent legislative amendments under the Bharatiya Sakshya Adhiniyam, 2023.

INTRODUCTION

In today's rapidly advancing technological era, the digital world has become just as essential to our lives as the physical one. A significant portion of social, administrative, and economic activities now occur online, turning the digital space into a hub for criminal activity. The profound impact of technology on society has led to the increased importance of digital media globally. This represents a paradigm shift from the traditional reliance on physical and oral evidence to a more convoluted dependence on electronic records, encapsulating the evolution of evidence in the modern legal landscape. With a rampant increase in digital offences, criminal investigations rely all the more on digital evidence to effectively address and resolve these cases. The escalation of technical conflicts and the rapid increase in cybercrime have prompted a paradigm shift that has changed the understanding of evidence as we know it. To overcome these obstacles, courts increasingly depend on electronic records to resolve disputes. The distinct characteristics of digital evidence make it susceptible and vulnerable to tampering and misuse, which can lead to the abuse of legal process and increase the risk of miscarriages of justice. As a consequence, digital evidence must ascribe to strict admissibility standards to ensure its authenticity, integrity, and reliability prior to being deemed acceptable during legal processes. Digital evidence includes extensive electronic materials, encompassing emails, text messages, social media content, digital photos, and data retrieved from Internet of Things (IoT) devices, providing crucial information in legal contexts and modern investigations. Crucial insights into crimes and suspect behaviour can be gathered from digital data on smartphones, computers, cloud storage, and social media. However, legal professionals encounter significant challenges in handling digital evidence, including ensuring its admissibility in court, verifying its authenticity, and confirming that it has not been tampered with. The prevalent and multifaceted nature of digital information is both a boon and a bane to the legal realm. Although digital evidence is more convenient to store, share, and search, it also raises concerns about authenticity, privacy, and technical complexities, making its use in legal proceedings both advantageous and complicated.

Sections 65A and 65B were introduced into the Indian Evidence Act, 1872 under the aegis of the Information Technology Act 2000, creating a legal supposition that electronic records qualify as "documents" for the purposes of the Evidence Act. This recognition is, however, subject to the fulfillment of specific conditions outlined in Section 65B[1]. These provisions act

[1] Ratanlal Ranchhoddas and Dhirajlal Keshavlal Thakore, *Ratanlal & Dhirajlal the Law of Evidence* (2016).

as safeguards to ensure that the electronic records are reliable and authentic, given their inherent vulnerability to tampering, alteration, and manipulation. The Information Technology Act 2000, defines "electronic record" as any data, record, or data produced, and any image or sound stored, received, or transmitted in electronic form, including micro-film or computer-generated micro-film[2]. This legal framework ensures that electronic records are treated with the same evidentiary value as physical documents, all the while prescribing more stringent rules and conditions for their admissibility, thereby addressing the complexities associated with the digital nature of evidence.

EVOLUTION OF ADMISSIBILITY

The definition of 'evidence' under Section 3(a) of the Indian Evidence Act has been amended to include electronic records. Evidence can now be presented in oral or documentary form, with the term 'documentary evidence' expanded to encompass all documents, including electronic records submitted for court inspection. The term 'electronic records' is defined as per the Information Technology Act, covering data, records, or any information generated, stored, received, or sent in electronic form, including images, sounds, microfilm, or computer-generated microfiche[3]. This amendment ensures electronic records are treated as valid documentary evidence in legal proceedings.

The appreciation of evidence refers to the judicial process of assessing the credibility and probative value of evidence presented during a trial. It is a structured, methodical, and analytical evaluation of material facts aimed at determining the rights and liabilities of the parties involved, ensuring a fair and just resolution of the legal dispute. The appreciation of evidence necessitates a broad, comprehensive perspective, rather than a narrow or limited one. The court must carefully separate the relevant and reliable facts from the irrelevant or unreliable ones. In appreciating the evidence, the Court must consider the context and circumstances surrounding the crime, as well as the comprehension level of the witnesses. With these broad principles in mind, the Court must evaluate the evidence to determine which parts reflect the true and accurate facts. The Court is tasked with distinguishing between credible and unreliable evidence, which has been duly accomplished.[4]

[2] Information Technology Act 2000, S 2(t)
[3] ibid.
[4] *Ganesh K.Gulve v. State of Maharashtra* 357 INSC (2002)

The definition of 'admission' under Section 17 of the Evidence Act has been expanded to include statements in oral, documentary, or electronic form that suggest an inference related to a fact at issue or relevance[5]. Section 22A has been newly added to the Evidence Act, addressing the relevance of oral evidence about electronic records. It stipulates that oral admissions concerning the contents of electronic records are only relevant when the authenticity of the electronic records presented is in dispute[6].

A "document" refers to one that is admissible as evidence. If a document is inadmissible due to a failure to register or improper stamping, secondary evidence of its existence cannot be provided. Where the original document is inadmissible owing to being unstamped or unregistered, secondary evidence is likewise inadmissible. Secondary evidence cannot be presented to prove a fact that requires primary evidence, and under no circumstances can secondary evidence replace inadmissible primary evidence[7]. Section 65 stipulates the conditions under which secondary evidence may be admitted without the submission of primary evidence. However, a party cannot seek the Court's permission to admit secondary evidence without first satisfying the prerequisites of Section 65. The party must demonstrate a bona fide reason for presenting secondary evidence, and it is the Court's discretion to admit such evidence. Secondary evidence may be permitted in the following scenarios[8]:

1. When the original document is in the possession of an opposing party, is in the possession of an individual who is unreachable, or is with someone who refuses to provide the original after being notified.

2. When the opposing party has admitted the contents of the original document in a subsequent document.

3. When the original document is lost, constitutes a public document, or cannot be easily produced before the court. In such cases, a legally obtained certified copy may be presented as secondary evidence.

[5] Indian Evidence Act 1872, S 17
[6] Dr. Pratyusha Das and Pradeepta Sarkar, 'The Importance of Digital Forensics in the Admissibility of Digital Evidence' [2022] NUJS Journal of Regulatory Studies 61
[7] Shabbeer Ahmed, Sahana Devanathan and Abhinay V, 'Arjun Panditrao: The Supreme Court's Attempt To Clarify A History Of Judicial Uncertainty' (2021) Mondaq <https://www.mondaq.com/india/telecoms-mobile-cable-communications/1038968/arjun-panditrao-the-supreme-courts-attempt-to-clarify-a-history-of-judicial-uncertainty> accessed 1 October 2024
[8] Indian Evidence Act 1872, S 65

4. Examination of a portion of an extensive or voluminous original document by a qualified expert can be qualified as secondary evidence.

In a case where permission was sought to produce secondary evidence of certain receipts on the grounds that the original receipts were lost, the court held that two conditions must be satisfied: there must be evidence of the existence of original receipts, and there must be proof of their loss. Since no evidence was presented to establish the existence of the original receipts, the permission granted by the lower court was held to be improper.[9]

In a case before the Supreme Court, the issue was whether the tenant had granted a sub-tenancy. The Rent Controller's finding of sub-tenancy was based on a tape-recorded conversation between the tenant and the landlady's husband. The court held that the tape-recorded conversation could be used to corroborate the deposition of one of the parties in court. However, in the absence of such deposition, the tape could not be treated as standalone evidence. The Supreme Court later reinforced the requirement that the tape must be shown to have been kept in proper custody. In that case, the Deputy Commissioner's decision to leave the tape with a stenographer was deemed sufficient to undermine its authenticity.[10]

Section 65 of the Indian Evidence Act 1872, allows parties to introduce secondary evidence, but this is subject to numerous limitations. If the original documents are never produced and no factual basis for admitting secondary evidence is established, the court cannot allow such evidence.[11] In conformity with the cases listed under section 65B, secondary evidence about the contents of the document is not admissible unless the non-production of the primary evidence is well justified. Furthermore, by demonstrating that the secondary evidence accurately depicts the original, secondary evidence has to be verified. Documentary evidence must be proven in accordance with legal standards; its mere admission is not proof of it. The Court is obliged to determine the admissibility of a document as secondary evidence before endorsing or admitting it into the record.[12] In this case, the crux was whether the respondent had executed a power of attorney in favour of Defendant No. 2, authorising the alienation of

[9] *Gurdial Kaur v Registrar of Co-op Societies* 124 PLR 156 (2000)
[10] *Ram Singh v Col Ram Singh* 611 SCC (1985)
[11] Shabbeer Ahmed, Sahana Devanathan and Abhinay V, 'Arjun Panditrao: The Supreme Court's Attempt To Clarify A History Of Judicial Uncertainty' (2021) Mondaq <https://www.mondaq.com/india/telecoms-mobile-cable-communications/1038968/arjun-panditrao-the-supreme-courts-attempt-to-clarify-a-history-of-judicial-uncertainty> accessed 1 October 2024
[12] Dr. Pratyusha Das and Pradeepta Sarkar, 'The Importance of Digital Forensics in the Admissibility of Digital Evidence' [2022] NUJS Journal of Regulatory Studies 61

the suit property, and whether the power of attorney had been lawfully proven. The trial court ruled in favour of the suit, noting that since the original power of attorney was not in the possession of the parties, laying any further factual foundation was unnecessary. However, the Supreme Court vitiated the proceedings of the trial court and held it to be inadequate, as only the respondent's signature on the photocopy of the power of attorney was certified but it did not acknowledge its contents. The Court emphasised that the admissibility of a document or its contents does not automatically lead to any inference unless those contents possess probative value. Furthermore, it is the Court's duty to assess whether the documents or their contents presented in court hold any evidentiary value.[13]

Sections 65A and 65B were both introduced through the Indian Evidence (Amendment) Act, 2000 and form part of Chapter V of the Evidence Act, dealing with documentary evidence. As per the provisions, Section 65A of the Evidence Act establishes a specific provision for recognizing electronic records as admissible evidence, while Section 65B regulates the admissibility of electronic records by establishing a legal presumption. The provisions implement safeguards to ensure the source and authenticity of electronic records, which are inherently vulnerable to tampering and modification.[14] The aim of these provisions is to enable the use of electronic evidence in legal proceedings. They also function as an exception to the best evidence rule, which mandates the production of the original document as primary evidence. The non-onstante clause in the Section 65B of the Evidence Act gives it a higher pedestal and states that, as long as the requirements outlined in the section are met, any information found in an electronic record is considered a document and is admissible as evidence without the need for additional verification of the original. The conditions specified in Section 65B(2) are[15]:

1. The computer output containing the information must have been generated by the computer during a period when it was regularly used to store or process information for activities consistently conducted by the person lawfully controlling the computer's usage during that time.

2. It must be proven that, during the pertinent time period, the data that was used to create

[13] *H Siddiqui v A Ramalingam* AIR 1492 (2011)
[14] Samiron Borkataky and Kritika Angirish, 'Electronic Evidence - Revisiting The Basics' (2023) Mondaq <https://www.mondaq.com/india/arbitration-dispute-resolution/1280114/electronic-evidence-revisiting-the-basics?msg=15#authors> accessed 2 October 2024
[15] Ratanlal Ranchhoddas and Dhirajlal Keshavlal Thakore, *Ratanlal & Dhirajlal the Law of Evidence* (2016).

the electronic record or the information contained within it was routinely input into the computer as part of the regular course of the relevant activity.

3. The third requirement is that, during the relevant period, the computer was functioning properly. If the computer experienced any malfunction during that time, it must be shown that the disruption did not impact the integrity of the record or the accuracy of its contents.

4. The fourth criteria is that the data in the record must be a copy of or generated from the data that is routinely entered into the computer during their regular activities.

These provisions establish a dichotomy between the magnetic digital data stored on the device, considered the original, and the copies derived from it. Electronic evidence obtained through cyber forensic methods is treated as the original document, while the printed versions of such data are classified as secondary evidence[16]. Certification of the authenticity of this secondary evidence by a competent authority, subject to cross-examination, is required. Section 65B of the Indian Evidence Act explicitly governs the admissibility of such secondary digital evidence[17].

Section 65B(4) requires the submission of a certificate identifying the electronic record containing the statement, outlining the production process and providing information about the instrument used to produce the electronic record, whenever a statement is admitted as evidence under Section 65B. To verify that the record was produced by a computer, this certificate has to be signed by a person holding a responsible official position who is either in charge of managing the related operations or supervising the operation of the relevant equipment, if applicable.[18]

Under Section 65B(4) of the Indian Evidence Act, the court decided in 2005 that printouts of

[16] Shabbeer Ahmed, Sahana Devanathan and Abhinay V, 'Arjun Panditrao: The Supreme Court's Attempt To Clarify A History Of Judicial Uncertainty' (2021) Mondaq <https://www.mondaq.com/india/telecoms-mobile-cable-communications/1038968/arjun-panditrao-the-supreme-courts-attempt-to-clarify-a-history-of-judicial-uncertainty> accessed 5 October 2024

[17] Aditya Mehta, Arjun Sreenivas and Swagata Ghosh, 'Section 65B Of The Indian Evidence Act, 1872: Requirements For Admissibility Of Electronic Evidence Revisited By The Supreme Court' (2021) Mondaq <https://www.mondaq.com/india/civil-law/1035072/section-65b-of-the-indian-evidence-act-1872-requirements-for-admissibility-of-electronic-evidence-revisited-by-the-supreme-court#authors> accessed 5 October 2024

[18] Ajay Bhargava, Aseem Chaturvedi , Karan Gupta and Shivank Diddi, 'India: Use Of Electronic Evidence In Judicial Proceedings' (2020) Mondaq <https://www.mondaq.com/india/trials-appeals-compensation/944810/use-of-electronicevidence-in-judicial-proceedings> accessed on 5 October 2024

phone records might be entered as evidence even in the absence of a certificate. The Hon'ble Court later overturned this ruling in Anvar P. v. P.K. Basheer[19], holding that Section 65B serves as a complete code for the admission of electronic documents and that any evidence from a source that falls outside of its purview is inadmissible. The Court further held that the certificate mandated under Section 65B(4) of the Indian Evidence Act is a prerequisite for the admissibility of electronic evidence. The certificate is essential for such evidence to be considered admissible, with Section 65B serving as the foundational provision governing its admissibility. It is important to note, nevertheless, that primary evidence such as laptop, cell phone, or tape recorder that contains electronic data will be admitted into evidence without having to follow the standards set by Section 65B if it is immediately placed before the court.

AUTHENTICATING THE INFORMATION ON ELECTRONIC DOCUMENTS

In judicial proceedings, the admissibility of digital evidence is evaluated based on three fundamental criteria: relevancy, authenticity, and integrity. Firstly, the evidence must be material to the case, demonstrating a clear and direct connection to the issues in dispute. Secondly, the evidence must be authentic, meaning it must remain unaltered or tampered with and must originate from a reliable and credible source. Lastly, the integrity of the evidence must be preserved, ensuring it has remained unaltered since its collection. To maintain this integrity, strict procedures are followed[20]. Any unauthorised access, improper handling, or insufficient documentation may compromise the evidence's integrity, potentially rendering it inadmissible in court. Section 65B of the Indian Evidence Act regulates the admissibility of electronic evidence in judicial proceedings. This provision sets forth specific conditions, extending beyond technical considerations, that must be satisfied to establish the authenticity of digital records. Prior to admitting electronic evidence, the court will evaluate if the evidence is relevant and authentic. The evidence must adhere to the legal standards of authenticity, reliability, and overall integrity.[21] To establish the authenticity of electronic evidence, submission of the certificate in accordance with Section 65B(4) of the Indian Evidence Act is a prerequisite. For an electronic record to be admissible as evidence, it must be certified to confirm its authenticity, including specific details about the computer system that produced it. If the certification process does not comply with the provisions of Section 65B, the electronic

[19] *Anvar P. v. P.K. Basheer* AIR 180 (2014)
[20] Neelabh Rai Shanker, 'The Role of Digital Evidence In Legal Proceedings: The Indian Perspective' [2024] IJRPR 7891
[21] Ratanlal Ranchhoddas and Dhirajlal Keshavlal Thakore, *Ratanlal & Dhirajlal the Law of Evidence* (2016).

evidence will be deemed inadmissible in court.[22]

With the advancement of information technology, a scientific approach must permeate investigation methods, both at the individual and institutional levels. The growing influence of technology in daily life has rendered the production of electronic evidence increasingly pertinent in establishing the guilt of the accused or the liability of the defendant. Electronic documents, in the stricto sensu, are admissible as material evidence.[23] Such evidence proves to be highly beneficial to investigating agencies and the prosecution in the conduct of criminal proceedings. When a document is to be introduced as evidence under this section, it must be accompanied by a certificate identifying the electronic record containing the document, specifying the manner of its production, and providing details of the device used to generate the record. The certificate must confirm that a computer produced the document and that the conditions set forth in sub-section (2) of this section were satisfied. The certificate must be signed by a person holding a responsible official position in relation to the operation or management of the relevant activities. This certificate shall serve as evidence of the facts stated therein and must be made to the best knowledge and belief of the certifying individual.[24]

When an electronic record is presented as primary evidence, it is admissible without requiring compliance with the conditions outlined in Section 65B of the Indian Evidence Act. The formalities under Section 65B apply only to secondary evidence of electronic records, not to the original or primary digital documents themselves.[25]

In order to submit a statement pertaining to an electronic record in legal proceedings, the following conditions under Section 65B(4) of the Indian Evidence Act must be met[26]:

(a) A certificate must identify the electronic record containing the statement;

(b) The certificate should describe how the electronic record was produced;

[22] *Anvar P. v. P.K. Basheer* AIR 180 (2014)
[23] Astha Jain, 'Admissibility of Electronic Evidence under The Indian Evidence Act, 1872' (2023) Manupatra <https://articles.manupatra.com/article-details/ADMISSIBILITY-OF-ELECTRONIC-EVIDENCE-UNDER-THE-INDIAN-EVIDENCE-ACT-1872> accessed 7 October 2024
[24] Batuk Lal, *Batuk Lal's Law of Evidence in India: The Only Single Volume Commentary on the Indian Evidence Act, 1872 with Exhaustive Case Law* (1999).
[25] *Vikram Singh v State of Punjab* AIR 1007 (2010)
[26] Batuk Lal, *Batuk Lal's Law of Evidence in India: The Only Single Volume Commentary on the Indian Evidence Act, 1872 with Exhaustive Case Law* (1999).

(c) It must provide details about the device used to generate the record;

(d) The certificate must address the conditions under Section 65B(2);

(e) It should be signed by a person holding a responsible official position related to the operation of the relevant device.

Crucially, such a certificate under Section 65B must accompany the electronic record, whether it is a computer printout, compact disc (CD), video compact disc (VCD), pen drive, or similar device when the statement related to it is introduced as evidence. These measures are essential to ensure both the source and authenticity and integrity, which are fundamental to the use of electronic records in evidence. Given the susceptibility of electronic records to tampering, alteration, transposition, or excision, failure to adhere to these safeguards can result in a miscarriage of justice in a trial reliant on such proof.[27]

The production of scientific and electronic evidence in court significantly aids the investigating agency and prosecution. Thus, in a murder case, the failure to produce CCTV footage, collect call records, or retrieve SIM details from seized mobile phones cannot merely be viewed as investigative lapses but constitutes the withholding of crucial evidence. As the prosecution has not claimed any inability to obtain or copy the CCTV footage, an adverse inference was drawn against the prosecution.[28] Spectrophotometric analysis could not be performed on a voice recorder recording that was the only proof of the accused's demand for a bribe, according to the Forensic Laboratory. Though there was a contention that the witnesses—who were not there during the recording—had translated and confirmed the discussion, it was pointed out that they had not heard it. This meant that depending only on the translated version was unnecessary because the voice recording itself could not be examined. For electronic evidence to be considered legitimate, the translation must have the original source; without it, it loses authenticity.[29]

The Supreme Court in Anvar P.V. vs. P.K. Basheer & Ors.[30] opined that a certificate must accompany the electronic record when it is presented as evidence. However, this principle, as established in Paras Jain vs. State of Rajasthan and Kundan Singh vs. State, was upheld in

[27] *Anvar P. v. P.K. Basheer* AIR 180 (2014)
[28] *Tomaso Bruno v State of UP* AIR 412 (2015)
[29] *Sanjaysinh Ramrao Chavan v Dattatray Gulabrao Phalke* SCC 3 (2015)
[30] *Anvar P. v. P.K. Basheer* AIR 180 (2014)

Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal[31], where the Court clarified that, as long as the trial proceedings have not concluded, the judge may direct the submission of the requisite certificate at any stage. This allows the electronic information to be admitted and relied upon as evidence. It was further established in Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal[32] that the trial judge is required to summon the individuals listed under Section 65B(4) of the Indian Evidence Act if an inadequate certificate is provided or if such a certificate is requested but not provided by the relevant person. The judge must ensure that the certificate is secured from the relevant individuals when the electronic record is introduced as evidence without the necessary certificate.

DIGITAL FORENSICS: UNCOVERING KEY EVIDENCE IN THE COURTROOM

Due to the inherent complexities of digital evidence, certain determined standards must be upheld for its admissibility in court. As Olivier Leroux has highlighted, "These unique characteristics do not exempt electronic evidence from the legal requirements applicable to traditional evidence. Computer-generated evidence must possess all the attributes of conventional evidence to be considered valid in legal proceedings."[33]

The examination of digital evidence within legal contexts involves a complex process that necessitates specialised expertise and skills, including data generated from computers, smartphones, social media, and various electronic devices. Such digital evidence may only be admitted after overcoming complex legal and technological issues. It must be proven to be genuine, trustworthy, and honest in order for it to be accepted as evidence in court. The collection, preservation, and analysis of digital evidence are expected to comply with strict and established protocols and a high degree of technical expertise.[34] The introduction of digital evidence in legal proceedings has raised numerous legal and ethical issues, including concerns about privacy, the risk of tampering or manipulation, and the imperative for well-defined guidelines and standards governing the collection and utilization of digital evidence. A deep comprehension of the complex interplay between technology and the law is essential in order to fulfill the requirements for handling digital evidence. Furthermore, to ensure proper

[31] *Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal* AIR 4908 (2020)
[32] *Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal* AIR 4908 (2020)
[33] Olivier Leroux, "Legal Admissibility of Electronic Evidence1" (2004) 18 International Review of Law Computers & Technology 193 <https://doi.org/10.1080/1360086042000223508>.
[34] Dr. Pratyusha Das and Pradeepta Sarkar, 'The Importance of Digital Forensics in the Admissibility of Digital Evidence' [2022] NUJS Journal of Regulatory Studies 61

supervision and admissibility of such data in judicial processes, it is vital to follow recognized best practices in digital forensics and evidence handling.[35]

The evaluation of the evidence in India by the judiciary depends upon its relevance to the case, authenticity, and fidelity to the original source. Digital evidence encompasses a wide range of information, including emails, digital photographs, ATM transaction logs, and computer-generated documents. There are crucial factors upon which the accuracy of digital evidence depends.[36] First, the evidence must have a well-documented chain of custody to confirm that it has not been tampered with or altered. Second, the tools employed for analyzing the evidence must be reliable, properly certified, and current, and the investigators handling them must possess the necessary training and expertise.[37] Emphasizing the importance of genuineness, reliability, and preserving the integrity of the evidence in its original form, The Supreme Court of India established the standards of admissibility of digital evidence in Anvar PV V. PK Basheer[38]. Digital evidence encompasses a range of modernized media formats used in court cases, inclusive of digitally enhanced latent fingerprints, forensic video analysis, and enhanced audio and photo files. The evidence must be handled with extreme care in order to protect its integrity and prevent claims of falsification or tampering. The competence of legal experts to handle cases containing digital evidence in a competent and unbiased manner determines the credibility of the judiciary.

APPLICATION AND SCOPE OF BHARTIYA SAKSHYA ADHINIYAM

The new criminal laws introduced in 2023 and brought in force in 2024 have brought significant changes to the criminal laws as we know it. Bharatiya Sakshya Adhiniyam, 2023 which superseded Indian Evidence Act, 1872 has expanded the definition of what constitutes as an admissible evidence and brought substantial alterations to the procedure and governing the evaluation of the evidence presented before the court. These modifications aim to enhance the evidentiary process in the legal framework. Section 57 of the Bharatiya Sakshya Adhiniyam, which addresses the concept of Primary Evidence, has enlarged the scope of what can be regarded as primary evidence in the legal framework. Section 57 in relation to electronic

[35] K.K. Arthur and H.S. Venter, 'An Investigation Into Computer Forensic Tools' [2004] ISSA 1-11
[36] Batuk Lal, *Batuk Lal's Law of Evidence in India: The Only Single Volume Commentary on the Indian Evidence Act, 1872 with Exhaustive Case Laws* (1999).
[37] Rahul K. Bharati, Pragati G. Khodke, 'Forensic Bytes: Admissibility and Challenges of Digital Evidence in Legal Proceedings' [2024] IJSRST 24-35
[38] *Anvar P. v. P.K. Basheer* AIR 180 (2014)

records now extends to include[39]:

1. An electronic or digital record stored, and such storage occurs simultaneously and subsequently in multiple files, each file would be primary evidence in the eyes of law.

2. Where an electronic record is produced from a proper custody legally, such digital record would be primary evidence unless the custody or the authenticity is disputed.

3. Simultaneous storage of video recording and it's broadcasting or transmission or transfer to other device would render all such recordings as primary evidence. Each version of the recording, regardless of the manner of transfer, is considered primary evidence.

4. Digital record stored in multiple storage spaces in a computer resource, each such automated storage, including temporary files, is primary evidence. Each instance of such automated storage, regardless of its nature, is regarded as primary evidence, provided they are generated from the same digital source.

Section 63 of Bharatiya Sakshya Adhiniyam provides a detailed framework for cases where multiple computers or devices connected through a network over a period involved in generating, transferring, or storing digital records might be involved.[40] Section 63 of BSA juxtaposes Section 65 of Indian Evidence Act dealing with the admissibility of the electronic records in the court.[41] Section 63 of BSA expands upon and refines these principles to better understand and navigate through the intricacies of modern digital evidence.

Section 63 of BSA encompasses all electronic records that are printed on paper, preserved, recorded, or duplicated in optical, magnetic, or semiconductor memory which is produced by a computer or any communication device or otherwise stored, recorded or copied in any electronic form. This provision broadens the scope of admissible digital evidence, ensuring the various forms of electronic storage, regardless of the medium, are recognised in legal proceedings.[42] The new law further expands the scope of digital records by including not only the electronic records but information or records generated by communication devices.

[39] Bharatiya Sakshya Adhiniyam 2023, s 57
[40] Bharatiya Sakshya Adhiniyam 2023, s 63
[41] Indian Evidence Act 1872, s 65
[42] Bharatiya Sakshya Adhiniyam 2023, s 63

Subclause 3 of Section 63 of BSA is includes the function of creating with storage or processing the information for the purpose of activity regularly carried on over that period which was regularly performed by means of one or more computers or communication devices, whether in a standalone mode, on a computer system, on a computer network, or on a computer resource enabling information, creation or providing information, its processing and storage.[43]

Subsection 4 of Section 63 of BSA stipulates that where it is desired to give a document in evidence by virtue of this section, it must be accompanied with a certificate with the electronic record at each instance where it is being submitted for admission.Such certificate shall identify the electronic record containing the statement and outline the method by which it was produced.[44] Additionally, it shall provide all the particulars of the device regarding the creation of that digital record. The certificate shall be signed by the person in charge of the computer or communication device from which the digital record has been generated. The provision ensures the authenticity and traceability of electronic records used in legal proceedings.

EVOLUTION THROUGH CASE LAWS

In the landmark case Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal[45], the Supreme Court addressed three imperative issues pertaining to SECTION 65B of the Indian Evidence Act. The aforementioned issues are:

1. Is Section 65B an all-inclusive code that governs the acceptance of secondary digital evidence in India?

2. Is getting a certificate under Section 65B(4) always necessary?

3. The precise point in criminal or civil proceedings where this certificate needs to be shown.

While addressing issue number 1, the Court in State(NCT Of Delhi) v. Navjot Sandhu @ Afsal Guru[46]stated that It was contended that whether or not standards mandated by Section 65B were satisfied, secondary digital evidence might be presented under other provisions of the

[43] Bharatiya Sakshya Adhiniyam 2023, s 63(3)
[44] Bharatiya Sakshya Adhiniyam 2023, s 63(4)
[45] *Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal* AIR 4908 (2020)
[46] *State(NCT Of Delhi) v. Navjot Sandhu @ Afsal Guru* 11 SCC 600 (2005)

Evidence Act, including Sections 63 and 65. This could be carried out even in the event that the certificate required by Section 65B, subsection 4, is not present. However, this was not the intention behind the enactment of the provisions after the amendment to the Indian Evidence Act. The court's decision was overruled in Anvar PV v PK Basheer and Others[47], and it became clear that careful adherence to the process specified in Section 65B is required when proving documentary evidence in the form of an electronic record. The legal interpretation of the verdict was upheld in the Arjun Panditrao[48] case, indicating that Section 65B functions as the all-inclusive code that regulates the acceptance of electronic documents. Since the court established strict requirements in Anvar's case, it was the case that the plaintiff lacked control over the exact language of a certificate in instances requiring certificates from third parties. As a result, since they could not receive the necessary certification in the required format, legitimate litigants have frequently been treated unfairly.

The Supreme Court in Arjun Panditrao case held that the non-obstante clause in Section 65B(1) of Indian Evidence Act makes it explicit that there should be strict adherence to the provisions laid down in Section 65B for the admissibility and proof of the information contained in the digital evidence. The non-obstante clause in Section 65B gives it a higher power making it a special provision which on the other hand rendered Section 62 to Section 65 of the Evidence Act inapplicable for proving electronic record.[49] The Apex Court observed that Section 65B(1) of Evidence Act draws a line between the original information contained within a computer and the copies made for the information thereof. The original information stored in a computer constitutes primary evidence, while the copies made or derived from it are regarded as secondary evidence.[50] The exclusion of the words "under section 62 of the Evidence Act" from the 24th paragraph of The Anvar P.V. v. P.K. Basheer[51] judgement depicts the ratification of affirmation of the observation by the Supreme Court. The Supreme Court further clarified that the original document may be authenticated by the owner of a laptop, computer, or mobile phone through verification of ownership of the device. The Court reaffirmed that compliance with Section 65B of the Evidence Act is a mandatory prerequisite for the admissibility of electronic evidence, particularly in relation to secondary evidence such as computer output. This distinction highlights the specific procedural requirements applicable to both primary and

[47] *Anvar P. v. P.K. Basheer* AIR 180 (2014)
[48] *Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal* AIR 4908 (2020)
[49] Batuk Lal, *Batuk Lal's Law of Evidence in India: The Only Single Volume Commentary on the Indian Evidence Act, 1872 with Exhaustive Case Laws* (1999).
[50] *Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal* AIR 4908 (2020)
[51] *Anvar P. v. P.K. Basheer* AIR 180 (2014)

secondary evidence.

CONCLUSION

Section 65B of the Indian Evidence Act, in its current form, poses substantial challenges for litigants on account of their inability to procure the certificate mandated, especially when the device from which the electronic record is produced is not in their ownership or control. Section 65B in its strict wording makes it mandatory for the certificate to be produced before the court in case of presenting an electronic evidence and offers no scope of flexibility or relaxation. This issue was addressed by the Apex Court in Arjun Panditrao where they attempted to make an exception for the cases in which the parties, despite making their best efforts, are unable to procure the certificate. The present ratio decidendi aims to mitigate the rigid application of the section and provides a window of flexibility and relief to the litigants facing obstacles in obtaining the certificate.

Prominently, Arjun Panditrao also casts an onus on the courts to summon the certificate from the person who is authorised to attest it as mandated under Section 65B(4), which in all likelihood leans to a mini-trial, thus delaying the justice to the parties and substantially increasing the expense. Furthermore, this process adds to the pendency of the matters before the courts, thereby exacerbating the judiciary's burden and adversely impacting the disposal of cases and speedy trial.