Page 81 - 97 **DOI:** *https://doij.org/10.10000/IJLSI.112094*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 6 | Issue 4

2024

Navigating the Legal Landscape of Electronic Evidence in India

DR. MANOJ KUMAR SHARMA[1] AND MANVEE SHARMA[2]

ABSTRACT

Advent of information technology affected every walk of life including the judicial system. Use of information technology and audio-video electronic means in day to day life led to the generation of new form of evidence i.e. electronic evidence. Electronic evidence was sought to be governed by insertion of provisions in the century old Indian Evidence Act, 1872 by Information Technology Act, 2000. Since the inception of the provisions relating to electronic evidence, the same have been subjected to varied judicial interpretations making it difficult for the parties to produce electronic evidence in Indian courts. Varied and often conflicting judgments and legislative gaps made it difficult for litigants to present electronic evidence in courts in India. To settle the law, the Constitutional Courts have interpreted the provisions and have given detailed standard operating procedure for identification, collection, production and admissibility of electronic evidence in India. In 2023, the Parliament of India came up with new criminal laws including the new law of evidence i.e. Bharatiya Sakshya Adhiniyam, 2023. The Adhiniyam has amended the law relating to production and admissibility of electronic evidence. This paper explores the law relating to production and admissibility of electronic evidence from 2000 to 2024 in the light of relevant judicial decisions and amendments introduced. The paper analyses the difficulties posed by the judicial decisions and the amendments introduced by the Adhiniyam.

***Keywords**: Electronic Evidence, IEA, BSA, Court.*

I. INTRODUCTION

Parliament of India enacted three important laws viz., *Bharatiya Nyaya Sanhita*, 2023; *Bharatiya Nagrik Suraksha Sanhita*, 2023; and, *Bharatiya Sakshya Adhiniyam*, 2023. These laws have been enacted with various purposes, including but not limited to, shedding colonial legacy, making laws gender neutral, aligning laws with the technological developments, ensuring expeditious trial, expanding the scope of audio-video electronic means and forensic evidence in justice delivery system. The increased emphasis on use of audio-video electronic means in inquiries, investigation and trial and the growth of use of IT tools in investigation and

[1] Author is an Associate Professor at Rajiv Gandhi National University of Law, Punja, India.
[2] Author is a student at Rajiv Gandhi National University of Law, Punja, India.

 [ISSN 2581-9453]

trial mandates the exploration of the law relating to production and admissibility of electronic evidence in India. The provisions for the relevance, production and admissibility of electronic evidence were primarily contained in *Indian Evidence Act*, 1872[3] (hereinafter, "IEA") which has been replaced by *Bharatiya Sakshya Adhiniyam, 2023*[4] (hereinafter, "BSA") with effect from July 1, 2024.

The present paper is an attempt to analyze the conundrum of electronic evidence in India. The paper analyses the journey of electronic evidence in India in the light of legal provisions enunciated in IEA and BSA and the judicial interpretation of legal provisions by constitutional Courts. The paper explores the legal position before the enactment and implementation of BSA and the impact of the BSA provisions on production and admissibility of electronic evidence in India.

II. ELECTRONIC EVIDENCE AND ITS ADMISSIBILITY UNDER INDIAN EVIDENCE ACT

(A) Electronic Evidence

Advent of internet and information technology has opened new vistas and posed new challenges for criminal justice system. The increased use of electronic means for financial transactions as well as for communication, storage, transmission etc. has impacted judicial system, as well. The increased use of information technology has brought to the fore, the electronic evidence and in the present-day era, in almost each case, electronic evidence, in one form or the other, has become a reality.[5] Before proceeding further, it is worthwhile to briefly refer to the meaning of the term electronic and digital evidence.

Electronic and Digital evidence includes information kept on third-party storage platforms, social media sites that are hosted across several jurisdictions, cloud services, and third-party cloud storage services. The majority of evidence provided in civil and criminal trials consists of emails and CCTV footage, among other recordings and images. Evidence may even be provided of in-game conversation sessions or data automatically saved by Internet of Things (IoT) devices etc.[6] As such, electronic and digital evidence may be found at several places including emails, CCTV DVR, files in computer and communication devices including deleted files, encrypted files, temporary files, files in recycle bin, cache files, cookies, web-history etc. In addition, evidence may also be found in cloud servers, domain access logs, email-server

[3] The Indian Evidence Act, 1872, No. 1, Acts of Parliament, 1872 (India).
[4] The Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
[5] Rajat Tripathi, *Whether Certificate u/s 65b (4) Evidence Act is Compulsory for the Admissibility of Electronic Evidence*, 2.4 JCLJ 642 (2022)
[6] N.S. Nappinai, *Electronic Evidence - The Great Indian Quagmire*, 3 SCC 3 J-41 SCC (2019).

access logs, recycle bin, pictures, videos etc. As such, the domain of electronic evidence is very wide.

Even *Whatsapp* chat can also be used in evidence. In *Ambalal Sarabhai Enterprise Ltd. v. KS Infraspace LLP Ltd.*,[7] the Apex Court held that WhatsApp messages which are virtual verbal communications are matters of evidence with respect to their meaning and their contents are to be proved during trial by examination-in -chief and cross-examination. Moreover, in *Mewa Mishri Enterprises Private Limited v. AST Enterprises Inc.*[8], there is no absolute bar on the use of WhatsApp messages in legal proceedings subject to the applicable rules of evidence.

(B) Admissibility of Electronic Evidence under IEA

Admissibility of electronic evidence in India was enabled by *Information Technology Act*, 2000 which amended IEA to provide for relevancy and admissibility of electronic record and statements made electronically. The relevant provisions were inserted in IEA in Sections 3, 17, 22A, 35, 45A, 47A, 59, 65A, 65-B, 73A, 85A, 85B, 85C, 90A etc. These provisions provided for the use of electronic records as evidence.

The primary provisions relating to production and admissibility of electronic evidence were enshrined in Sections 65A and 65-B of the IEA.

Section 65-B (1) provides that a printout of an electronic record or saving it onto a USB drive or CD will be treated as a regular document and can be used as evidence.[9] However, several requirements need to be fulfilled before electronic evidence may be used in court, to prevent corruption or tampering. Section 65-B (2) enumerates the technical conditions regarding admissibility of computer output of electronic record. Further, section 65-B (4) lays down the non-technical conditions and calls for a certificate to prove compliance with the requirements of section 65-B (2). This certificate needs to be signed by a responsible person who is aware of electronic records and the way it was produced.

Technical conditions for admissibility of computer output of electronic record as laid down in section 65-B(2) are:

(a) The information was created by the computer while it was being used regularly to store or process data for activities that were regularly carried out by the person with legal control over the computer.

(b) During that time, the computer was regularly fed data that is either contained in the

[7] Ambalal Sarabhai Enterprise Ltd. v. KS Infraspace LLP Ltd., (2020) 5 SCC 410
[8] Mewa Mishri Enterprises Private limited v. AST Enterprises Inc., (2021) SCC Online Del 3332.
[9] The Indian Evidence Act, 1872, § 65-B (1), No. 1, Acts of Parliament, 1872 (India).

electronic record or used to generate that data.

(c) Throughout a significant portion of that time, the computer was functioning properly.

(d) Computer output is directly or indirectly derived from data entered into the computer as part of the aforementioned actions.

Non-technical conditions were provided in section 65-B(4) of the IEA. Section 65-B(4) contemplated a certificate regarding the computer output of the electronic record satisfying the following conditions:

(a) The certificate must identify the electronic record containing the statement and explain its production process;

(b) Certificate should provide details about device(s) used to create the record;

(c) Certificate must contain a declaration as to technical conditions listed in Section 65-B(2);

(d) Certificate must be signed by a responsible official.

III. JUDICIAL INTERPRETATION OF THE PROVISIONS RELATING TO ELECTRONIC EVIDENCE: THE PRE-BSA DEBATE

Section 65-B of the IEA pertaining to the production and admissibility of the computer output of the electronic record as evidence was one of the most contentious sections under the IEA over the last two decades. Introduced in the year 2000 as a result of an amendment introduced by the *Information Technology Act*, the clause was designed to address concerns over the validity of electronic documents while also guaranteeing general adaptability to their use in courtrooms.

The crucial issue regarding electronic evidence is its trustworthiness. Maintaining the integrity of the electronic evidence throughout the process of investigation, examination and trial is difficult[10], if not impossible since its tempering is easy. One does not need to be a rocket scientist to temper the electronic evidence. Therefore, the Courts have to grapple with the issues of relevancy, admissibility and more importantly, the credibility of electronic evidence. In this backdrop, in this section, the discussion shall be focussed on the judicial trends regarding the admissibility of electronic evidence before the BSA.

There have been various cases, where the requirement of the certificate has been discussed and

[10] Vipul Vinod, *Snag of Electronic Evidence*, 12 RMLNLUJ 166 (2020).

debated at large. For instance, in *State (NCT of Delhi) v. Navjot Sandhu*[11], the primary issue before the court was whether the printouts of call records could be considered as evidence without a certificate u/s 65-B (4). To this, the Apex Court held that secondary evidence can be admitted to prove the contents of electronic records and ruled out the necessity of a certificate by acknowledging the practical difficulties in cases involving large volumes of electronic records. The court emphasized that practical difficulties might be posed by strict adherence to the certificate requirement and called for flexibility in the admission of electronic evidence by allowing the use of secondary evidence under other provisions of the IEA.

However, in *Anvar v. Basheer*[12], the three judge bench overruled the above portion of the judgment in *Navjot Sandhu*. This case involve the production of CDs containing electronic records wherein the Supreme Court held that electronic evidence would not be admitted as evidence unless produced with a certificate under section 65-B(4) as it was mandatory requirement. The Apex Court ruled that section 65B is a complete code in itself and evidence outside it cannot be used to prove genuineness. The Court ruled that the primary evidence of electronic record in the form of the computer, mobile etc. can be given, however, whenever the secondary evidence in the form of computer output is to be given, the certificate under section 65-B shall be mandatory.

Further, in *Tomaso Bruno v. State of UP*[13], the court reviewed whether the IEA admits secondary evidence of electronic record without compliance with section 65-B. The three-judge bench ruled that secondary evidence can be given under section 65, therefore without complying the requirement of certificate. The ruling in *Tomaso Bruno* is consistent with the ruling in *Navjot Sandhu.* The decision in *Anvar* was, however, not referred to and hence was not taken into account. The observations in *Navjot Sandhu* were also echoed by a two-judge bench in *Sonu v. State of Haryana*[14], where the court held that a Section 65-B(4) certificate is merely a "mode of proof" and there might be other ways to prove the authenticity of records. This was followed by *Shafhi Mohammad*[15] wherein the court carved out an exception to cases where a party has no control over the device in which original electronic evidence is stored.

Thus, both the cases (*Anvar v. Basheer* and *Navjot Sandhu)* represent contrasting interpretations concerning the admissibility of electronic evidence and therefore an authoritative ruling on the subject matter was required. Thereby, the case was referred to a

[11] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
[12] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[13] Tomaso Bruno v. State of UP, (2015) 7 SCC 178.
[14] Sonu v. State of Haryana, (2017) 8 SCC 570.
[15] Shafhi Mohammad v. State of H.P., (2018) 2 SCC 801.

three-judge bench in *Arjun Panditrao,*[16] wherein the court held that Section 65-B operates as a non-obstante clause meaning that it creates its own rules and is applicable independently of other provisions.

Accordingly, three-judge of the Supreme Court in the case of *Arjun Panditrao Khotkar* revisited the meaning and interpretation of Section 65-B. The factual backdrop concerns the appellant's election (a successful candidate) to the State Legislative Assembly which was challenged by the respondent (a defeated candidate) and an elector in the constituency. The complaint was filed because the appellant's nomination papers were incorrectly accepted by the Election Commission after the deadline on the stipulated date i.e., after the stipulated time. The respondents attempted to use video-camera recordings from arrangements made both inside and outside the Returning Officer's (RO) office to bolster their claim. Following the directive from the High Court to provide original video recordings of the two days designated for filing nomination form, the Election Commission presented Video Compact Disks (VCDs) to the Court. These VCDs' recordings made it abundantly evident that the nomination papers were submitted after the deadline. Interestingly, though, even after the respondents requested it, the RO's office declined to provide a certificate under Section 65-B (4) of the Act.

The main issue which the High Court had to decide was whether VCDs could be produced as evidence in the absence of certificate u/s 65-B(4) of the Act. Interestingly, during cross-examination, an official from RO's office acknowledged that no complaints had been made regarding the performance of the cameras that were placed there. She also acknowledged that the RO's office frequently utilized the cameras to capture events and that a VCD of the recordings was collected daily. The VCDs were even included as a part of the Election Commission record. In light of the evidence gathered during the cross-examination, the High Court noted that the requirements outlined in the Act regarding the credibility of electronic evidence have been fulfilled.

The primary contention before the Supreme Court was that as per the earlier ruling of three Judges in *Anvar P.V. v. P.K. Basheer*, a written and signed 65-B (4) certificate was held mandatory for the admissibility of electronic records, and no oral evidence could be presented to support the requirement thereof. It was thus claimed that the VCDs could not have been brought as evidence without such a certificate. Further, in *Shafhi Mohammad v. State of H.P.*, a two-judge bench of the Apex Court held that the certificate under Section 65-B(4) was not always necessary and might be waived in the interest of justice. In light of an apparent

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

discrepancy regarding the interpretation of Section-65-B by two Judges in *Shafi Mohammad* and three justices in *Anvar*, the matter was submitted to a three-judge bench in *Arjun Panditrao* for clarification.

The judgment in *Anvar* was upheld by a three-judge bench of the Supreme Court, holding that Sections 65-A and Section 65-B fully regulate the admissibility of electronic evidence under the Act and ordinary procedures – that are included in other parts of the Act – are not relevant. The Court declared the observations in *Shafi Mohammad* as *per incuriam* and held that in cases where the original electronic record – as it exists on the computer device – cannot be produced then, a certificate under 65-B (4) is mandatory.

In deciding *Arjun Panditrao*, the Supreme reiterated decision in *Anvar P.V.* and might have committed the same mistake by making it mandatory to produce a certificate.[17] It is indeed very difficult to produce a certificate when the party is not in possession of the device as is evident from the facts of the *Arjun Panditrao* case. However, the Supreme Court did admitted that a party can-not be compelled to do an impossible act and accordingly, if a party has done everything to procure the certificate and has obtained an order from the Magistrate to procure the certificate, then the Court may admit the electronic evidence even without a certificate under section 65-B of IEA, thus settling the law regarding admissibility of electronic evidence.

However, the Supreme Court did not clarify in *Arjun Panditrao* regarding at what stage, the certificate is required to be filed, whether the same is required to be filed at the time of filing the charge-sheet or can it be supplied at a later stage.[18] This question was dealt with by the Rajasthan High Court in *Paras Jain* v. *State of Rajasthan*[19]. Rajasthan High Court ruled that when the additional evidence can be given during trial with the permission of the Court, there is no reason to deny the production of section 65-B certificate at a later stage, if the same was not available or not produced at the time of filling the charge-sheet. Court ruled that it is merely a cosmetic issue that may be easily corrected.

Same view was taken by the division bench of the Delhi High Court in *Kundan Singh* v. *State*[20]. In the instant matter certificate under section 65-B regarding call data record was not filed earlier and was filed only during the re-examination of the official of telecom company. Based on the decision in the *Anvar P.V.* case, the division bench of Delhi High Court ruled that certification of electronic records is not required to be done simultaneously under Section 65-

[17] Devang Chhtrapati and Arun B Prasad, *Electronic Evidence-Admissibility and Authentication: A Judicial Perception of Apex Court of India*, 3.1 GLS LJ 50 (2021).
[18] Kurain Joseph, *Admissibility of Electronic Evidence*, 5 SCC J- 1 (2016).
[19] 2015 SCC OnLine Raj 8331.
[20] 2015 SCC OnLine Del 13647.

B.The requirement that an authorised person certify the computer output under sub-section (4) to Section 65-B at the same time as it is reproduced on optical or magnetic media is not posited or imposed by Section 65-B.

In *Sonu v. State of Haryana*[21] the Supreme Court clarified another aspect regarding production of certificate under section 65-B. In the instant matter, CDRs were marked before trial Court without a certificate under section 65B (4). The objection was raised at the later stage. Court ruled that an objection to the form or method of proof must be brought at the time that the document is marked as an exhibit and not at a later time. The Court finally held that an argument that CDRs are unreliable because of a violation of the procedure established in Section 65 B (4) cannot be allowed to be raised at the appellate stage since the objection pertains to the form or technique of proof.

Perusal of the judicial decisions brings to surface that certificate is mandatorily required when the computer output of electronic record i.e. secondary evidence is produced whereas when the original device (primary evidence), for example mobile containing the electronic record, is produced, certificate is not mandatory as stated in *Anvar* and *Arjun Panditrao.*

It must be kept in mind that ordinarily the information is recorded in computer in a binary language which is computer readable and not human readable.[22] The computer output is human readable and therefore, if we apply the traditional notion of primary and secondary evidence to electronic records, the information shown in communication devices and computers may never be primary but only secondary.

IV. ELECTRONIC EVIDENCE UNDER THE BHARATIYA SAKSHYA ADHINIYAM

BSA, 2023 has introduced several amendments regarding admissibility of electronic records. The amendments range from amending the statutory dictionary clause regarding the electronic and digital evidence, broadening the scope of primary evidence of electronic records by inserting explanations to section 57, and amendment of the procedure for admissibility of evidence and digital evidence. These amendments are discussed in this section.

(A) Deciphering the Amendments in the Statutory Dictionary Clause

IEA was enacted in 1872 and thus, has become outdated due to technological advancements that have occurred since then. Despite updation by IT Act, IEA has not fully kept pace with the rapid evolution of technology. Provisions for dealing with Digital Evidence, electronic

[21] (2017) 8 SCC 570.
[22] Yuvaraj v. State, 2023 SCC OnLine Mad 3621.

signatures, cybercrimes and forensic evidence, audio-video evidence, and virtual hearings etc were found insufficient. To address these issues, there have been constant calls for reforms to amend the Evidence Act and incorporate provisions that reflect the realities of the modern digital age.

Echoing this sentiment, amendments have been introduced to Section 2 of the BSA which deals with definitions. These involve:

a. Definition of 'Document': Section 2(1)(d) of BSA

Section 2(1)(d) of the BSA (corresponding to IEA, Section 3 (para 5) defines "document" in consonance with the modern digital era. It specifically includes digital and electronic records within the ambit of "document." The five statutory illustrations in the previous definition have been kept. The new definition has introduced a sixth illustration that clarifies that "an electronic record on server logs, emails, documents on laptops, computers, or smartphones, websites, messages, locational evidence, an voice mail messages stored on digital devices are documents."[23]

According to the new definition, the matter need not necessarily be described upon any substance using solely letters, figures, or marks to be considered a "document" or "documentary evidence." Any matter that is "otherwise recorded" on a substance "by any other means" is likewise acceptable as "document" or "documentary evidence." Given that scenario, a video recording on mobile phone would be acceptable as a "documentary evidence" as it is "otherwise recorded" upon any substance "by any other means."

The updated definition signifies a marked change in approach in acknowledging the realities of the modern digital world. This is because parties involved in a legal proceeding often depend on digital and electronic records to support their allegations, and claims. The new definition ensures that they are not disadvantaged because of the format of their evidence while also acknowledging the pervasiveness of digital communication and transactions in today's society.

Further, Section 61 of the BSA states that "*Nothing in this Adhiniyam shall apply to deny the admissibility of an electronic or digital record in the evidence on the ground that it is an electronic or digital record and such record shall, subject to section 63, have the same legal effect, validity, and enforceability as other documents*." Thus, the Adhiniyam treats electronic evidence at par with documentary evidence.

[23] The Bharatiya Sakshya Adhiniyam, 2023, § 2(d), *Illustration (vi),* No. 47, Acts of Parliament, 2023 (India).

b. Definition of 'Evidence': Section 2(1)(e) of BSA

Section 2(1)(e) of BSA is corresponding to section 3, para 6 of the IEA. In the new definition of "evidence," 'statements including statements given electronically' are considered as evidence as well as oral evidence. This is logical in the light of section 530 of the *Bharatiya Nagrik Suraksha Sanhita*, 2023 (BNSS) which provides for examination of complainant and witnesses, trial etc. through audio-visual or electronic communication methods.[24]

Traditionally, oral and documentary evidence have always been the two primary categories of "evidence" under the IEA. However, as digital technology and electronic records proliferate, there is a growing realization that electronic evidence must be treated as a separate and distinct category.

The Supreme Court in *Arjun Panditrao v. Kailash Kushanrao* held that Section 65-B is a non-obstante clause that operates independently of all other provisions thus, creating a separate category for electronic evidence. Moreover, with the enactment of new provisions in the BSA, electronic evidence has been explicitly included within the ambit of "documentary evidence." This inclusion signifies an expansion of the scope of electronic records in legal proceedings and a proactive approach to adapt to technological advancements.

Parties are often troubled due to logistical obstacles like scheduling travel, travel hazards etc. The new provision allows the statements given electronically to be considered as evidence thus, ensuring convenience and accessibility. The provision is progressive and it takes into account the possibilities of trial through audio-video electronic means.

Further, we should take note the ruling of the Supreme Court in *Vincent v. The State*[25], where the Court held that the Court should be generous in defending the rights of the accused, however, it also needs to make sure that this generosity does not become a headache for the witnesses and victims of the offenses, thereby resulting in failure of justice.

It is further submitted that even in the new Act, the definition of "Evidence" given in BSA is also narrow and defective as it does not include the statements that are made by the accused or answer to the questions that are put by a judge to the accused. It does not include the evidence that is collected through local investigation and real evidence. So, for instance, as per the definition, blood-stained clothes do not fall under the category of evidence. Similarly, the conundrum of primary and secondary evidence especially with regard to electronic evidence remains unresolved.

[24] The Bharatiya Nagarik Suraksha Sanhita, 2023, § 530, No. 46, Acts of Parliament, 2023 (India).
[25] Vincent v. The State, (2016) SCC OnLine Mad 9048.

(B) Broadening the Scope of Primary Evidence of Electronic Records

Section 57 BSA, 2023 corresponding to Section 62 of IEA has added additional explanations (explanations 4 to 7) to the original section to expand the scope of electronic records, particularly in defining primary evidence.

Explanation 4 – Simultaneous Storage in Electronic Devices

"Where an electronic or digital record is created or stored, and such storage occurs simultaneously or sequentially in multiple files, each such file is primary evidence."

'Primary evidence' refers to original records[26], whereas 'secondary evidence' refers to records which prove the existence of original records. This provision widens the ambit of primary evidence to include electronic records that are stored across multiple devices simultaneously.

For instance, consider a scenario where a customer uses Internet banking for a transaction. The details of the transaction are simultaneously recorded and stored in the bank's main computer system and the customer's device (such as a smartphone or computer) at the same. In such a case, the electronic record of the transaction on the customer's device or bank system would constitute primary evidence under Explanation 4.

Similarly, a post on a social media platform like Twitter or Instagram would also be treated as primary evidence under Explanation 4 as it is simultaneously stored on the platform's servers and the user's device. Likewise, when a person sends an email using a mobile device or desktop, a copy of the email is stored in both the email server and the sender's device.

Explanation 5 – Production from Proper Custody

"*Where an electronic or digital record is produced from proper custody, such electronic and digital record is primary evidence unless it is disputed."*

It specifies that when a digital or electronic record is produced from proper custody then, it would be treated as primary evidence, unless disputed. This provision emphasizes the importance of maintaining proper custody and documentation of electronic records for their admission as primary evidence.

It will also cover digital contracts through online platforms such as e-commerce websites where the platform provider produces copies of the contracts from the custody or financial statements produced by a bank directly from its custody.

[26] LEXOLOGY, https://www.lexology.com/library/detail.aspx?g=ea6bba74-3506-4083-9849-756bc506082d (last visited Mar. 24, 2023).

Explanation 6 – Video Recordings with Simultaneous Storage and Transmission

"Where a video recording is simultaneously stored in electronic form and transmitted or broadcast or transferred to another, each of the stored recordings is primary evidence."

This explanation intends to include video recordings which are simultaneously stored in electronic form and broadcasted or transmitted. It is particularly relevant for video evidence, such as recordings of events or surveillance footage. For example, the recording of an incident of theft in a retail store by the store's CCTV camera, live broadcast of press conferences, or news events over the internet or television streams as they are simultaneously stored in electronic form and transmitted to viewers worldwide.

Explanation 7 – Automated Storage

"Where an electronic or digital record is stored in multiple storage spaces in a computer resource, each such automated storage, including temporary files, is primary evidence."

This explanation pertains to multiple storage spaces in a computer resource, including temporary files and each such automated storage shall be considered primary evidence. It extends beyond individual files to include all automated storage areas within a computer resource. Explanation 4 specifically emphasizes upon sequential or simultaneous storage of electronic records in multiple files whereas Explanation 7 widens the ambit to include all automated storage spaces irrespective of whether they are stored in individual files or distributed across.

Examples of Explanation 7 vis a vis Explanation 4

Consider a scenario where a graphic designer is working on a digital illustration using software; as he creates a design, he modifies it as and when he gets a new idea. The software automatically saves the previous data by generating temporary files. Thus, each temporary file along with the final saved file would be primary evidence under Explanation 4 as they are sequential storage of electronic records.

On the other hand, suppose an individual uses Google Cloud to store his data like text files, videos, and photos. These documents are synchronized on multiple devices, including tablets, computers, and smartphones. The cloud service also creates backups and temporary caches to ensure data integrity. Thus, all these storages, including backups, temporary caches, and synchronized files over various devices, are primary evidence under Explanation 7.

(C) The Four Explanations and their Implications

These explanations have expanded the ambit of primary evidence which means that parties can

now present a broader variety of electronic evidence, such as information kept on several platforms or devices like smartphones, core computer systems, cloud storage devices, etc., They can rely on these electronic records to strength their case and providing detailed corroboration of events.

In cases of documents that are obtained from proper custody like official custodians or legitimate sources then, parties can present them without the need for extensive authentication procedures.

Even in cases where electronic records are obtained from stolen devices (that are seized from the custody of the accused) then, despite the illicit nature of the source, they can still be considered as primary evidence if they are obtained and produced from proper custody.

By acknowledging electronic records in multiple locations and formats as primary evidence, parties can present them with assurance that they will be accorded the same weight and validity as any other evidence. Thus, in a cyberbullying case, if a victim presents screenshots of the offensive texts received from the perpetrator that are stored in her smartphone and backed up on the cloud, they would be given equal weightage and validity as any other form of evidence.

(D) Changes Regarding Admissibility of Electronic Evidence

Section 61, BSA is a new provision about the Admissibility of electronic or digital records. Phrase, "*Nothing in this Adhiniyam shall apply to deny the admissibility***"** in section 61, BSA hold significance. It ensures that digital or electronic records are not denied admissibility merely because they are in electronic format. Thus, parties can rely on them to bolster their case without any threat of rejection due to their digital nature. They are often easily accessible and more convenient to store and retrieve, especially when present in large quantities. Section 61, therefore, equates both the documents contained in physical form as well documents in electronic form.

As discussed in the previous part, Section 65-B of IEA has been subject to varied interpretations especially whether it is an exclusive provision for proving electronic records. BSA now clarifies that Section 65-B like provision (section 63 of BSA) is a non-obstante clause and an enabling provision which is applicable notwithstanding the other provisions of the Act, significantly overriding contrasting and conflicting judicial interpretations. However, this does not mean that Section 63 of BSA (section 65-B, IEA) is the only way to prove electronic evidence rather the law intends to make it easier to use electronic evidence. Thus, section 65-B, IEA provides one way, and Section 61, BSA suggests that there might be other ways as well!

 [ISSN 2581-9453]

It is submitted that section 63, BSA necessitates the requirement of a certificate to prove a computer output of electronic record including a copy or a print-out of an electronic record as was mandated in *Arjun Panditrao v. Kailash Kushanrao.*

Perusal of section 63, BSA and its comparison with section 65-B, IEA suggests that many changes have been made regarding the production and admissibility of electronic evidence. Firstly, section 63 BSA has added the terms communication device, semiconductor memory etc. in addition to computers thus widening the scope of its applicability.

Another important change introduced by section 63 BSA is regarding the stage at which certificate is required to be produced. Section 63 BSA clearly stipulates that certificate must be submitted along with the electronic record at each instance when the evidence is submitted for admission. As stated earlier, section 65-B did not specify when the certificate is required to be submitted whether along with the charge-sheet or at the trial.

Further, section 63, BSA requires a twin certificate as prescribed in Schedule appended to BSA. Part B of the certificate is required to be signed by an expert whereas Part A of the certificate is required to be signed by the person in charge of the device. Earlier under section 65-B, IEA, there was requirement of a single certificate which was required to be signed by the person holding responsible official position. The phrase "person holding responsible official position" in section 65-B, IEA perhaps signified that the provision was applicable only to commercial or governmental enterprises and not to individuals.

The certificate under section 63, BSA requires the HASH value to be mentioned in it. The HASH value is required to be declared by the person in charge of communication device as well as by the expert.

It is important to refer here to the meaning of HASh value. A HASH value is a string of characters and integers that serve as a unique ID to electronic records. It is created using an algorithm to identify any tampering with the electronic record. Each electronic record has a unique HASH value, and any modification to the record will cause it to alter drastically. [27]

The requirement for HASH certificates under section 63, BSA might impose an additional burden on parties, particularly if they lack the money or technical know-how to get such certificates. The necessity for further documentation and technical specifications might delay the cases, extending the period parties must wait to receive justice. It may also make the judicial system more complicated, which would make it difficult for parties to understand.

[27] Jon Berryhill, *What is a Hash Value?*, NEWS & COMPUTER FORENSICS (Mar. 27, 2024, 9:24), https://www.computerforensics.com/news/what-is-a-hash-value.

However, the requirement for the HASH certificate might appear unnecessary, especially in cases where the electronic record is undisputed. In such cases, bringing the original device (such as a smartphone or computer) may be easier for the people to bring to the court than having a HASH value rectified by a professional.

V. SEQUENCE OF CUSTODY OF ELECTRONIC DEVICE

Maintaining integrity of electronic evidence is crucial since it is prone to tempering. The matter was highlighted in *CBI v. Nasib Singh Constable*[28]. In the instant matter in Delhi District Courts, the CDs containing the sting operation of a constable accepting bribe were produced in the court along with the certificate under section 65-B(4), IEA. Further, the evidence in the form of certificate from Forensic Science Lab was also produced. However, the evidence was not relied upon by the Court and the accused was acquitted. The electronic evidence in the form of CD was held unreliable despite certificate from Forensic Science Lab and certificate from the owner/journalist under section 65-B(4) on the ground of failure to maintain and prove chain of custody. In the instant matter, the CDs were written by a third party and that third party was not examined as a witness and the factum of his custody of the electronic records was not mentioned in the charge-sheet. This case highlighted the importance of maintaining the record of chain of custody of electronic devices.

Accordingly, when the draft criminal law bills were referred to the Parliamentary Committee, the Parliamentary Committee was of the opinion that safeguarding the authenticity and integrity of electronic and digital records acquired during the course of investigation is crucial due to the fact that such evidences are prone to tampering. Therefore, keeping in view the increased use of audio-video means and the increasing use of electronic evidence, Committee observed that there is dire need to maintain the integrity of electronic evidence. Committee accordingly recommended a provision mandating that all electronic and digital records acquired as evidence during the course of investigation are securely handled and processed through proper chain of custody. This led to insertion of provision in section 193(3)(i) in *Bharatiya Nagrik Suraksha Sanhita*, 2023 which now requires that while submitting the charge-sheet, it shall also include detailed report as to sequence of custody in case of electronic devices.

VI. QUESTIONS LEFT UNANSWERED BY BSA

Undoubtedly new criminal laws have made amendments of far reaching consequence and have

[28] CNR No. DLCT01-012173-2016, Court of Special Judge (PC), decision dated January 19, 2019

cleared the air regarding various lacunas in the criminal justice system. BSA has fortified the law relating to electronic evidence in civil and criminal trials. However, there are still unanswered questions which require clarity.

The first question is who is an expert regrading electronic evidence. Section 39(2) of BSA, 2023 (section 45A, IEA) throws light on the same. Section reads,

"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 79-A of the Information Technology Act, 2000 (21 of 2000), is a relevant fact.

Explanation.—For the purposes of this sub-section, an Examiner of Electronic Evidence shall be an expert."

The aforesaid provision makes the Examiner of Electronic Evidence as an expert but it must be kept in mind that so far the Central Government has notified only the institutions (labs) as examiner of electronic records under section 79A of IT Act. Currently there are 15 such labs which have been notified and most of them are concentrated in Delhi and Gujarat. In-fact there are only seven labs in the rest of the country, making it extremely difficult to have the certificate of the expert of electronic evidence as referred to in section 63, BSA.

Thus, the provision enunciated in section 63 is little difficult to implement. However, the problem may be resolved to an extent by proper interpretation and implementation of section 329, BNSS, 2023 (section 293, CrPC). Section 329 BNSS allows the report of government scientific expert on any matter referred to him for examination and analysis to be used as evidence. BNSS has further expanded the scope of this provision by empowering the state governments to notify any scientific expert whose report can be used as evidence. Accordingly, both the union and state governments can notify any scientific expert including a cyber expert in a forensic lab and his report can be used as expert evidence in electronic and digital evidence matters, as well.

Further, BSA has failed to provide the procedure for identification, collection, preservation and production of electronic evidence in Court. It is apt to mention that Karnataka High Court in *Virendra Khanna v. State of Karnataka*[29] has given detailed guidelines regarding procedure for search of electronic evidence, search of information on the mobile and other communication devices of the accused, procedure for search, identification, collection and preservation of

[29] 2021 SCC OnLine Kar 5032: (2021) 3 AIR Kant R 455

electronic evidence including the use of Faraday bags for preservation of electronic evidence etc. These guidelines were issued by the Karnataka High Court to fill the vacuum and to guide the investigation agencies about the procedure to be followed. However, the legislature has lost the opportunity to provide a comprehensive procedure by inserting and improving upon the guidelines.

VII. CONCLUSION

The advent of Artificial Intelligence powered by Machine Learning and deepfake has added another facet to the use of electronic evidence raising questions about its reliability and credibility.[30] This is important to note that like other evidence, in case of electronic evidence also, source and authenticity are two important factors to be kept in mind.[31]

BSA has made a slew of amendments regarding the acknowledgment of electronic evidence as "evidence" under the Indian law of evidence replacing the archaic law relating to electronic evidence.[32] The goal of these modifications is to improve the accuracy and consistency of electronic evidence. The amendments provide parties with enhanced opportunities to produce crucial electronic evidence that might bolster their case. Further, with the inclusion of electronic evidence, parties can now provide their statements remotely thus, avoiding logistical barriers.

These amendments have attempted to clarify and consolidate the law relating to electronic evidence which was murky and hitherto scattered in various judgments. In addition, the amendments have also attempted to reign in the provisions for ensuring the integrity of electronic evidence by providing for a certification from the person in charge of the device and from an expert. The inclusion of the provision for submission with charge-sheet a document showing the sequence of custody of electronic device is another attempt on the part of the legislature to ensure integrity of electronic evidence. However, the efficacy of such amendments is yet to be seen in times to come.

The journey of admissibility of electronic evidence in India has been rather topsy-turvy from *Navjot Sandhu to Arjun Panditrao.* Amendments have added further scope for making this journey more thunderous by providing complicated solutions and leaving certain questions unanswered.

[30] Daniel Seng and Stephen Mason, *Artificial Intelligence and Evidence*, 33 SAcLJ 241 (2021).
[31] Kumar Askand Pandey, *Appreciation of Electronic Evidence: A Critique of Judicial Approach*, 6 RMLNLUJ 24 (2014).
[32] Yuvaraj v. State, 2023 SCC OnLine Mad 3621.