VOLUME 5 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

INTERPRETATION OF ELECTRONIC EVIDENCE

- Viswa Ganesh K[1]

ABSTRACT

The electronic evidence is born in the digital world and generated, evolved as much as the technologies is developed. The digital world expands the module of human communication as to the physical world. The help taken from the other statute to derive the meaning the electronic evidence. As so many ambiguities are there to exhaustively define the term of digital evidence and its admissibility in the purview of the evidence act.

The Justice in the department of Judiciary have utilized the tool of interpretation vested in their hands to construe the meaning, intent and scope of the particular provisions as it is embedded in the statute or sometimes it is on the discretion of the judge to go beyond the letters on the basis of reasonable ground as the situation made before them in the courts of law. These rules had their own nature of construction to construe the ambit of electronic evidence as per the Indian law.

The research paper addresses the dodge in the applying of the interpreting rule in the evidence as well as the electronic evidence and to adopt the adequate rule to construe its nature, meaning and the scope of the electronic evidence in the ambit of the evidence statute in the secular nation.

Keywords: Digital Evidence, Digital World, Interpretation, Admissibility, Technology.

INTRODUCTION:

Electronic Evidence is a growing concept. It evolves day to day. Making amendments to this growing concept is significant. Society is dynamic in the mode of committing an offence increases and improves according to the changes in society which include economic change and technological changes. The technological changes lead to both positive and negative impacts. Provided its positive or negative they are two sides of the same coin.

[1]4th Year BA LLB (Hons) Student, School Of Excellence In Law, Dr. Ambedkar Law University.

An amendment to a statute not only impacts that particular statute it creates its impacts on the connecting statutes. Likewise, an amendment to the Information Technology Act of 2000 had made its impact on the Indian Evidence Act of 1872, the Indian Penal Code of 1860, and the Banker Book Evidence Act, of 1891.The contemporary evolving concepts are issues with regard to emerging Artificial Intelligence and Digital Forensics.

"WE CAN'T IMAGINE A DAY WITHOUT ELECTRONIC GADGETS"

ELECTRONIC EVIDENCE – MEANING:

The information is created, generated, and transferred in the form of a computer and a digital forum is electronic evidence.

The Authenticity of the computer forum is taken into consideration.

DEFINITION – AN EXTERNAL TOOL USED:

External aid is available outside the purview of the statute as to certain the meaning of the terms that are embedded in the law. The **Connecting statute** is an aid used to find out the meaning of Electronic evidence as it is embedded in the evidence statute. Here the **Information Technology Act of 2000** is a tool for connecting statutes.

The Definition embedded in **section 79A**[2] of the IT Act, 2000 is taken into consideration for the electronic evidence as used in the Evidence Act of 1872.

"Electronic form of evidence means any information of probative value that is stored or transmitted in electronic form and includes digital audio, video, and computer evidence.

Electronic record means data generated, stored, received, or sent in an electronic form."

OVERVIEW OF THE IT ACT OF 2000:

The Information Technology Act provides legal recognition for transactions carried out utilizing electronic data interchange and other modes of electronic communication.[3]

Electronic evidence is a piece of information that is generated in digital devices and has its protection in the scope of the act.

RULES OF INTERPRETATION IN EVIDENCE ACT:

[2]s.79A of IT Act, 2000.
[3]https://dhsgsu.edu.in last visited on Feb 10,2024.

The strict rule of interpretation such as the literal and golden rule is applied in the courts as it comes under the category of substantive as well as procedural statute.

The ordinary and natural sense of the word used in the statute is taken in the interpretation of the provision of evidence act and is termed as a **literal rule of interpretation**.

The judges apply their minds in the terms used in the provisions beyond their natural sense and without modifying their intent of the evidence act and it is termed as **Golden rule of interpretation.**

ELECTRONIC EVIDENCE UNDER THE EVIDENCE ACT OF 1872:

The IT Act amended the Indian Evidence Act of 1872 to recognize electronic records as documentary evidence under section 3 and provide a special procedure to govern their admissibility under **section 65A and section 65B** [4]of the Evidence Act.

The judiciary made contrary opinions on the admissibility of electronic records in the courts. It further clarified the circumstances of its applicability and admissibility in the filed as it was strictly construed.

INTERPRETATION OF SECTION 65B:

The Section 65B of IEA has undergone various interpretations by judicial scrutiny. In the application of the literal as well as the golden rule it is interpreted as follows:

In the case of **State V. Navjot Sandhu**, the electronic records are admitted in the court without the certification of the authenticity as under s.65B of the Evidence Act.[5]

Later, it was overruled in the case of **Anvar P.V. V. P.K. Basheer**[6], the court ruled that the certificate is mandatory for the admissibility of the electronic evidence as secondary evidence as it was construed in the application of the literal rule.

The Supreme Court made de-coding of each sub-section embedded in s.65B in the case of **Arjun Panditrao V. Kailash Gorantyal**[7],

Sub-section (1) – Established the Electronic records as potential evidence.

Sub-section (2) – sets the criteria for the reliability of these records.

[4]s.65A of IEA, 1872.
[5]Dr. S. R. Myneni, Law of Evidence, 205-210 (Asia Law House, 3rd edition, Hyderabad).
[6]Anvar P.V. V. P.K.Basheer AIR 2015 SC 980.
[7]https://www.scconline.com last visited on Feb 13, 2024.

Sub-section (3) – ensures the continuity and integrity of the electronic record are maintained, regardless of the number of devices involved.

Sub-section (4) – mandates the certificate requirement for authenticity of the electronic record.

Sub-section (5) – gives the definition and scope of information supply to the computer.

The New Evidence Bill of 2021 is drafted and the electronic evidence is considered primary evidence based on the landmark judgments delivered in the court of law.

CHANGES PERTAINING TO THE BANKER BOOK EVIDENCE ACT, 1891:

The Bankers' Books Evidence Act of 1891 was amended by the Information Technology Act of 2000 to change the definition of bankers' books. The definition of the Banker book had been put to an amendment to encompass printouts of the data featured on a floppy, disc as well as electromagnetic devices under section 2(3).[8]

Amendment to Section 2(3):

Formerly, the word "bankers' books" solely referred to catalogs, daybooks, money books, accounts books, and other books used in the ordinary course of the bank's operations. Following the amendment, it now covers documents stored on small films, magnetic tape, or other mechanical data retrieval technologies.[9]

Section 2(8)(b):

This section summarizes the definition of a certified copy and states that it includes printouts of any entries accumulated on a small film, magnetic tape, or any other type of mechanical or electronic data retrieval mechanism, as long as the mechanism itself guarantees the printout's precision as an exact replication of the original entry.[10]

Section 2A specifies that a printout or copy of an entry must be accompanied with a certificate from the principal accountant or manager of the branch as well as a certificate from the person in charge of the computer system outlining the system's safeguards.[11]

Radheshyam G. Garg vs. Safiya Bai Ibrahim Lightwalla[12]:

[8]Bankers' Books Evidence Act ,1891, s.2(3) [India]
[9] Ibid
[10]Bankers' Books Evidence Act ,1891, s.2(8)(b) [India]
[11]Bankers' Books Evidence Act ,1891, s.2A [India]

It was stated that the tribunal should not focus on all of the conditions outlined in Section 2(8) of the Act and apply a hyper-technical approach when determining whether a record was legitimately obtained from the source, sustained in the corporation's procedure, and preserved in the bank's possession. The provisions in Section 2(8) of the Act are only advisory and not mandatory.[13]

CHANGES PERTAINING TO THE INDIAN PENAL CODE 1860:

The First Schedule of the IT Act added new offenses and altered the Indian Penal Code (IPC) [14]for certain offenses.The production of documents that have been amended to include electronic records.

- Additional offenses include evading judicial production of documents or electronic records punishable under the IPC section.
- Section 173 of the Indian Penal Code prohibits unlawfully impeding the serving of summons, notice, or proclamation to present a paper or electronic record in court[15].
- Intentionally failing to produce or provide a paper or electronic record to a public official is punishable under section 175, IPC.
- Sections 192 [16]and 193 of the IPC [17]prohibit creating false entries or statements in electronic records with the intent to use them as evidence in court proceedings.
- Section 204 of the IPC prohibits the destruction of electronic records with the aim of impeding their production or use as evidence.[18]
- Creating fraudulent electronic records is punishable under IPC sections 463 [19]and 465.[20]

RECENT RULINGS – CASES:

Case laws play a vital role in interpreting sections of the statute. When there arises an ambiguity about whether to take a strict interpretation or a liberal interpretation the judgment of the cases based on circumstances and facts clears such ambiguity. Precedents serve as the source of interpretation.

---

[12]*Radheshyam G. Garg vs. Safiya Bai Ibrahim Lightwalla* AIR 1988 BOM 361

[13]Bankers' Books Evidence Act ,1891, s.2(8) [India]
[14]Indian Penal Code,1860,[India]
[15]Indian Penal Code,1860,s.173 [India]
[16]Indian Penal Code,1860,s.192 [India]
[17]Indian Penal Code,1860,s.193 [India]
[18]Indian Penal Code,1860,s..204[India]
[19]Indian Penal Code,1860,s.463 [India]
[20]Indian Penal Code,1860,[India]

In ***State v. Navjot Sandhu, 2005***[21]it was held the printouts of phone records could be considered admissible evidence even without a certificate under section 65B(4) of the Indian Evidence Act 1872. [22]

In ***Anvar v. P.K.Basheer, 2015***[23]**,** The above decision was overruled. The Hon'ble Court held section 65B is a complete code. Evidence from any other source would not be permissible. The Indian Evidence Act does not allow proof of an electronic record through oral evidence and states that a certificate under section 65B is mandatory.[24]

In ***Amar v. State of Haryana, 2017***[25]The court reevaluated the requirement of a certificate and concluded the certificate under section 65B(4) a "mode of proof". Therefore non production of a certificate on earlier occasions is a curable defect[26].

In ***Shafi Mohammad, 2018***[27]It was held that the requirement of a certificate is procedural and not mandatory. Relaxation could be provided under certain circumstances. When a party does not have control over the original device 65B is not considered as a complete court. [28]

Based on all these cases there is an inference there is a gap in the interpretation of section 65B of the Evidence Act. **The question of interpretation is whether the certification of electronic evidence under section 65B is mandatory or directory.**[29]

Arjun PanditraoKhotker v. Kailash Krishnarao,2020[30]addressed the contradictions of section 65B. It is regarding the admissibility of electronic evidence. Information in the computer is original and the copies made are secondary evidence.A three-judge bench of the Hon'ble Supreme Court upheld the ruling in Anwar PV's case. This decision has settled the issues that arose as a consequence of the various inconsistent rulings, establishing a standard for the techniques utilized in Trial Courts when it comes to the admission of electronic evidence. The court's legal interpretation of Sections 22A, 45A, 59, 65A, and 65B[31]of the Evidence Act has confirmed that recorded data on a CD/DVD/Pen Drive is not admissible without a certificate under Section 65 B(4) of the Evidence Act[32], and that in the absence of such a certificate, oral evidence to prove the existence of such electronic evidence and expert opinion under

[21]*State v. Navjot Sandhu*,2005 SCC 16 208.
[22]Indian Evidence Act,s.65B(4),1872 [India]
[23]*Anvar v. P.K.Basheer*(2015) 10 SCC 473
[24]Indian Evidence Act,s.65B(4),1872 [India]
[25]*Amar v. State of Haryana* (2017) 8 SCC 746.
[26]Indian Evidence Act,s.65B(4),1872 [India]
[27]*Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801
[28]Indian Evidence Act,s.65B(4),1872 [India]
[29]Ibid
[30]Arjun PanditraoKotkar v. Kailash KishanraoKotkar, Para 21, Part IV JLJ pg. 193 (2020).
[31]Indian Evidence Act,s.22A, 45A,59,65A,and 65B,1872 [India]
[32]Indian Evidence Act,s.65B(4),1872 [India]

Section 45A of the Evidence Act cannot be used to prove the authenticity thereof. This is the latest interpretation of the relevant provisions.

DIGITAL FORENSICS:

Digital forensics is the practice of detecting, collecting, and evaluating electronic evidence. Today, practically all criminal activity involves digital forensics, and digital forensics professionals play an important role in police investigations. Digital forensic data is frequently utilized in judicial procedures. The study of suspected cyberattacks is a critical component of digital forensics, with the goal of discovering, mitigating, and eliminating cyber risks. This makes digital forensics an essential component of the incident response process. Digital forensics is also important in the wake of an attack, providing information needed by auditors, legal teams, or law enforcement. Electronic evidence may be obtained from a multitude of sources, including computers, mobile devices, remote storage devices, the internet of Things, devices, and almost any other computerized network. Digital evidence has a broader scope, might be more personally highly sensitive, is mobile, and necessitates training and tools that differ from tangible evidence.

In the case of ***Darshan T S v. State of Karnataka***, the High Court of Karnataka ruled that investigating a criminal case is not a simple or routine task; it needs vast professionalism, that is only possible through proper training. It was pointed out that a lot of crimes have become high-tech, in the sense that mobile phones and electronic gadgets are used to plan conspiracies, and communications are conveyed by SMS and e-mail. Many cases rely heavily on digital evidence. Seizures of hard disks, collecting of call information, and other digital documents need extensive expertise in Digital Forensics. Sections 65-A and B of the Indian Evidence Act, of 1872,[33] provide that proof of such digital evidence must be tighter. The standards for demonstrating digital evidence are made more stringent.

EMERGING ISSUE – AI IN ELECTRONIC EVIDENCE:

As artificial intelligence (AI) becomes more prevalent in many sectors of society, its use in criminal, civil, and other investigations will expand. However, unlike in other applications, the use of AI in digital forensics requires various considerations before being accepted in judicial proceedings. These issues emerge from the seriousness of the questions being addressed by AI in digital forensics, which have the potential to impact people's liberty, livelihoods, and money. It is critical that any AI used in digital

[33]Indian Evidence Act,s.65A and 65B,1872 [India]

evidence analysis be treated with the same rigor as other types of forensic evidence. Implementation of AI techniques designed without regard for legal admissibility has the potential for terrible consequences, whether evidence is judged inadmissible or, worse, erroneously evaluated. In this digital era soon AI will be brought up as digital evidence under the purview of the Evidence Act. Provisions are to be interpreted as inclusive of the recent changes in the digital world. It has to be interpreted according to golden rule to adapt to the recent and upcoming developments.

EXPERT TESTIMONY:

Electronic evidence, also known as electronic form of evidence, refers to any information of proof value that is kept or transferred in digital form, such as computer evidence, digital audio, digital video, cell phones, and digital fax machines. If the concerned Court develops an opinion on an issue pertaining to computerized information or information in electronic or digital form, the opinion of an expert examiner of electronic evidence could potentially be deemed to be significant. Furthermore, in order to provide expert opinion on electronic form evidence before any court or another authority, the Central Government must designate any department, entity, or body of the Central Government or a State Government as the Examiner of Digital Evidence. A special provision for the examination of electronic evidence is inserted as section 45A of the Indian Evidence Act in accordance with the Information Technology(Amendment) Act 2008.[34]

Section 45A provides that when in a court proceeding there is a requirement for an opinion on any matter relating to information transmitted or stored in any computer resource or any other form of electronic or digital evidence, the opinion of the examiner of electronic evidence is referred under section 79A of the Information Technology Act 2000[35]is relevant. For the purposes of this provision, an Examiner of Electronic Evidence is an expert. This expert evidence has to be given strict interpretation because the purpose of this expert evidence through an examiner of electronic evidence who is specialized and trained in that field is to test or examine the originality of the produced electronic or digital evidence.

NEW DIMENSION:

The **Bhartiya SakshyaAdhiniyam**is considered to be the new evidence law and implemented in the year of 2023. It repealed and made changes, adding new provisions in the evidence act, 1873. The **section 2(1)(e)** of the BSA defines the electronic evidence as “any information of probative value that is stored,

[34]Indian Evidence Act,s.45A,1872 [India]
[35]Information Technology Act, s.79A, 2000 [India]

transmitted, or received in an electronic form, including, but not limited to any other form of electronic data." The **section 62 and 63** of the BSA, 2023 dealt with the electronic evidence:

1. The scope of the term of "document" as it includes the **electronic and digital records.**
2. The ambit of evidence also included the "information given electronically".
3. It is considered to be the **primary evidence under the section 57 of the Act.**
4. **The section 61 and section 63** provides the admissibility of the electronic evidence.

SUGGESTIONS:

1. In accordance with the changing circumstances digital evidence or electronic evidence has to be admitted as primary evidence.
2. As society is subject to change golden rule of interpretation has to be used instead of the literal rule of interpretation due to the reason there is no exhaustive definition of electronic evidence.
3. Strict interpretation has to be given for the procedural aspects relating to Electronic Evidence.

CONCLUSION:

It is vital to understand the methods employed by law enforcement departments and the challenges they encounter when working with electronic evidence. Many police officers are unclear on how to conduct a competent search in a computerized environment, particularly in a networked ecosystem. As a result, they miss important information and hints. As a result, perpetrators are acquitted, undermining the primary objective of the criminal justice system. Every crime scene involving computer-based evidence has its unique set of challenges, and digital investigators must be able to use forensic science concepts in innovative ways.Consistency is necessary for preventing inadmissibility owing to flaws non the evidence-gathering and management processes. This also ensures that the most effective accessible collection and storage procedures are employed, enhancing the possibility that two forensic examiners would reach the same findings when examining the evidence.

REFERENCE:

Bibliography:

1. Dr. S. R. Myneni, Law of Evidence, 205-210 (Asia Law House, 3rd edition, Hyderabad)
2. Suresh T. Viswanathan, The Indian Cyber law with the Information Technology Act,2000 (Aggarwal law house, New Delhi)
3. Dr.V. Krishnamachari, Law of Evidence, 476- 487(Narender Gogia & Company, Hyderabad)

4. B.M. Gandhi, Interpretation of Statutes, 19-69(Eastern Book Company, Lucknow)
5. Justice G.P.Singh, Principles of Statutory Interpretation,47-102 (LexisNexis, Haryana)

Webliography:

1. https://student.manupatra.com/Academic/Abk/Law-of-Evidence/chapter5.htm#:~:text=The%20electronic%20evidence%20or%20the,and%20the%20digital%20fax%20machines
2. https://articles.manupatra.com/article-details/ADMISSIBILITY-OF-ELECTRONIC-EVIDENCE-UNDER-THE-INDIAN-EVIDENCE-ACT-1872
3. https://www.scconline.in
4. https://www.legalserviceindia.in
5. https://www.lexisnexis.com