

# Admissibility of Electronic Record under Section 65B of The Indian Evidence Act Vis-à-vis Judicial Interpretation

Swaroop S. Sonone<sup>1</sup>, Rahul K. Gawade<sup>2\*</sup>, Damodar M. Hake<sup>3</sup>, Nikhil V. Rathod<sup>4</sup>

<sup>1</sup>School of Forensic Science, JSPM University Pune- 412207, Maharashtra, India

<sup>2</sup>Department of Law, Government Institute of Forensic Science, Chhatrapati Sambhajanagar- 431004, Maharashtra, India

<sup>3</sup>Maharashtra National Law University Mumbai- 400076, Maharashtra, India

<sup>4</sup>Department of Forensic Science, Dr. Babasaheb Ambedkar Marathwada University, Chhatrapati Sambhajanagar – 431004, Maharashtra, India

## ARTICLE INFO

### Article History:

Accepted: 26 Jan 2024

Published: 29 Feb 2024

### Publication Issue :

Volume 11, Issue 16

Jan-Feb-2024

### Page Number :

36-41

## ABSTRACT

In the digital era, persons are interconnected through gadgets, vivid technologies, and internet connections. Digital platforms have been proved as a boon but have given birth to various challenges in the form of vulnerabilities, attacks, and cybercrimes. From time to time, the law has impacted society and society has been impacting law. Until the Information Technology Act, 2000 was introduced; digital data, gadgets, or electronic evidence were not admissible as evidence in India. IT Act made several changes with respect to 'Admissibility of Electronic Evidence' in the Indian Evidence Act, 1872. The rampant use of technology has given birth to new laws and regulations and the Apex Court of the land interprets the same from time to time. One such meaningful interpretation is regarding the 'Admissibility of Electronic Records' under Section 65B of the Indian Evidence Act, 1872. Deficiency of simplified interpretations through judiciary on 'Certificate of Authentication' has posed many doubts on the varied electronic evidence viz., Emails, CCTV footages, CDs/DVDs, USBs. This paper focuses on the admissibility of digital evidence in the court of law and presents detailed insight on the relevancy/irrelevancy of the 'Certificate of Authentication.'

**Keywords** - Certificate of Authentication, Digital Evidence, Cybercrimes, IT Act-2000, Judiciary, Justice.

## I. INTRODUCTION

Technological expansions have profited the world by offering many luxuries and comforts of life and also offered newer extents to human abilities and human actions in the modern world. Technology has never been that easy as is today. Its credit goes to convenient digital/electronic inventions. With the arrival of globalisation and the rise in the digitization of everything, a major variation in modes & methods of intercommunication among businesses was observed in last few years. In 1996, The United Nations Commission on International Trade Law (UNCITRAL), by the means of Model Law on Electronic Commerce (MLEC), introduced a set of globally justifiable rules to eliminate lawful difficulties and increase legal expectedness for e-commerce. This enhanced the efficacy in worldwide trade by offering common action to paper-based & electronic data, consequently allowing the usage of paperless statements. MLECaimed at cheering lawmakers to accept a set of universally admissible rules managing electronic commerce. MLEC escorted a guide that gives framework and descriptive guidelines to support the states in making the essential jurisdictive provisions. Digital/electronic evidence, being least appraised, based on significance and credibility are now one of the most important key elements in proving or disproving the case.

The Indian Information Technology Act-2000 (hereinafter referred to as IT Act, 2000) provides lawful admission to digital signatures and electronic records. Prior to this Act, electronic records & digital evidence were not considered vital pieces of evidence. The Indian IT Amendment Act, 2008 provides the admissibility of evidence produced through communication devices. Common digital evidence on the crime scene are CDs, DVDs, Pendrive, Memory Cards, CCTV footages, Mobile handsets, and Cameras. Electronic evidence like social network communications, website information, E-mails, computer-generated documents and even SMS/MMS,

pose distinct problems and challenge for appropriate validation and are subjected to a diverse set of interpretations. These days, Pendrive and USBs are some of most common means for transferring digital data. Throughout the courtroom proceeding, Judges are frequently requested to instruct on the admissibility of electronic evidence and it significantly influences the results of civil law cases or conviction/acquittal of an accused. Court of law endures to wrestle with this new electronic edge as the specific behaviour of electronic evidence, whether it's fake or fabricated, creates difficulty to admissibility not confronted with the rest of the evidence.

Digital evidence is used not only in cybercrimes but also useful to solve other crimes. As the applicability of the IT Act and succeeding amendments to the Indian Evidence Act (hereinafter referred to as IEA, 1872), the usage of electronic records in trials/suits in the courts of law has come a long way. Due to the application of Section-92 of IT Act 2000, various laws were amended which includes IEA-1872. This includes: The phrase under section 3 of the IEA, 1872 "*All documents produced for the inspection of the Court*" were substituted by "*All documents including electronic records produced for the inspection of the Court*". Regarding the documentary evidence, in Section 59, for the words "Content of documents" the words "Content of documents or electronic records" have been substituted and Section 65A & 65B were inserted to incorporate the admissibility of electronic evidence. However, in spite of numerous legal precedents emphasising the significance of the 'Certificate of Authentication', the journey of the 'Certificate of Authentication' has developed a confused state for lawmakers.

### **Admissibility of Electronic Records**

Electronic information is very easy to produce, duplicate, modify, terminate, and transfer from one platform to another. In short, by their very nature, electronic records can be easily manipulated. Consequently, their accuracy and trustworthiness are

often suspected. This creates a conflict between the applicability and acceptability of digital evidence, something that has been recognized by authorities across the globe. The rule concerning to the admissibility of evidence in India is dealt under the IEA, 1872. According to Section 65B of the IEA, 1872, ‘Any information contained in an electronic record whether printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer is to be considered as a document, if the conditions mentioned in this section are satisfied then the evidence will be admissible in the court of law.’ Section 65B states –“For the purpose of admissibility of evidence, a certification shall have the following matters as necessary: (a) identifying the relevant electronic records relating to the certificate and describing the manner in which it was produced, (b) details of the device producing it, (c) satisfying the conditions of 65B (2) i.e., the computer from which the output was produced was used regularly to store or process information during its regular course of activities and (d) throughout the material part of the said period, the computer was operating properly”. Certification of matters is to be stated to the best of the knowledge and belief of the person signing the certificate i.e., the officer in charge of the operation or management of the related activities.

The Supreme court of Nigeria in the case of *Esso West Africa Inc. v.T. Oyegbola* observed that “The law cannot be and is not ignorant of modern business methods and must not shut its eyes to the mysteries of the computer.” According to Section 2 (t) of the Indian IT Act, 2000, Electronic Record means “Data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer-generated microfiche”. It fundamentally means electronic records can be referred to as such data or image or sound or anything which can be either sent or received in the electronic medium. Digital evidence contains the data that is kept or communicated digitally. Electronic evidence is secondary evidence. Sec. 3 of IT Act, 2000 i.e., the

meaning of authentication of the electronic record states that it is compulsory to affix a digital signature so that an electronic record produces the identical hash value every time a particular algorithm is implemented. This is done so that individuals are not able to replicate original evidence and form duplicated or falsified evidence. Electronic records can vary from Pendrive (PDs) to Compact Discs (CDs). It consists of E-Mails, computer generated documents, databases, digital spreadsheets, images, etc. Any data documented by a computer that is produced or received is labelled under an electronic record. There are different interpretations of different countries with respect to the digital evidence and its admissibility in their courts.

In Malaysia, Sections 90A, 90B, and 90C of the Malaysian Evidence Act, 1950 provide the rules which are responsible for admissibility of electronic evidence in the court of law. Over the dispute of verification of electronic evidence, section 90A (2) of the Malaysian Evidence Act 1950 demands the presentation of a certificate from an individual accountable for the tasks related to the computers. Failure to submit certificate regarding computer generated evidence may result in rejection of the evidence for authenticity failure. While in United Kingdom (UK), electronic evidence is accepted at both criminal and civil trials. For civil cases, the Civil Evidence Act, 1995 was approved which provided the admissibility of electronic evidence, the authentication of certain documents, and proof of official actuarial tables in civil proceedings. Computer generated documents are acceptable as an evidence under Sec. 3 of the Civil Evidence Act. Similarly, in the United States (US), prior admitting the digital evidence, it shall be certified i.e., the supporter of the evidence must make sufficient findings to support the genuineness of an evidence.

#### **Admissibility of Social Media Evidence**

The time of two decades is already elapsed after the passing of the IT Act-2000, the laws on digital evidences are still in its infancy. It is noticed that

social media chats, communications over any of the social media or IM (Instant Messaging) platforms for that case, etc. are still presented in the form of printouts of actual conversations. Such exercises take the social media chats beyond the scope of Sec. 62 of the IEA and thus can't be considered as primary evidence and hence, treated as secondary evidence. Social media platforms like WhatsApp, Instagram, Facebook, Twitter, Telegram, etc. play an important role in present times as the most common ways of online communications. The subsidiary role of social media evidence, considered through judiciary is a hindrance for speedy disposal matters. There requires a strong judicial mindset to prioritise them, which can be considered as effective utilization of technology because the very aim of technology was to reduce the time, human intervention, etc. These evidences have a potential to shift the burden of proof from one party to another.

#### **Admissibility of Electronic Evidences: An Indian Approach**

As the exposure to electronic records has increased the evidentiary value of digital evidence, there has been a transition from a time of treating 'Electronic Records' as normal documents to treating them as important pieces of evidence. Unfortunately, it is observed that the legal system does not always keep up with the pace of technological advancements. The court system believes that evidence is acceptable as far as any of the evidence is appropriate. The court must practise judicious options at the time of verdict of the case. Simply accepting evidence does not prove any fact in itself.

Over the years, it has been observed that the Indian judiciary shows the 'difference of opinions' in the interpretation of laws. A judgment may vary as per the difference of opinion between/among judges. The differences in the admissibility/ inadmissibility can be observed from the following cases -

In the case of *State (NCT of Delhi) v. Navjot Sandhu*, it was observed that, although the certificate with the details mentioned in Section 65B has not been issued,

secondary evidence may be provided if the provisions under Sections 63 and under 65 of the Indian Evidence Act are complied with.

Whereas an overruling judgment was pronounced by the Hon'ble Supreme court through *Anvar P.V v. P.K Basheer*. The court held that the electronic records will not be admissible as an evidence by way of secondary evidence unless the requirements under Section 65B have been met. As Sec 65A and Sec 65B are special provisions, they have precedence over general law (*Generalia specialibus non derogant*).

The subsequent judgment of *Sanjaysinh Ramrao Chavan v. Dattatray Gulabrao Phalke & Ors* provided that without the source, there is no truth to the translation. Sources and veracity are the two main reasons for accepting electronic evidence in a court of law.

In the case of *Abdul Rahaman Kunji v. State of West Bengal*, the High Court of Calcutta, while determining the eligibility of emails, had said that - an email sent by downloading an email from a person's email account can be proved by Sec. 65B r/w Sec 88A. The court also held that the testimony of witnesses was sufficient to prove the communication in order to carry out such a process for downloading and printing the conversation.

In *Girwar Singh v. CBI* the court directed that the electronic evidence is inadmissible in the court of justice because the electronic record was moved into two new cassettes and the original recording was deleted and was not brought in the eyes of the court for a very long duration. The court stated that the applicability of Section 65B is present only if the original evidence is produced.

In the case of *Vikram v. State of Punjab* the court noted that the tape-recorded conversation in the present case was kept as primary evidence, not secondary evidence which required certification under Sec 65 B of the IEA, 1872. It also gave reference to the *Anvar case* by saying that Electronic evidence is used as primary evidence to be admissible as evidence, without complying with the terms of Section 65B.

Also, in the case of *Sonu v. State of Haryana* the court held that a call data record (CDR) without any certificate under section 65B was not congenitally unacceptable. The method of such authentication is related to the method of taking evidence and objections and should be raised as soon as possible. The judge in the present case recommended that the appropriate bench consider this in the future. But, despite knowing that their hands were tied, the two judges rejected the appeal by refusing to apply the law in the *Anwar case*.

In the famous *Shafhi Mohammad V. State of U. P.* the court ruled that the need to obtain a certificate of judicial process could be easily met by a court where the interests of justice are preferred. For example, the procedure required under section 65B of the IEA-1872 for shop bills, electronic tickets, etc., applies only when electronic evidence is submitted by a person in a position to issue such a certificate, that is under the control of the device. When the party does not have such a device, the applicability of sections 63, 63 and 65 of the IEA-1872 cannot be omitted from the application.

In contrast to the above verdict, *State of Karnataka Lokayukta Police Station, Bengaluru v. R. Hiremath* the Supreme Court has ruled that a certificate under Section 65B can be issued after the chargesheet has been filed, which is required to be produced when an electronic record is required to be submitted as evidence at the time of trial.

From the decisions of the above cases, one may go with a 'confused state of mind' concerning the admissibility of electronic evidence and exact need for a certificate of authentication before the court proceeding.

### **Certificate of Authentication – An Obstacle to Speedy Trial?**

Day-by-day, Judiciary is highly burdened due to the rapid increase in the rate of crimes. National Crime Record Bureau (NCRB) report of 2018-19 shows that the crime rate registered per lakh population has increased marginally from 383.5 in 2018 to 385.5 in

2019. Specifically, Crime rate under the cybercrimes category increased from 2.0 in 2018 to 3.3 in 2019 per lakh population. As per the Law Ministry of India records, there is just one judge per 50,000 citizens as against the recommended number of one per 20,000 in the year 2019. This results in the delaying of judgments. In recent times, with the increase of digital devices, it's one of the most difficult tasks to verify each digital evidence present on a crime scene. Preparation of certificate after authentication of each digital device present on the scene is not a good option in every matter. One can lose the crucial/credible information stored on the volatile storage devices due to delay in response to these devices as well as delaying in verification and authentication e.g., data stored on RAM. Digital evidences or gadgets are genuine unless altered or modified. The court should consider that; such evidence may change the order from acquittal to conviction and vice versa. It should also consider the perspective of an expert while admitting evidence. Delay in the presentation of 'Certificate of authentication' is one of the reasons, ultimately leads to a bunch of confusions. The law on electronic evidence under the IT Act 2000 is still in its infancy and is expected to make significant progress in the near future.

## **II. CONCLUSION**

Law must change as per the needs of changing demands of society. Unfortunately, lack of political will from lawmakers, undue execution through executors, and many times, discretion-based interpretation through judiciary is the reason behind many problems. Because discretion may lead to arbitrariness. Recent Indian pronouncements on the admissibility of electronic evidence stress on the requirement of the 'Certificate of Authentication' and non-adherence is violative to section 65B of the Indian Evidence Act. The Hon'ble Supreme Court's verdicts on the admissibility of electronic evidence

evoke mixed feelings. One may say, that it wilfully disregards Section 65B of IEA, by ignoring and wilfully reading with statutory requirements as it sees fit. But, the implementation of time-consuming procedures may lead to injustice. A proper and judicious explanation to the admittance or rejection of electronic evidence is the need of the day and should be reflected through the judgments of the apex court of the land.

### III. REFERENCES

- [1]. Garg, A. Model Law on Electronic Commerce, Accessed on [20/02/2024] Available at: <https://blog.ipleaders.in/model-law-on-electronic-commerce/>
- [2]. Kumar, S. (2015). Digital Evidence–Technical Issues. *Advances in Computer Science and Information Technology (ACSIT)*, 2(11), 42-47.
- [3]. Aarora, N. Admissibility of Electronic Evidence: Challenges for Legal Fraternity, Accessed on [14/2/2024] Available at: [https://cyberpandit.org/?article\\_post=admissibility-of-electronic-evidence-challenges-for-legal-fraternity](https://cyberpandit.org/?article_post=admissibility-of-electronic-evidence-challenges-for-legal-fraternity)
- [4]. Vaidialingam, A. (2015). Authenticating Electronic Evidence: Sec. 65B, Indian Evidence Act, 1872. *NUJS L. Rev.*, 8, 43.
- [5]. Section 65B of the Indian Evidence Act, 1872.
- [6]. (1969) 1 N.M.L.R. 194 at 198.
- [7]. Section 2(t) of the Information Technology Act, 2000.
- [8]. Section 3 of the Information Technology Act, 2000.
- [9]. The Commissioner of Law Revision, Malaysia, Evidence Act 1950 (Revised 1971), Accessed on [16/2/2021], Available at: [http://www.commonlii.org/my/legis/consol\\_act/ea19501971155/](http://www.commonlii.org/my/legis/consol_act/ea19501971155/)
- [10]. Mohamad, A. M. (2019). Admissibility and authenticity of electronic evidence in the courts of Malaysia and United Kingdom. *Int J Law Gov Commun*, 4(15), 121-129. {Citation}
- [11]. Rule 901 of Federal Rules of Evidence, 2020.
- [12]. Akiwate, S. Admissibility of WhatsApp Chats in a Court of Law, Accessed on [28/2/2021] Available at: <https://cyberblogindia.in/admissibility-of-whatsapp-chats-in-court-law/>
- [13]. Singh, R. R. WhatsApp Chats as Evidence in Court- Admissible or Not? Accessed on [2/3/2021] Available at: <https://lawtrend.in/whatsapp-chats-as-evidence-in-court-admissible-or-not/>
- [14]. Shairwal, S. Right to privacy and admissibility of evidence, Accessed on [14/2/2021] Available at: <https://www.lexology.com/library/detail.aspx?g=43191c48-aabb-451c-99ec-46d3dff6e99d>
- [15]. (2005) 11 SCC 600.
- [16]. (2014) 10 SCC 473.
- [17]. (2015) 3 SCC 123.
- [18]. (2016) CLRJ 1159.
- [19]. (2016) 5 RCR (Cri) 757.
- [20]. (2017) 8 SCC 5180.
- [21]. (2017) 8 SCC 570.
- [22]. (2018) 1 SCC (Cri) 860.
- [23]. (2019) SCC 734.
- [24]. Crime in India–2019, Accessed on [4/3/2021] Available at: <https://ncrb.gov.in/sites/default/files/CII%202019%20SNAPSHOTS%20STATES.pdf>
- [25]. Menon, R. India Justice Report Shows Legal System Needs Urgent Attention, Accessed on [2/3/2021] Available at: <https://www.theleaflet.in/india-justice-report-shows-legal-system-needs-urgent-attention/>
- [26]. Kalaskar, K. D. Admissibility of E-evidence; Are WhatsApp chats and E-mails admissible in Court? Accessed on [2/3/2021] Available at: <http://www.legalserviceindia.com/legal/article-4632-admissibility-of-e-evidence-are-whatsapp-chats-and-e-mails-admissible-in-court-.html>