

**INTERNATIONAL JOURNAL OF LAW**  
**MANAGEMENT & HUMANITIES**

**[ISSN 2581-5369]**

---

**Volume 4 | Issue 3**

---

**2021**

© 2021 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com>)

---

This Article is brought to you for “free” and “open access” by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in International Journal of Law Management & Humanities after due review.

In case of **any suggestion or complaint**, please contact [Gyan@vidhiaagaz.com](mailto:Gyan@vidhiaagaz.com).

---

**To submit your Manuscript** for Publication at **International Journal of Law Management & Humanities**, kindly email your Manuscript at [submission@ijlmh.com](mailto:submission@ijlmh.com).

---

# Admissibility of Digital Evidence in Cyberspace

---

SAKSHI NATHANI<sup>1</sup> AND PRATIKSHA GAUTAM<sup>2</sup>

## ABSTRACT

*The emergence of Digitalization an advancement of technology gave birth to the introduction of Information Technology Act and the role of electronic evidences in the cyberspace. The present paper provides the in-depth analysis of electronic evidences and its importance in the era of digitalization. The increasing dependency on electronic gadgets caused a need to transform the law relating to information technology, cyber law and ruled of admissibility of electronic evidences both under the civil and criminal cases. Thus, the paper discussed the provisions incorporated under the Indian Evidence Act and IT Act dealing with meaning of cyber forensic, electronic records, electronic evidences and role of controller to authorize the validity of digital signature. The paper further deals with the amendments brought by IT Act under Second Schedule to modify and amend the existing meaning and definition of Evidence under the Evidence Act, the inclusion of various provisions relating to 'electronic records' under Indian Evidence Act are contained in sections 17, 22A, 39, 45A, 59, 65A and 65B. Out of which sections 65A and 65B is most important as it provided the rules relating to admissibility of electronic records as evidence. In the later part of the paper, the question regarding the admissibility of electronic evidence without certificate is also discussed with the followed precedents and recent judgments. At the end, the paper discusses various case laws, the intention of Indian Judiciary to form and bring the amendment of Indian Evidence Act, and also how the digital evidence may led to some serious challenges to cybercrime committed widely and intensively.*

**Keywords-** *IT Act, Indian Evidence Act, electronic/digital evidences, admissibility of electronic evidence, cyber forensic, cybercrime.*

## I. INTRODUCTION

The creation and advancement of technology has given a new and ever changing face to the litigation. Human Civilization has, with passage of time, made tremendous progress and consequently resulted in various inventions and discoveries. One of the greatest inventions of mankind is the development of personal computers and internet which led to the development

---

<sup>1</sup> Author is a student at Alliance University, School of Law, Bangalore, India.

<sup>2</sup> Author is a student at Alliance University, School of Law, Bangalore, India.

of cyberspace. The evolution made by humans in cyberspace had led various changes because of its diversity of contents, information, posts, pictures, opinions, ease accessibility and wide reach, and pose several dangers to the society<sup>3</sup>. This paper seeks to examine one of the most important legal issues in cyber forensics, i.e. the admissibility of digital evidences in India. The art and science of applying computer science to collect digital evidence has emerged as an important aid to criminal prosecution of cyber-crimes.

The United Nations Commission on international Trade (UNCITRAL) adopted, in June 1996, a Model law on e-commerce, intended to give States a legislative framework to remove barriers in e-commerce sector. Similarly, the Information Technology Act, 2000 was based on the UNCITRAL Model Law, which facilitates the regulatory mechanism in respect of the issues relating thereto. The enactment of the legislation helped in dealing with issues relating to cyber space. The act in addition to the substantive law has made incidental and consequential changes in the Indian Penal Code, The Indian Evidence Act, the Banker's Book Evidence Act and Reserve Bank of India Act etc.<sup>4</sup> The amendment also brought a vast change in the interpretation and acceptance of electronic evidence in the court of law. The introduction of Section 65-A and 65-B in the Indian Evidence Act, 1872 provides the validity to the digital evidences and valid authenticity to the electronic records produced as an evidence. This massive change helped the contesting parties to produce the evidence not only in documents or by way of oral evidence but also includes electronic evidence that may be considered as primary evidence even conditions prescribed under Section 65-B of the Evidence Act are satisfied and fulfilled.

## II. PROVISIONS RELATING TO ADMISSIBILITY OF ELECTRONIC EVIDENCES

### (A) Meaning of Electronic Evidences

As per the explanation to Section 79A of the IT Act,<sup>5</sup> 'electronic form of evidence' means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, cell phones, digital fax machines. Courts can thus permit the use of digital evidence such as e-mails, digital photographs, word processing documents, instant message histories, spread sheets, internet browser histories, data bases, content of computer memory, computer backup, cloud stored data, secured electronic records

---

<sup>3</sup> Aneesh V Pillai, *ADMISSIBILITY OF DIGITAL EVIDENCES: AN OVERVIEW OF THE LEGISLATIVE AND JUDICIAL PERSPECTIVES* (April 24, 2021, 10.00pm) [https://www.researchgate.net/publication/340738664\\_ADMISSIBILITY\\_OF\\_DIGITAL\\_EVIDENCES\\_AN\\_OVERVIEW\\_OF\\_THE\\_LEGISLATIVE\\_AND\\_JUDICIAL\\_PERSPECTIVES](https://www.researchgate.net/publication/340738664_ADMISSIBILITY_OF_DIGITAL_EVIDENCES_AN_OVERVIEW_OF_THE_LEGISLATIVE_AND_JUDICIAL_PERSPECTIVES)

<sup>4</sup> Ghanshyam Singh, *Cyber Space and the Law-Issues and Challenges*, 1st Edn. NALSAR Law Review Sept 2004, at 299.

<sup>5</sup> The Information Technology Act, 2002, s.79A.

and secured electronic signatures. In simple word, electronic evidences means data comprising the output of analogue devices or data in digital form that is manipulated, stored and communicated by any ma-made devices, computer or transmitted over any communication system, that may help to make factual records of evidences.<sup>6</sup>

### **(B) Cyber Forensics and Digital Evidences**

Computer Forensics is a branch of forensic science pertaining to legal evidence found in computers and digital storage mediums. Computer forensics is also known as digital forensic. The goal of computer forensics is to explain the current state of digital artifact. The term digital artifact can include: A computer storage medium like hard disk or CD-ROM, or an electronic document like email message and JPEG image or sequence of packets moving over a computer network. Continue from chapter. Thus, the cyber forensic is the application of investigative techniques in the automated environment and the search, discovery, and analysis of potential evidence. It is method used to investigate and analyze data maintained on electronic form for the purpose of presentation of case involving digital evidences. The term digital evidences means any information or data of value to an investigation that is stored on, received by, or transmitted by an electronic device. It can include where the evidences obtained by analyzing data retrieved from digital media or the data which have been deleted but are still possible to be recovered using certain tools and technology.<sup>7</sup>

### **(C) Admissibility of Electronic Evidences**

The law relating to admissibility of evidence in India is dealt under Indian Evidence Act, 1872. The word ‘admission’ has a technical meaning in law and it has been defined in Sections 17, 18, 19 and 20 of the Evidence Act. Section 17 lays down that ‘An admission is a statement, oral or documentary or contained in electronic form, which suggest any inference as to any fact in issue or relevant fact, and which is made by any of the persons, and under the circumstances, hereinafter mentioned in Sections 18-20. Thus, before the introduction of Information Technology Act, 2000, the digital evidences collected through all means including through cyber forensics was considered as a document and secondary evidence of these electronic ‘document’ was adduced through printed reproductions or transcript, he authenticity of which was certified by competent signatory. He signatory would identify his signature in court and be open for cross examination. Analyzing the case of Anver P.K. v. P.K. Basheer & Ors. Case,

---

<sup>6</sup> A. Venkateswara Rao, *Admissibility of Digital Evidences*, WEBINOR (April 25, 2021, 11.00 AM) [https://districts.ecourts.gov.in/sites/default/files/Webinar on Admissibility of Electronic Evidence By Sri A Venkateshwara Rao.pdf](https://districts.ecourts.gov.in/sites/default/files/Webinar%20on%20Admissibility%20of%20Electronic%20Evidence%20By%20Sri%20A%20Venkateshwara%20Rao.pdf)

<sup>7</sup> Diaz, “*Computer Forensics*”, Uppsala University 8th October 2007 (April 25, 2021, 9.00PM) <https://www.it.uu.se/edu/course/homepage/sakdat/ht07/pm/programme/Forensics.pdf>

the Supreme Court has noted that ‘there is revolution in the way that evidence is produced before the court.’ As the pace and proliferation of technology is expanded, and the creation and storage of electronic information is constantly changing, there exist a need to change and modify the laws substantially and systematically.

The enactment of IT Act along with the massive amendments in Indian Evidence Act and Indian Penal Code has introduced the concept of ‘evidence record’ and declared it as an admissible evidence subject to certain conditions mentioned under Section 65B of the Evidence Act. The term ‘electronic record’ is defined under Section 2(t) of the IT Act, as ‘data, record or data generated, image or sound stored received or sent in electronic form or micro film or computer generated micro fiche’. Moreover, Section 6 of the IT Act the electronic records and electronic signatures can be used in Government and its agency. Thus, if there is any dispute regarding online contracts or e-crimes, then production of admissible evidence becomes necessary to decide the merits of the case.

### **1. Provisions under Indian Evidence Act, 1872 and Informational Technology Act, 2000**

Section 3 of the Evidence Act defines the term ‘document’ as any matter expressed or described upon any substance by means of letters, figure or marks, or by more than of those means mentioned, intended to be used, or which may be used, for the purpose of recording that matter falls under the meaning of Documents produced before court of law.<sup>8</sup>

In the advent of increasing digitalization and use of Technology across the country. The definition of ‘evidence’ has been amended to include electronic records. Thus, As per Section 3 of the Evidence Act, the term ‘*Evidences*’ means and includes-

- a) All statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence;
- b) All documents including electronic records produced for the inspection of the Court, such documents are called documentary evidences<sup>9</sup>.

Moreover, a new section 22-A has been inserted into Evidence Act, in order to provide for the relevancy of the oral evidence regarding the contents of electronic records. It provides that oral admissions regarding the contents of electronic records are not relevant unless the genuineness of the electronic records produced is in question. Also, the IT Act, amended Section 59 of the Evidence<sup>10</sup> to exclude electronic records from the probative force of oral evidence in the same

---

<sup>8</sup> The Indian Evidence Act, 1872, s.3.

<sup>9</sup> *ibid*

<sup>10</sup> The Information Technology Act, 2000, Second Schedule.

manner as it excluded documents. The electronic records cannot be proved by oral evidences.<sup>11</sup>

Section 45A of the Evidence Act is with regard to the opinion of the Examiner of Electronic Evidences, in cases where there exists electronic evidence or information stored or transmitted in digital form, the court may undertake the opinion of the Examiner of Electronic Evidence who shall be an expert referred to in section 79A of IT is considered as a relevant fact to manifest the case findings. Additionally, section 67A of the Evidence Act is deals with proof as to a digital signature and its thorough verification under Section 73A of the Evidence Act.<sup>12</sup>

## **2. SECTIONS 65- A and 65-B of the Evidence Act**

After the enactment of the IT Act, 2000, the legislature has amended and inserted two new evidentiary rules for ascertaining the electronic records validity and proof under the Evidence Act, namely sections 65-A and 65-B under Chapter V of the Act which deals with documentary evidences. The intention is to introduce the specific provisions which has its origin to the technical nature of the evidence particularly as the evidence in the electronic form that can be objected if sufficient genuineness is not proved.

### **(a) Position before and after adopting Section 65-A and 65-B**

Before the year 2000, courts used to adopt Sections 61 to 65 of the Evidence Act, while declaring the admissibility of electronic records which could be proved either by primary evidence or by secondary evidence. But in case where the original document/primary evidence is not available with the party who wants to adduce it as evidence or if it becomes impossible for a party to produce the original document, then it is absolutely compulsory to comply with Section 65 of the Act.

However, with the addition of Section 65 A and 65B, the legislature, by way of a deemed fiction, has made a computer output also a document/primary evidence, provided the conditions mentioned under section 65B of the Act are fulfilled.<sup>13</sup>

Section 65A expressly states that, ‘the contents of electronic records may be proved in accordance with the provisions of section 65B (1) states that, ‘if any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by computer shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question

---

<sup>11</sup> Bhima Tima Dhotre v. The Pioneer Chemical Co, (1967) 70 BOMLR 683.

<sup>12</sup> The Indian Evidence Act, 1872, s.73A.

<sup>13</sup> HARDHIK GAUTAM, *SECTIONS 65A AND 65B OF THE INDIAN EVIDENCE ACT: A COMPLETE CODE IN ITSELF*, BAR AND BENCH, 2020 (APRIL 28, 2021, 9.00 PM) [HTTPS://WWW.BARANDBENCH.COM/COLUMNS/SECTION-65A-AND-SECTION-65B-A-COMPLETE-CODE-IN-ITSELF](https://www.barandbench.com/columns/section-65a-and-section-65b-a-complete-code-in-itself)

and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible in any proceeding before the court of law'<sup>14</sup>. Thus, an electronic record printed on paper, stored, recorded or copied in optical or magnetic media produced by a computer is admissible as documentary evidence before the court of law if it satisfies the conditions, mentioned under 65B.

Section 65B provides for both technical condition and non-technical grounds. Thus, the list of technical conditions upon which a duplicate copy of an original electronic record may be used are as follows<sup>15</sup>-

- a. Firstly, the computer output containing the information should have been produced by the computer during the period over which the computer was used regularly to store or process information for the purpose of any activities regularly carried on over that period by the person having lawful control over the use of the computer.
- b. The second requirement is that it must be shown that during the said period the information of the kind contained is derived was 'regularly fed into the computer in the ordinary course of the said activity.'
- c. A third requirement is that during the material part of the said period, the computer was operating properly and that even it was not operating properly for some time that break did not affect either the record or the accuracy of its contents stored.
- d. The fourth requirement is that the information contained in the record should be a reproduction or derived from the information fed into the computer in the ordinary course of the said activity.

Further, the non-technical conditions are provided under Section 65-B (4) it provides for the requirement of a certificate which identifies the electronic record containing the statement and describes the manner in which it was produced giving the particulars of the device involved in the production of that record and deals with the conditions mentioned in Sections 65-B (2) and is signed by a person occupying a responsible official position in relation to the operation of the relevant device 'shall be evidence of any matter stated in the certificate'.<sup>16</sup> Thus, if any electronic record printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer, if duly proved in the manner stated in section 65-B, can be considered

---

<sup>14</sup> The Indian Evidence Act, 1872, s.65-B (1).

<sup>15</sup> The Indian Evidence Act, 1872, s.65-B (2).

<sup>16</sup> Karia T. D., AkhilAnand and BahaarDhawan, "*The Supreme Court of India re-defines admissibility of electronic evidence in India*", Digital Evidence and Electronic Signature Law Review 2015, (April 27, 2021, 4.00PM) <http://www.journals.sas.ac.uk/deeslr/article/download/2215/2149>.

as strong evidence for civil or criminal trial under Indian Evidence Act.

### **3. Admissibility of Electronic Evidence without certificate- Section 65-B (4)**

The question whether admissibility of electronic evidence without certificate under Section 65B of Evidence Act is maintainable or not? Was prominently interpreted by the Supreme Court recently, in case of *Arjun Panditrao Khotkar v. Kailash Kushanrao Goranyal*,<sup>17</sup> here the 3-judge bench of RF Nariman, S. Ravindra Bhat and V. Ramasubramanian, JJ held that the certificate required under Section 65-B (4) is a condition precedent to the admissibility of evidences by way of electronic record, as correctly held in by 3-judge bench in *Anvar P.V. v. P.K. Basheer*,<sup>18</sup> where court stated that, '*if an electronic record as such is used as primary evidence under Section 62 of the Evidence Act, the same is admissible in evidence without compliance with the conditions specified under Section 65-B of the Evidence Act.*' Also, court added that, '*Sections 65A and 65B being a complete code as to admissibility of electronic evidences, the 'baggage' of Primary and Secondary Evidence contained in Sections 62 and 65 of the Evidence Act should not at all be adverted to.*'

Later, indirectly the question was 'clarified' by a division bench in *Shafhi Mohammad v. State of Himachal Pradesh*<sup>19</sup>, where court held that the requirement of a certificate under Section 65-B(4), being procedural, can be relaxed by the Court whenever the interest of justice so justifies, and one circumstance in which the interest of justice so justifies would be where the electronic device is produced by a party who is not in possession of such device, as a result of which such party would not be in a position to secure the requisite certificate. Thus, the court further clarified that the required certificate under Section 65-B (4) is unnecessary if the original document itself is produced before the court.

#### **(D) Presumptions under Electronic Records**

Again the Indian Evidence Act, 1872 was amended on account of IT Act, 2000 and inserted provisions which creates presumptions regarding electronic records in different situations.

- i. Firstly, Section 81A, which contains presumption as to genuineness of every electronic record purporting to be the Official Gazette.
- ii. Secondly, Section 85A, which creates presumption that every electronic record purporting to be an agreement containing digital signatures of the parties was so concluded by affixing the digital signature of the parties.

---

<sup>17</sup> *Arjun Panditrao Khotkar v. Kailash Kushanrao Goranyal*, (2020) SC 571

<sup>18</sup> *Anvar P.V. v. P.K. Basheer*,(2014) 10 SCC 473

<sup>19</sup> *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.



- iii. Thirdly, Section 85B also creates a presumption of authenticity of secured digital signatures unless proven otherwise.
- iv. Fourthly, Section 85C provides a presumption of authenticity of secured DSC (Digital Signature Certificate) unless proven otherwise.
- v. Fifthly, Section 88A also creates a presumption as to the contents of electronic messages, but the originator of the electronic messages.
- vi. Finally, Section 90A creates a presumption as to the authenticity electronic records five years old, which is produced from the custody of a person.

### **(E) Challenges under the admissibility of Digital Evidences**

Although, the advancement of technology and digitalization is at increasing pace and requires unanimous acceptance. Still there exist the problem of valid admission and justified solution. In the era of globalization and technological world, where the primary requisite is to accept the dynamics of law, the parties litigating before the court of law must be aware of all advanced requirements of court for proving the electronic records. The process of accepting electronic evidences under section 65B is hostile but requires a strict interpretation in order to curb the most practiced cybercrimes like child pornography, online grooming, hacking, data theft etc.

The following are various challenges under the Cyber Forensics-

- Faulty case management through inadequate analysis and presentation of the digital evidences
- Incomplete and incorrect validation of the digital evidences
- Biases, examiner inexperience and pressures to process cases with limited time resources can also challenge the validity of electronic evidences
- Inadequate reasoning during analysis, compounded by poor presentation of even the basic facts, further degraded by inadequate validation of digital evidence.<sup>20</sup>
- Non-compliance with the prescribed provisions under the section and lack of acceptance due to unreasonable facts.

### **III. JUDICIAL APPROACH TO THE ADMISSIBILITY OF ELECTRONIC EVIDENCES**

In this digital era the cyberspace has made a tremendous progress, whether it is the internet or personal computers. These days it's very easy to spread information through internet it may be true or it may be misleading. Development of cyberspace has led to many dangerous

---

<sup>20</sup> Richard Boddington, *A Case Study of the Challenges of Cyber Forensics Analysis of Digital Evidence in a Child Pornography Trial Digital Evidence in a Child Pornography Trial*, ADFSL 2012, (May 2, 2021, 9:00 PM) <https://core.ac.uk/download/pdf/217157595.pdf>.

consequences; cybercrime today is one of the biggest challenges in many countries. Various cybercrimes have been exposed by many investigation agencies from different countries in last few years where the evidence derived from computers, internet and any other device. The word evidence is derived from the Latin word 'Evidentia' which means – the state of being evident or the definition of evidence is also defined under the section 3 of the Indian evidence act 1872<sup>21</sup>. Case laws-

### **(A) Admissibility of Digital Evidence in Indian Court**

The law which specifically deals with admissibility of evidence is mentioned under Indian evidence act, 1872. Before the introduction of IT act the digital evidences used to be collected through all means and cyber forensics used to verify them as relevant or not, but after the enactment of IT act in the year 2000 many amendments were also introduced in Indian evidence act and Indian Penal Code like the concept of electronic record. Now with the coming time the judiciary also started to recognize the relevance of electronic evidences rather than treating them as ordinary evidences in the case of *NCT of Delhi vs. Navjot Sandhu*<sup>22</sup>, SC held that irrespective of the compliance of the requirements of Section 65B which is a provision allocating with admissibility of electronic records, there is no bar to citing secondary evidence under the other provisions of the Evidence Act. But in another case of *Anvar P.V*<sup>23</sup> the SC recognized the importance of section 65B the Supreme Court observed that, *any documentary evidence by way of an electronic record under the Evidence Act, in view of Sections 59 and 65A, can be proved only in accordance with the procedure prescribed under Section 65B.*

Section 65B particularly deals with electronic record, the section is only admissible when the electronic record printed on a document generated by a computer fulfill the conditions mentioned under section 65B (2) of Indian Evidence act, 1872. In the case of *Abdul Rehman Kunji*<sup>24</sup>, the Calcutta high court apportioned the issue of e-mails as evidence, later the court said that the these mails will be considered as an evidence only if they satisfied the conditions mentioned under section 65B of Indian Evidence act, 1872. In the *Jagjit Singh case*<sup>25</sup> (2006), the speaker of the Legislative Assembly from the State of Haryana excluded a member for defection. While hearing the matter, the Supreme Court deliberated the digital evidence in the form of *interview transcripts* from the Zee News television channel, the AajTak television channel and the Haryana News of Punjab Today television channel. The Court held that, *the*

---

<sup>21</sup> Indian Evidence Act, 1872, § 3, Acts of Parliament, 1949 (India)

<sup>22</sup> NCT of Delhi v. Navjot Sandhu Alias Afzal Guru, (2005) 11 SCC 600

<sup>23</sup> Anvar P.V v. P.K Basheer and others, (2014) 10 SCC 473

<sup>24</sup> Abdul RahmanKunji v. State of West Bengal, 2004 C.R.A. Nos. 454 & 624

<sup>25</sup> Jagjit Singh v. State of Haryana, (2006) 11 SCC 1

*electronic evidence placed on record was admissible and upheld the reliance placed by the speaker on the recorded interview when reaching the conclusion that the voices recorded on the CD were those of the persons taking action''.* The electronic records are easy to tampered there must be some safeguards like integrity of data, to make sure the data collected is not tampered or the system which is used to access the electronic record must be secured. As these days it is very easy to tamper the evidence make it faulty. In the case of *Arjun Panditrao Khotkar*,<sup>26</sup> the apex court quoted some guidelines for the confusion among the admissibility of electronic evidences, that *the following Sections 22A, 45A, 59, 65A & 65B of the Evidence Act has confirmed that the stored data in CD/DVD/Pen Drive is not admissible without a certificate u/s 65 B(4) of Evidence Act and further clarified that in the absence of such a certificate, the oral evidence to prove the existence of such electronic evidence and the expert view under section 45A Evidence Act cannot be availed to prove authenticity thereof.*<sup>27</sup>

### **1. THE BOIS LOCKER ROOM CONTROVERSY**

In the recent events the case of bois locker room came to limelight where it was seen that some of the members of this group (mostly teenagers) shared obscene materials, morphed pictures of minor girls in the group. These teenage boys were planning rape and other acts of sexual attacks. Later the screenshots of the chats were posted on Instagram and exploded the social media, making a private group is not a crime but the incident is an offense under POSCO act, 2012. Here in this case the only evidence was those chats screenshots which were collected by Delhi police and they can be easily verified by cyber forensics. There are several presumptions like section 92 of the IT act made some amendments to Indian evidence act, 1872 and added some presumptions in regard to the electronic evidences. Presumption as to electronic messages: It includes emails, SMS, etc. of messages sent via social networking sites, like Whatsapp, Twitter etc. Under Section 88A of the IT Act, there is a presumption as to such messages, which allows the Court to assume that an electronic message forwarded by the instigator through an electronic mail server to the recipient to whom the message senses to be addressed resembles with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent. Till as of late, the Indian Evidence Act, 1872 didn't have explicit arrangements perceiving acceptability and enthusiasm for digital evidence. Significantly, it was not at standard with present day innovative turn of events. Subsequently, to perceive exchanges that are helped out through electronic information exchange and different methods for electronic correspondence, law was

---

<sup>26</sup> *Arjun Panditrao Khotkar v. Kailash Kushanrao Goranyal*, (2020) SC 571

<sup>27</sup> *Ibid*

needed to be corrected. As needs be, Information Technology Act, 2000 (Act 21 of 2000) came to be established. The IT Act depends on the UNCITRAL Model Law on Electronic Commerce. Aside from giving changes to Indian Evidence Act, 1872 (Evidence Act), the Indian Penal Code, 1860 and the Banker's Book Evidence Act, 1891, the IT Act primarily perceives the exchanges that are done through Electronic Data Interchange (implies, correspondence among computers) and other methods for correspondence. The introduction of IT Act and the comparing amendments Indian Evidence Act, 1872 have to set up a legitimate structure for the admissibility of digital evidence. Despite the fact that at first there was disarray in regards to the use of these new provisions while managing the issue of admissibility, the Indian judiciary particularly in the case of Anwar PV (2015) explained the law in regards to the admissibility of digital evidence in India. The ensuing choices of different high courts moreover explained the issue of various kinds of digital evidences. Consequently, the advanced confirmations or electronic records are permissible in India, in the event that it fulfills the conditions recommended by section 65B. In this manner the law identifying with acceptability of digital evidence is well indeed coagulated. Anyway one of the worries actually emerging is in situations where if a secondary electronic record is seized from the accused, the certification under 65B (4) normally could not be attained. Besides, because of the bar of self-incrimination under Article 20(3) of the Constitution of India, the accused can't be made a witness against himself. Consequently, in such circumstance the subject of acceptability such electronic record is in risk. It tends to be imagined that in future through judicial intervention, our legal executive may discover an answer for this situation too. With the sanctioning of the IT Act and the resulting Amendments in the Evidence Act, the utilization of electronics records in legal procedures has gone far. Nonetheless, regardless of different legal points of reference pushing on the significance of the certificate, the certificate has become a simple custom. With the necessity of an authentication under Section 65B of the Evidence Act being weakened by the decision of the Supreme Court *Shafhi Mohammed*, it is intriguing to perceive how the equivalent is explained by the Supreme Court. Indeed, even from there on, with the continuous development of the internet, it would be suitable that the courts stay aware of the progressions in the internet, to advance sureness in the utilization of such electronic records, while considering every single point in all aspects. Notwithstanding electronic records being driven in evidence, there has additionally been an expansion in dependence on electronic media for different purposes in legal procedures. While perceiving the upside of electronic media like messages, WhatsApp messages, and so on, the Supreme Court hosts energized gatherings/their promoters to serve the counter party through email, notwithstanding the standard methods of

service<sup>28</sup> in commercial case and prosecution wherein between time alleviation is appealed for. A comparable view has additionally been taken by the Hon'ble Bombay High Court<sup>29</sup>. In the recent occasions, even services through WhatsApp have been perceived by the Hon'ble Delhi High Court and the Hon'ble Bombay High Court<sup>30</sup>. Hence many things have been said regarding the admissibility of electronic evidences it would be better if the judiciary make this provision more flexible. The provisions made under Indian evidence act, 1872 are quite clear with the admissibility of electronic evidences and there are many cases which prove that the digital evidences are really important in the digital era. With the coming time the cases will demand more of digital evidences or electronic records rather than the printed or documented evidences.

#### **IV. CONCLUSION**

Thus, the introduction of IT Act and the corresponding amendments in the Indian Evidence Act, 1872 have to an extent established a legal framework for the admissibility of digital evidences. Though, the provisions where unclear and lacks applicability in certain cases while dealing with the question of admissibility, the Indian judiciary especially in the case of Anwar PV clarified the law regarding the admissibility of digital evidence in India. Hence, the evidentiary value of electronic records are elaborated under sections 65-A and 65-B of the Indian Evidence Act, 1872. These sections provide that if the four conditions listed under Section 65-B are satisfied any information contained in an electronic record which is printed on paper, stored, recorded and copied in an optical or magnetic media, produced by a computer is deemed to a document and becomes admissible in proceeding without further proof or production of the original, as evidence of any content of the original or any facts stated therein, which direct evidence would be admissible. However, the lack of resources and lack of technology availability in lower courts may led to some problems and have negative impact on disputing parties as well as court's decree. Moreover, due to the bar of self-incrimination under Article 20(3) of the Constitution of India, the accused cannot be made a witness against himself. Hence, in such situation the question of admissibility such electronic record is in peril. It can be envisioned that in future through judicial intervention, and founded and debated precedents across the common law countries and find a solution for this situation. Also, there are various challenges in the Cyber forensic reports and inclusion of digital evidences like the ongoing

---

<sup>28</sup> Central Electricity Regulatory Commission v National Hydroelectric Power Corporation Ltd. & Ors. (2010) 10 SCC 280

<sup>29</sup> Dr. Madhav Vishwanath Dawalbhakta v M/s. Bendale Brothers, (2018) SCC Online 2652

<sup>30</sup> SBI Cards & Payments Services Pvt. Ltd. v Rohidas Jadhav, (2018) SCC Online 1262

practice of child pornography, online frauds, data theft and etc. which needs strong mechanism and interpretation by judiciary.

\*\*\*\*\*