ELECTRONIC EVIDENCE IN CYBER SPACE LAW: AN ANALYSIS OF ITS ADMISSIBILITY IN INDIA

Written by ***Dr. Banamali Barik***

Asst. Professor in Mayurbhanj Law College, North Orissa University, Baripada

ABSTRACT

The evolution of Information Technology gave birth to the cyberspace, wherein internet provides equal opportunities to everyone to access any information, data storage, analysis etc., with the use of high technology. The increasing dependence on electronic means of communications, e-commerce and storage of information in digital form has most certainly caused a need to transform the law relating to information technology, cyber law and rules of admissibility of electronic evidence both in civil and criminal matters in India. The Information Technology Act, 2000 is a step in this direction. It was with this aim that the Act was enacted. The Act secures a regulatory environment for e-commerce by providing a legal framework governing e-contracting, security and integrity of e-transactions, and use of digital signatures and others. In the 21stcentury, Indian courts have developed guidelines while deciding cases relating to electronic evidence. Judges have also demonstrated perceptiveness towards the intrinsic electronic nature of evidence, which includes insight regarding the admissibility of such evidence and the interpretation of the law in relation to the manner in which electronic evidence can be brought and filed before the court. The e-evidence can be found in e-mails, digital photographs, ATM transaction logs, word processing, documents, internet browser histories databases, contents of computer memory, logs from a hotel's electronic door locks etc., Electronic evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive and more readily available. The present topic analyses the challenges posed with respect to the admissibility of electronic evidence (Section 65-A and 65-B of Indian Evidence Act, 1872) in India and the guidelines laid down by the courts for admissibility of electronic evidence.

Keywords: Electronic Evidence, Admissibility, Information Technology, Digital Signature, Electronic record etc.

INTRODUCTION

The world wide web is a mechanism, or system, for linking together millions of electronic documents, or web pages, each of which can be accessed through a unique, yet changeable, Universal Resource Locator (URL). A website is simple a collection of web pages.[1]

The United Nations Commission on International Trade Law (UNCITRAL) adopted, in June 1996, a Model Law on e-commerce, intended to give States a legislative framework to remove barriers e-commerce. The Model Law provides, among other things, that where the law requires a signature, it could be met electronically if e- signature provided a link between the signer and the record and evidence of intent to be associated with the record, both to be sufficiently reliable for the purposes of the record.[2]

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 corresponding amendments in other legislations are in tune with the provisions and aim at realization of the objectives of the information Technology Act, 2000.[3]

The Act has been brought about to foster an environment in which laws are simple and transparent and in which the advantages of new technologies can be tapped. 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.[4]

---

1. Yee Fen Lim, Cyberspace Law, 2nd edn. (New Delhi: Oxford University Press, 2007) at 2.

2. Ranbir Singh & Ghanshyam Singh et al., Cyber Space and The Law-Issues and Challenges, 1st edn. (Hyderabad: NALSAR University, 2004) at iii (Preface).

3. *Ibid*.

4. Ghanshyam Singh, in et al., Ranbir Singh, Cyber Space and The Law-Issues and Challenges, 1st edn. (Hyderabad: NALSAR University, 2004) at 299.

Though there are several kinds of evidence, the Evidence Act allows mainly two kind of evidence i.e. the oral and documentary evidence, which are most important and reliable evidences. The definition of evidence as given in this Act, as (a) the evidence of witness i.e. oral evidence and (b) documentary evidence which includes electronic record produced for the inspection of the court.[5] Section 3 of the Act was amended and the phrase "All document produced for the inspection of the Court" was substituted by "All documents including electronic records produced for the inspection of the Court".[6] 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 65- A & 65-B were inserted to incorporate the admissibility of electronic evidence. Traditionally, the fundamental rule of evidence is that direct oral evidence may be adduced to prove all facts, except documents. The hearsay rule suggests that any oral evidence that is not direct cannot be relied upon unless it is saved by one of the exceptions as outlined in Section 59 and 60 of the Evidence Act dealing with the hearsay rule. However, the hearsay rule[7] is not as restrictive or as straight forward in the case of documents as it is in the case of oral evidence. This is because it is settled law that oral evidence cannot prove the contents of a document, and the document speaks for itself. Therefore, where a document is absent, oral evidence cannot be given as to the accuracy of the document, and it cannot be compared with the contents of the documents. This is because it would disturb the hearsay rule. (Since the document is absent, the truth or accuracy of the oral evidence cannot be compared to the document.) In order to prove the contents of a document, either primary or secondary evidence must be offered.[8]

---

5. Indian Evidence Act, 1872, s. 3.

6. The Indian Evidence Act has been amended by virtue of Section 92 of Information Technology Act, 2000.

7. Hearsay evidence is anything said outside a court by a person absent from a trial, but which is offered by a third person during the trial as evidence. The law excludes hearsay evidence because it is difficult or impossible to determine its truth and accuracy, which is usually achieved through cross examination. Since the person made the statement and the person to whom it was said cannot be cross examined, a third person's account of it is excluded. There are few exceptions to this rule which need no explanation here.

8. The Centre for Internet and Society, available at http://cisindia.org/internetgovernance/blog/anvarvbasheernewoldlawofeletronicevidence.

While primary evidence of the document is the document itself[9] it was realized that there would be situations in which primary evidence may not be available. Thus secondary evidence in the form of certified copies of the document, copies made by mechanical processes and oral accounts of someone who has seen the document, was permitted under section 63 of the Evidence Act, for the purposes of proving the contents of a document. Therefore, the provision for allowing secondary evidence in a way dilutes the principles of the hearsay rule and is an attempt to reconcile the difficulties of securing the production of documentary primary evidence where the original is not available. Section 65 of the Evidence Act sets out the situations in which primary evidence of the document need not be produced, and secondary evidence, as listed in section 63 of the Evidence Ac, can be offered. This includes situations when the original document: (i) Is in hostile possession; (ii) oral has been proved by the prejudiced party itself or any of its representatives; (iii) Is lost or destroyed; (iv) Cannot be easily moved, i.e. physically brought to the court; (v) Is a public document of the state; (vi) Can be proved by certified when the law narrowly permits; and (vii) Is a collection of several documents.[10] The paper presents the principle of electronic evidence with light of information technology law under statutory provisions and the apex courts have declared the guide lines for admissibility of electronic evidence through the judiciary interpretation.

ELECTRONIC EVIDENCE AND THE INFORMATION TECHNOLOGY ACT, 2000[11]

Section 3 of the Evidence Act, states that the expression "Certifying Authority", "digital signature", Digital Signature Certificate", "electronic form", "electronic record", "information", "secure electronic record", "secure digital signature", and "subscriber" shall have the same meanings respectively assigned to them in the Information Technology Act, 2000.[12]

9. Indian Evidence Act, 1872, s. 62.

10. Manisha T. Karia & Tejas D. Karia, in Stephen Mason et al., Electronic Evidence, 3rd edn. (Lexis Nexis Butterworths, 2012).

11. The expression used in Indian Evidence Act, 1872 but defined in the Information Technology Act, 2000, (w.e.f.17-10-2000).

12. S. R. Myneni, The Law of Evidence, 1stedn., (Hyderabad: Asia Law House, 2008). at 13.

1) 'Digital signature' means authentication of any electronic record by a subscriber by means of an electronic method or produce in accordance with the provision of Section 3 (of the Information Technology Act, 2000) [Sec. 2(p)].
2) 'Digital Signature Certificate' means a Digital Signature Certificate issued under sub- section (4) of Section 35 (of the Information Technology Act, 2000). [Sec. 2(q)].
3) 'electronic form' with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.[Sec. 2(r)].
4) '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 micro fiche. [Sec. 2(t)].
5) 'Information' includes data, text, images, sound, voice, codes, computer programs, software and databases or micro film or computer generated micro fiche. [Sec. 2 (v)].
6) 'secure system' means computer hardware, software, and procedure that:
   a) are reasonably secure from unauthorized access and misuse;
   b) provide a reasonable level of reliability and correct operation;
   c) are reasonably suited to performing the intended functions;
   d) adhere to generally accepted security procedures. [Sec. 2(ze)].
7) 'Security Procedure' means the security procedure prescribed under Section 16 by the Central Government. [Sec. 2(zf)].
8) 'Subscriber' means a person in whose name the Digital Signature Certificate is issued. [Sec. 2(zg)].

The above expression 'secure electronic records' and 'secure digital signature' are not defined in the Information Technology Act, 2000.

ADMISSION UNDER SECTIONSS 17-23 AND 31 OF INDIAN EVIDENCE ACT

The word 'admission' has a technical meaning in law and it has been defined in Section 17 of the Evidence Act thus: "An admission is a statement, oral or documentary or contained in electronic form, which suggests 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 Section 18-20)".

If we take into consideration the Section 18, 19 and 20 along Section 17, the term "admission, can be defined comprehensively.[13]

LEGAL PROVISIONS ON ELECTRONIC EVIDENCE IN INDIA

The law on electronic/digital evidence varies from country to country. In India, the legislation that introduced the Cyber space technology to law was I.T. Act, 2000 (amended in 2008). The Act makes minimal mention of electronic/digital evidence or even the type of crimes happening today. Electronic/digital is also incorporated in the Indian Evidence Act, 1817.

While the law had mostly anticipated primary evidence (i.e. the original document itself) and had created special conditions for secondary evidence, increasing digitization meant that more and more documents were electronically stored. As a result, the abduction of secondary evidence of documents increased.[14] In Anvar P.K. v. P.K. Basheer & Ors. Case,[15] the Supreme Court noted that "there is a revolution in the way that evidence is produced before the court. In India before 2000, electronically stored information was treated as a document and secondary evidence of these electronic 'documents' was adduced through printed re-production or transcripts, the authenticity of which was certified by a competent signatory. The signatory would identify her signature in court and be open to cross examination. However, as the pace and proliferation of technology expanded, and as the creation and storage of electronic information grew more complex, the law had to change more substantially.[16] Under the provisions of Section 61 to 65 of the Indian Evidence Act, 1872, has

13. *Ibid*. at 163.

14. Indian Evidence Act, 1872, s. 62.

15. (2014) 10 SCC 473.

16. Indian Evidence Act, 1872, s. 62.

Mentioned the word "Document or content of document" have not been replaced by the word "Electronic documents or content of electronic documents".

Thus, the intention of the legislature is explicitly clear i.e. not to extend the applicability of section 61to 65 to the electronic record. It is the cardinal principle of interpretation that if the legislature has omitted to use any word, the presumption is that the omission is intentional. It is well settled that the legislature does not use any word unnecessarily.[17] In this regards, the Apex Court in Utkal Contractors & Joinery Pvt. V. State of Orissa,[18] held that "…Parliament is also not expected to express itself unnecessarily. Even as Parliament does not use any word without meaning something, Parliament does not legislate where no legislation is called for. Parliament cannot be assumed to legislate for the sake of legislature; nor indulge in legislation merely to state what it is unnecessary to state or to do what is already validly done. Parliament may not be assumed to legislate unnecessarily".

The IT Act, amended section 59 of the Evidence Act, 1872 to exclude electronic records from the probative force of oral evidence in the same manner as it excluded documents. This is the re-application of the documentary hearsay rule to electronic records. But, instead of submitting electronic records to the test of secondary evidence which, for documents, is contained in section 63 and 65, it inserted two new evidentiary rules for electronic records in the Evidence Act: section 65-A and 65-B. The intention of the legislature 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 cannot be produced in the court of law owing to the size of computer/server, residing in the machine language and thus, requiring the interpreter to read the same.[19] Section 65-A of the Evidence Act, creates special law for electronic evidence-The contents of electronic records may be proved in accordance with the provisions of section 65-B.[20] This section performs the same function for electronic records that section 61 does for documentary evidence: it creates a separate procedure, distinct from the simple procedure for oral evidence, to ensure that the adduction of electronic records obeys the hearsay rule.

17. Prashanti, available at: www.legalservicesindia.com.

18. AIR 1987 SC 1454.

19. *Ibid*.

20. Indian Evidence Act, 1872, s. 62: Special provision as to evidence relating to electronic record.

It also secures other interests, such as the authenticity of the technology and the sanctity of the information retrieval procedure. But section 65-A is further distinguished because it is a special law that stands apart from the documentary evidence procedure in section 63 and 65.

Section 65-B of the Evidence Act, details this special procedure for adducing electronic records in evidence. Sub-section (2) lists the technological conditions upon which a duplicate copy (including a print-out) of an original electronic record may be used:

(i) At the time of the creation of the electronic record, the computer that produced it must have been in regular use;
(ii) The kind of information contained in the electronic record must have been regularly and ordinarily fed in to the computer;
(iii) The computer was operating properly; and
(iv) The duplicate copy must be a reproduction of the original electronic record.

The Section 65-B of the Evidence Act makes the secondary copy in the form of computer output comprising of printout or data copied on electronic/magnetic media admissible.

Section 65-B:[21]

(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on paper, stored recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be in any proceeding, without further proof or production of the original, as evidence of any fact started therein of which direct evidence would be admissible.
(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following namely:
    (a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process

21. Admissibility of electronic records.

information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in any respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed in the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computer, whether:

(a) by a combination of computer operating over that period;

(b) by different computers operating in succession over that period;

(c) by different combination of computers operating in succession over that period;

(d) in any other manner involving successive operation over that period, in whatever order of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purpose of this section as constituting a single computer, and references in this section to a computer shall be accordingly.

(4) In any proceeding where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is, to say:

(a) Identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was production of that electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,

and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person startingit.[22]

The above contention is further strengthened by the insertion words "Notwithstanding anything contained in this Act" to 65-A &65-B, which is non obstante clause, further fortifies the fact that the legislature has intended the production or exhibition of the electronic records by Section 65-A & 65-B only.

A non-obstante clause is generally appended to a section with a view the enacting part of the section, in case of conflict, an overriding effect over the provision in the same or other act mentioned in the non-obstante clause. It is equivalent to saying that despite the provisions or act mentioned in the non-obstante clause, the provision following it will have its full operation or the provisions embraced in the non-obstante clause will not be an impediment for the operation of the enactment or the provision in which the non-obstante clause occurs.

The aforesaid, principles of interpretation with respect to the non-obstante clause in form of "Notwithstanding anything contained in this Act" is further supported by the Hon'ble Apex Court in G. M. Kokil & Ors. V. Union of India and Anr.,[23] observed "It is well known that a non- obstante clause is a legislative device which is usually employed to give overriding effect to certain provisions over some contrary provisions that may be found either in the same enactment or some other enactment, that is to say, to avoid the operation and effect of all contrary provisions". Further, the Hon'ble Court in the case cited as Chandavarkar Sita Ratna Rao v. Ashalata S. Guram,[24] explained the scope of non-obstante clause as "It is equivalent to saying that in spite of the provision of the Act or any other Act mentioned in the non obstante clause or any contract or document mentioned the enactment following it will have its full operation".[25]

22. S. R. Myneni, Supra note 12 at 406-08.

23. (1984) SCR 196.

24. (1986) 3 SCR 866.

25. Vivek Dubey, "Admissibility of Electronic Evidence: An Indian Perspective" (2017) 4(2) Forensic Res Criminal Int J. at 3.

Further, the Supreme Court[26] has held that Section 65-B of the Evidence Act being a 'non-obstante clause' would override the general law on secondary evidence under Section 63 and 65 of the Evidence Act. The section 63 and section 65 of the Evidence Act have no application to the secondary evidence of the electronic evidence and same shall be wholly governed by the Section 65-A and 65-B of the Evidence Act.

JUDICIAL TRENDS

The Supreme Court and High Courts of India have been challenging the electronic evidence and its admissibility in the court of law from time to time. Some principles and guidelines have discussed below.

In State (NCT of Delhi) v. Sandhu Alias Afzal Guru case,[27] the Supreme Court has rightly observed that "in our technological age nothing more primitive can be conceived of than denying discoveries and nothing cruder can retard forensic efficiency than swearing by traditional oral evidence only thereby discouraging the liberal use of scientific aids to prove guilt". Statutory changes are needed to develop more fully a problem solving approach to criminal trials and to deal with heavy workload on the investigators and judges.

In Sil Import, USA v. Exim Aides Exporters, Bangalore,[28] the Supreme Court held that "Technological advancement like facsimile, Internet, e-mail, etc. were in swift progress even before the Bill for the Amendment Act was discussed by Parliament. So when Parliament contemplated notice in writing to be given, we cannot overlook the fact Parliament was aware of modern devices and equipment already in vogue". In State v. Mohd. Afzal and Ors.,[29] the court held that computer generated electronic records is evidence, admissible at a trail if proved in the manner specified by section 65-B of the Evidence Act. In Navjyot Sandhu case, the court held that merely because a certificate containing the details in sub-section (4) of section 65-B is not filed in the instant case, does not mean that secondary evidence cannot be given even if the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely section 63 and 65.

26. Civil Appeal No. 4226 of 2012.

27. (2005) 11 SCC 600.

28. MANU/SC/0312/1999, (1999) 4 SCC 567.

29.(2003) DLT 385, 2003 (71)DRJ 17.

The Supreme Court also finding in this case, raised uncomfortable questions about the integrity of prosecution evidence, especially in trails related to national security or in high-profile cases of political importance. The state's investigation of the Parliament attacks was shoddy with respect to the interception of telephone calls. The Supreme Court's judgment notes (in para 148,153 and 154) held that the law and procedure of wiretaps was violated in several ways.

In BodalaMurali Krishna v. Smt. Bodala Prathima case,[30] the court held that, "… the amendment carried to the Evidence Act by introduction of section 65-A and 65-B are in relation to the electronic record. Section 67-A and 73-A were introduced as regard proof and verification of digital signatures. As regards presumption to be drawn about such records, Section 85-A, 85-B, 85-C, 88-A and 90-A were added. These provisions are referred only to demonstrate that the emphasis, at present, is to recognize the electronic records and digital signatures, as admissible pieces of evidence".

In Anvar P. v. P.K. Basheer and Ors.,[31] the Supreme Court said, "Irrespective of the compliance of the requirements of section 65-B, which is a provision dealing with admissibility of electronic records, there is no bar to adducing secondary evidence under the other provisions of the Evidence Act, namely, section 63 and 65. It may be that the certificate containing the details in sub-section (4) of section 65-B is not filed in the instant case, but that does not mean that secondary evidence cannot be given even if the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely section 63 and 65. This case also overrules the judgment of Navjot Sandhu case,[32] by the two Bench of the Supreme Court and observed that the statement of law on admissibility of electronic evidence pertaining to electronic record of this court, does not lay down correct position and is required to be overruled. This judgment has put to rest the controversies arising from the various conflicting judgments and thereby provided a guideline regarding the practices being followed in the various High Courts and the Trail Court as to the admissibility of the electronic evidence.

30. 2007 (2) ALD 72.

31. In Civil Appeal No. 4226 of 2012.

32. (2005) 11 SCC 600.

In Sanjaysinh Ramrao Chavan v. Dattarry Gulabrao Phalke case,[33] it was held that as the voice recorder had itself not subjected to analysis, there is no point in placing reliance on the translated version. Without source, there is no authenticity for the translation. Source and authenticity are the two key factors for electronic evidence.

Lastly, the judgment of Jadeo Singh v.The State and Ors.[34] pronounced by Hon 'ble High Court of Delhi, while dealing with the admissibility of intercepted telephone call in a CD and CDR which were without a certificate under section 65-B of Evidence Act, the court observed that the secondary electronic evidence without certificate under section 65-B is inadmissible and cannot be looked into by the court for any purpose whatsoever.

CONCLUSION

The evidentiary value of electronic records is elaborated under section 65-A and 65-B of the Indian Evidence Act, 1872. These sections provide that if the four conditions listed 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 be a document and becomes admissible in proceeding without further proof or production of the original, as evidence of any contacts of the original or any facts stated therein, which direct evidence would be admissible. The trial courts judges are not technologically sound and do not have forensic laboratory in the courts premises. Hence, the judges and prosecutors in lower courts should be imparted training and knowledge relating to electronically stored information to equip them with new developments in this field.

The legal interpretation by the court of Sections 22-A, 45-A, 59, 65-A & 65-B of the Indian Evidence Act, 1872 has confirmed that the stored data in CD/DVD/Pen Drive is not admissible without a certificate, under section 65-B(4) of Evidence Act and further clarified that in absence of such a certificate, the oral evidence to prove existence of such electronic evidence and the expert view under section 45-AEvidence Act cannot be availed to prove authenticity thereof.

33. MANU/SC/0040/2015.

34. MANU/DE/0376/2015.

In this context, the law enforcement agencies and investigating officers should be update and have knowledge about authentication process prescribed by the court for the admissibility of electronic/digital evidences.

Special law and procedure was created by amending section 65-A and 65-B of the Indian Evidence Act for electronic evidence, but practically it was not used. For example, in the parliament attacks case (Navjot Sandhu), the Supreme Court, admitted copies of call detail records without following procedures of Section 65-A and 65-B.The records should have been admitted following the procedures laid down of said two sections.