Munish Rathi et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 4, Issue 3, Sept 2017, pp. 300-305

Use of Technology and the Rule of Evidence in Law

Munish Rathi

LL.B., LLM Kurukshetra University, Kurukshetra

Abstract: **The entire existence of Law and Justice is governed by the law of evidence itself and there is or will be no exceptions to it. Today the whole world is wired, living in a state of electronic connectivity with digital technologies whether they be cameras, print and electronic media, or computers and mobile devices. Thus, our societies are super-connected. Measures are under way to facilitate growth of e- commerce, electronic communication through internet and accelerated induction of technology in critical sectors and therefore the Information Technology Act, 2000 was introduced it seeks to provide legal frame work for recognition of electronic contracts and prevention of computer crimes.**

Keywords: Rule of Evidence, Law, Technology

I. INTRODUCTION

It paves for electronic filing of documents and legalise digital signatures. For the purpose amendments were carried out in the Indian Evidence Act, Indian Penal Code, Bankers Book Evidence Act and RBI Act. However rapid shits in technology have made the collection and analysis of evidence in court more challenging but it also at the same time became an important tool to solve crimes and to find out the locations of criminals. As a matter of fact in India today there is a revolution in the way the evidence is produced before the Court. When electronically stored information was treated as a document in India before 2000, secondary evidence of these electronic "documents" was adduced through printed reproductions or transcripts, and the authenticity was certified. When the creation and storage of electronic information grew more complex, the law had to change more substantially.[i]

II. USE OF TECHNOLOGY IN COURT ROOMS

According to Section 273 of Cr.PC, 1973 the evidence in course of trial or other proceedings shall be recorded in presence of accused. If personal attendance of the accused has been exempted, then the evidence shall be recorded in presence of his pleader. It was held by the Hon'ble Supreme Court that section 273 does not provide that at the time of recording of evidence witness/victim must be remain present physically before the accused so that accused may see him/her eye to eye . Thus in this way it is permissible to take evidence through video conferencing under section 273 of the Code.[ii] Such a procedure under the Code can only be permissible only when it is not possible to procure the attendance of a witness without the amount of delay, inconvenience or expenses.[iii] Through the mode of video conferencing accused can hear what is being said by the witness against him while it is no so possible even when the accused itself present in Court room.

III. EVIDENTIARY VALUE AND MODES OF TENDERING AND ADMITTING DIGITAL EVIDENCE

Today information can be stored in computer hard drive, optical disks, floppy disks, remote internet storage, handheld devices, memory cards, network servers, emails etc. Though electronic evidence is defined as information of investigative value relating to a broad range of devices and data formats, a formal legal definition of digital evidence is elusive, but is generally accepted to be information held in digital form that has some probative value. And when we say that evidence must be admissible we mean that it must conform to certain rules before it can be considered by the court for its probative value. For example a telephone company can produce records of calls made from a particular telephone line, Mobile or through internet which is installed in a suspect's home. However, the accuracy of such evidence can refer to several things and in relation to computer evidence which is typical sought in legal cases includes system logs; audit logs, application logs, network management logs, network traffic capture, and file system data.[iv]

Tape and Video Records

Tape recorded conversation could be only relied upon as corroborative evidence of conversation deposed by any of the parties of the conversation. In the absence of any such corroboration or corroborative evidenced the tape is not a proper evidence and could not be relied upon.[1] And a video is

[1] Mahabir Parshad v Surinder Kaur, AIR 1982 SC 1043

to be supported by an independent testimony.[2] Moreover the time and place and accuracy of the recording must be proved by a competent witness and the voices must be properly identified. One of the features of magnetic tape recording is the ability to erase and re-use the recording medium. Because of this facility of erasure and re-use, the evidence must be received with caution. The court must be satisfied beyond reasonable doubt that the record has not been tampered with.[3] The authenticity of the video and audio recording should be certified either by the Forensic Laboratory[4] or by a competent authority or Independent testimony of the person tendering or who has recorded or made it.

IV. CHARACTERISTICS OF DIGITAL EVIDENCE

Denial or admissibility of techno based evidences or the digital evidences in Court under the roof of law are basically found place primarily due to following:-

1. It is intangible and transient nature of data, especially in a networked environment where such evidence can be created, stored, copied and transmitted with relative ease.
2. It can also be modified or tampered without signs of obvious distortions, thereby rendering the process of investigation and recording of evidence extremely vulnerable to claims of errors, accidental alteration, prejudicial interference or fabrication.[5]
3. Errors can be introduced during examination and interpretation of the evidence or the examination tools being used can contain malicious software or viruses that can cause them to represent the data incorrectly.[6]
4. It is not easy to prove.
5. Not easy to preserve for long time, technical obsolescence is a major problem maintaining access to digital records over the long - term involves interdependent strategies for preservation in the short to medium term based on safeguarding storage media, content and documentation, and computer software and hardware; and strategies for long - term preservation to address the issues of software and hardware obsolescence.[7]
6. Difficult to be translated and interpreted for the court - Electronic evidence is, by its very nature, binary patterns in magnetic, optical or electronic form all of which need to be translated and interpreted for the court - "Evidence of these crimes is neither physical nor human, but, if it exists, is little more than electronic impulses and programming codes. If someone opened a digital storage device, they would see no letters, numbers, or pictures on it.

V. AUTHENTICATION OF ELECTRONIC RECORDS

According to Section 3 of the Information Technology Act, 2000, any subscriber may authenticate an electronic record by affixing his digital signature. The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record. It further explains that "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller. Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person (then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government. "Signed", with its grammatical Variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.[8] Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is -[9]

(a) Rendered or made available in an electronic form; and

(b) Accessible so as to be usable for a subsequent reference

Where for providing expert opinion on electronic form of evidence before any court or other authority the central Government may by notification, empowered or specify any department, body or agency for the same.[10] Section 2 - A of the Bankers Book Evidence Act, 1891, provides that a printout

[2] R.K Malkani v State of Maharashtra, AIR 1973 SC 157

[3] Yusufalli Esmail Nagree vs The State Of Maharashtra, AIR 1968 SC 147

[4] R. Venkatesh v State, 1980 Cri.LJ 103

[5] I Walden, Computer Crime, http://kavehh.com/my%20Document/KCL/Internet%20Law/reading/Computer%252Crime%2520%25286th%2520ed.%2529.pdf.

[6] E Casey, Digital Evidence and Computer Crime, 231, (Elsevier Academic Press CA, 2nd edn, 2004)

[7] Digital Preservation Coalition, Organizational Activities, http://handbook.dpconline.org/organisationalactivities/ storage.

[8] Section 4, Information Technology Act, 2000

[9] Section 5, Information Technology Act, 2000

[10] Section 79 – A, Information Technology Act, 2000

of entry or a copy of printout shall be accompanied by the following, namely:-

a. a certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and
b. a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of:-
    1. he safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons;
    2. the safeguards adopted to prevent and detect unauthorised change of data;
    3. he safeguards available to retrieve data that is lost due to systemic failure or any other reasons;
    4. the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices;
    5. the mode of verification in order to ensure that data has been accurately transferred to such removable media;
    6. the mode of identification of such data storage devices;
    7. the arrangements for the storage and custody of such storage devices;
    8. the safeguards to prevent and detect any tampering with the system; and
    9. any other factor which will vouch for the integrity and accuracy of the system.
c. A further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, the relevant data.

Proving electronic evidence in court

According to Section 3 of the Indian evidence Act, 1872 "evidence" means and includes-

(1) All statements which the court permits or requires to be made before it by witnesses, in relation to the matter of fact under inquiry; Such statements are called oral evidence;
(2) All documents (including electronic records) produced for the inspection of the court; such documents are called documentary evidence.[11]

Before the insertion of amendment in evidence Act in year 2000, Evidence means and includes:

(1) All statements which the Court permits or requires to be made before it by witness, in relation to matters of fact under inquiry.
(2) All documents produce for the inspection of court; such documents are called documentary evidence.

Section 65 A of the Indian Evidence Act states that the contents of electronic records may be proved in accordance with the provisions of section 65B. Section 65B deals with the Admissibility of electronic records and provides that any information contained in an electronic record which is printed on a 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 also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question 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.

Conditions for admissibility of Electronic Records

The Section provides following conditions for admissibility of electronic records.

1. That 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 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
2. That 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;
3. That throughout the material part of the said period, the computer was operating properly or, if not, then in 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
4. That the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

Sub section 4 of section 65B provides that in any proceedings 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:-

1. identifying the electronic record containing the statement and describing the manner in which it was produced;
2. giving such particulars of any device involved in the production of that electronic record as may be

[11] Section 3, The Indian evidence Act, 1872

appropriate for the purpose of showing that the electronic record was produced by a computer;

3. 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 stating it.

VI. DIGITAL EVIDENCE AND JUDICIAL APPROACH

In *State of Punjab v. Amritsar Beverages Ltd.*[12] a search by the Sales Tax Department was conducted and the seizure of computer hard disks and documents from the dealer's premises is done. The computer hard disk was seized under the provisions set out in section 14 of the Punjab General Sales Tax Act, 1948, the Act under section 14(3) which provides that If any officer referred to in sub-section (1) of section 14(3) has reasonable ground for believing that any dealer is trying to evade liability for tax or other dues under this Act, and that anything necessary for the Purpose of an investigation into his liability may be found in any book, account, register or document; he may seize such book, account, register or document, as may be necessary. For the purpose of sub-section (2) or sub-section (3), an officer referred to in sub-section (1) may enter and search any office, shop, godown, vessel, vehicle, or any other place of business of the dealer or any building or place except residential houses where such officer has reason to believe that the dealer keeps or is, for the time being, keeping any book account, register, document or goods, relating to his business. The power conferred by sub-section (4) shall include the power to open and search any box or receptacle in which any books, accounts, register or other relevant document of the dealer may be contained. The section entitles the officer concerned to affix his signature and seal at one or more places on the document seized, and to include in the receipt the number of places where the signature and seal of the officer had been affixed. In this instance, the officers concerned called upon the dealer, but the dealer failed to pay heed to their requests. The Sales Tax Authority was required to return all the documents seized after examination within 60 days. However, the Authority failed to return the hard disk, claiming it is not a document. When the matter came before the Supreme Court, a creative interpretation was adopted, taking into account the fact that the Act was enacted in 1948, when information technology at that time was far from being developed. It was determined that the Constitution of India is a document that must be interpreted in the light of contemporary life. This mean a creative interpretation was necessary to enable the judiciary to respond to the development of technologies, and the court could use its own interpretative principles to achieve a balance in the absence of the failure of Parliament to respond to the need to amend the statute having regard to the developments in the field of science. The court stated that the Evidence Act, which is part of the procedural laws, should be construed to be an ongoing statute, similar to the Constitution, which meant a creative interpretation was possible, in accordance with the circumstances. It was held that the proper course for the officers in such circumstances was to make out copies of the hard disk or to obtain a hard copy and affix their signatures or official seal in physical form upon the hard copy and furnish a copy to the dealer or the person concerned. In, State *of Maharashtra v. Dr Praful B Desai*,[13] The question was involved whether a witness can be examined by means of a video conference. The Supreme Court observed that video conferencing is an advancement of science and technology which permits seeing, hearing and talking with someone who is not physically present with the same facility and ease as if they were physically present. The legal requirement for the presence of the witness does not mean actual physical presence. The court allowed the examination of a witness through video conferencing and concluded that there is no reason why the examination of a witness by video conferencing should not be an essential part of electronic evidence. In case of *Tukaram S.Dighole v Manikrao Shivaji Kokate*[14], a cassette placed before the Court was discarded from evidence. This was the cassette produced from the custody of an Election Commissioner's office. It was taken to be a public document. It was held that mere production of the audio cassette even certified by the Election Commissioner is not conclusive of the fact that what is contained in the cassette was true and correct. This is on par with the certified copy of any document produced from public record. Such a document would show that it was a document filed in the public office and is a true production of whatever was filed in the public office. It however cannot prove the truth of the contents of the document merely by the production of even its certified copy by the public office .Consequently, in that case when the party who produced the record did not lead any evidence to prove that the cassette produced on record was a true reproduction of the original speeches by the Respondent or his agent, which he was incumbent to be proved either himself or through his witness who is the maker of the record, it was held not to be considered in evidence. It was held by the Supreme Court that the "standard of proof" in the form of electronic evidence should be "more accurate and stringent" as compared to other documentary evidence. In, *Fatima Riswana v. State and others*,[15] the prosecution was relating to exploitation of certain men and women for the purpose of making pornographic

[12] (2006) 7 SCC 607
[13] AIR 2003 SC 2053
[14] 2008 (3) BomCR 141
[15] AIR 2005 SC 712

photos and videos in various acts of sexual intercourse and thereafter selling them to foreign websites. The case was allotted to fast track court presided over by a lady judge. The accused applied for copies of the CDs. The trial court rejected that prayer. The High Court also rejected such prayer by observing that if their copies are provided, they can be copied further and put into circulation. However, the High Court allowed viewing of the CDs in the chamber of the judge. It was contended on behalf of the accused that it may cause embarrassment to the lady judge. Hence, the matter was directed to be transferred to the court of a male judge. However, the concern of the victim side was not considered. The apex court observed that a judicial officer be it a female or male is expected to face this challenge when call of duty required it. Therefore that order was set aside. In *Anvar v. P. K. Basheer*.,[16] the Supreme Court noted that "there is a revolution in the way that evidence is produced before the court". When electronically stored information was treated as a document in India before 2000, secondary evidence of these electronic 'documents' was adduced through printed reproductions or transcripts, and the authenticity was certified. The signatory would identify signature in court and be open to cross examination by meeting the conditions of both Sections 63 and 65 of the Evidence Act. When the creation and storage of electronic information grew more complex, the law had to change more substantially. By the Information Technology Act, 2000 new definitions are given to the words "data", "electronic record", and "computer". New Section 22A has been inserted into Evidence Act, to provide for the relevancy of 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. Section 59 of the Evidence Act is amended by the IT Act to exclude electronic records and inserted section 65A and section 65B, instead of submitting electronic records to the test of secondary evidence as contained in sections 63 and 65. Section 65A has given the right to prove the contents of electronic records in accordance with the provisions of section 65B. Section 65A of the Evidence Act is for electronic records just as section 61 does is for documentary evidence. A procedure, distinct from the one for oral evidence is formulated, to ensure electronic records obeys the hearsay rule. Section 65A is a special law that stands apart from the documentary evidence procedure in sections 63 and 65. Any probative information stored or transmitted in digital form is digital evidence or electronic evidence. Also the Court has settled the controversies arising from the various conflicting judgments as well as the practices being followed in the various High Courts and the Trial Courts as to the admissibility of the Electronic Evidences. The Court has interpreted the Section 22A, 45A, 59, 65A & 65B of the Evidence Act and held that secondary data in CD/DVD/Pen Drive are not admissible without a certificate U/s 65 B(4) of Evidence Act. It has been elucidated that electronic evidence without certificate U/s 65B cannot be proved by oral evidence and also the opinion of the expert U/s 45A Evidence Act cannot be resorted to make such electronic evidence admissible. The judgment would have serious implications in all the cases where the prosecution relies on the electronic data and particularly in the cases of anticorruption where the reliance is being placed on the audio video recordings which are being forwarded in the form of CD/DVD to the Court. In all such cases, where the CD/DVD are being forwarded without a certificate U/s 65B Evidence Act, such CD/DVD are not admissible in evidence and further expert opinion as to their genuineness cannot be looked into by the Court as evident from the Supreme Court Judgment. Electronic records being more susceptible to tampering, alteration, transposition, excision, etc. without such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice. Thus, the only options left to prove the electronic record/evidence is by producing the original electronic media as Primary Evidence court or it's copy by way secondary evidence U/s 65A/65B of Evidence Act. Thus, in the case of CD, DVD, Memory Card etc. containing secondary evidence, the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible

VII. CONCLUSION

From legal point of view digital evidence is not very different from other forms of evidence. Like any other form of evidence, it has to be relevant to the dispute, and it has to pass admissibility test. Also the advanced analysis of digital evidence, such as event reconstruction, often requires specialist knowledge and, therefore, falls into the category of expert evidence. As expert evidence, it may have to pass daubert criteria or similar admissibility test that verifies that its analysis methodology is scientifically valid. Thus, passing admissibility test for expert evidence is an important requirement for event reconstruction in digital investigations. But with the changing face of globalization, the use of information and telecommunication technologies should not be limited to facilitate the context of E-commerce, but also on individual, personal level. In the cyber age the evidence of crime lies in the digital formats like e-mails, chats, documents, digital pictures, pen drives, mobile phones etc. but the law enforcement agencies are handicapped in understanding these technical evidences and therefore there is need for digital forensics training to be imparted to them in order to make them more sound. Because the Criminals will be eager to use computers and other digital and electronic gadgets, if they know that attorneys, forensic examiners, or computer security Professionals are ill equipped to deal with digital evidence.

[16] AIR 2015 SC 180

Therefore it is necessary for one who is involved with criminal investigation, prosecution, or defense work that he should be comfortable with the personal computers and networks as a source of evidence. Moreover legislation continues to change to keep up with technological and societal change. Therefore it is also important to consider the legal requirements and restrictions when examining digital evidence because evidence is the consideration for justice.

[i] Anvar v. P. K. Basheer, AIR 2015 SC 180
[ii] Sakshi V. Union of India, 2004 CriLJ 2881 SC
[iii] State of Maharashtra v Dr. P. Desai, AIR 2003 SC 3114
[iv] Dr. Swarupa Dholam, "Electronic evidence and its challenges" 4, (Maharashtra Judicial Academy)

