Admissibility Of Electronic Evidence- A Legislative Analysis

Rishabh Raj
Managing Partner QUADLegal
1. Introduction........................................................................................................... 1-2
2. Meaning............................................................................................................... 3-4
3. Legal Framework- A Comparative Study....................................................... 5-13
   a. Evidentiary value as a document............................................................. 5-7
      i. Indian Evidence Act, 1872..................................................................... 5-6
      ii. UNCITRAL Model Law....................................................................... 6
      iii. Information Technology Act, 2000...................................................... 6-7
   b. Rule against Hearsay..................................................................................... 7-13
      i. In United States of America (U.S)......................................................... 8-9
      ii. In United Kingdom (U.K).................................................................... 9-10
      iii. In Canada.......................................................................................... 10-11
      iv. In India............................................................................................ 11-13
         ❖ Authenticity.......................................................................................... 12
         ❖ Electronic Signature............................................................................. 12
         ❖ Primary or Secondary Evidence.......................................................... 13
4. Admissibility of Electronic Evidence: Challenges for Legal Fraternity
   (Case Laws)......................................................................................................... 14-17
5. Conclusion & Suggestions............................................................................ 18-19
Introduction

The Evidence Act was drafted to codify principles of evidence in the common law. Indian Evidence Act was drafted in the 19th century. With the advent of Technology, the definition and scope of evidence as under Section 3 of the Act is not limited merely to oral evidence and documentary evidence. A majority of transactions are now done in cyberspace where electronic contracts are executed with the help of digital signatures.

The rapid development of information and communication technologies over the past decade has revolutionized both business and individual practices. The worldwide explosion of electronic commerce and the developments in the computer and telecommunications sectors are deeply changing the delivery and availability of information, acts, transactions and services.

The proliferation of computers has created a number of problems for the law. Many legal rules assume the existence of paper records, of signed records, of original records. The law of evidence traditionally relies on paper records as well, though of course oral testimony and other kinds of physical objects have always been part of our courtrooms, too. As more and more activities are carried out by electronic means, it becomes more and more important that evidence of these activities be available to demonstrate the legal rights that flow from them.

Most electronic records are, in practice, being admitted in litigation. However, courts have struggled with the traditional rules of evidence, with inconsistent results. The common term “reliability” has caused confusion between the principles of authentication, best evidence, hearsay and weight.

1 For the impact of the Internet and related Information Technologies on Indian citizens, see “World Without Borders: E-mail and Cyberchat are revolutionizing the way we live”, The Week, Aug. 8, 1999, p. 12; on individual based business.

2 Litigation based on computer records has been extensive in countries like the United States, Canada, Japan, UK, etc., where the establishment of facts depends entirely on computer generated evidence. In India too, electronic records have been dealt with, albeit not comprehensively. In this context, see Section 610 A, Companies Act, 1956 (Admissibility of micro-films, facsimile copies of documents, computer print-outs and documents on computer media as documents and as evidence) which was inserted by the Companies (Amendment) Act, 1996.
What is worse, many record managers and their legal advisers have not been confident that modern information systems, especially electronic imaging with the paper originals destroyed, will produce records suitable for use in court. For this reason, there has been a growing demand from industry and users for new types of signature, to effectively substitute the hand-written signature in the electronic environment, granting integrity, confidentiality and authenticity of information and documents.
Meaning

The Indian Evidence Act has been amended by virtue of Section 92 of Information Technology Act, 2000 (Before amendment). Section 3 of the Act was amended and the phrase “All documents produced for the inspection of the Court” were substituted by “All documents including electronic records produced for the inspection of the Court”. Regarding the documentary evidence, in Section 59, for the words “Content of documents” the words “Content of documents or electronic records” have been substituted and Section 65A & 65B were inserted to incorporate the admissibility of electronic evidence. In Section 61 to 65, the word “Document or content of documents” 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 61 to 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. In this regard, the Apex Court in *Utkal Contractors & Joinery Pvt. Ltd. v. State of Orissa*3 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 legislation; 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.”

Thus, the omission of the word, “Electronic Records” in the scheme of Section 61 to 65 signifies the clear and explicit legislative intention, i.e. not to extend the applicability of Section 61 to 65 to the electronic record in view of overriding provision of Section 65-B Indian Evidence Act dealing exclusively with the admissibility of the electronic record which in view of the compelling technological reasons can be admitted only in the manner specified under Section 65-B Indian Evidence Act.

The Admissibility of Electronic Evidence as explained under Section 65(B) is that:

---

3 1987 AIR 2310
Notwithstanding anything contained in this Act, 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
- 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.

The Intention of the legislature being quite clear that an electronic signature would be adduced the admissibility of a primary evidence and also as a direct evidence as opposed to rule of hearsay.
Legal framework - A Comparative study

a. EVIDENTIARY VALUE AS A DOCUMENT

i. Indian Evidence Act, 1872

The Indian Evidence Act, 1872, when compared with the General Clauses Act, 1897, excludes the word “written” from its definition of “document.” The focus of this statute is on the purpose the document is to be used for, i.e. recording the matter. The laws of interpretation indicate that when a statute specifically excludes, that definition overrides any general definition, in this case, the General Clauses Act. The Evidence Act further state that, with some limited exception, when the contents of a document are to be proved, the document itself has to be adduced and copies of it shall not be admissible. Electronic records raise the question of what is an original. If being adduced as original, the electronic document itself has to be examined by the trier. The only way to examine an electronic document is by displaying it on a secondary device, either a screen or a printout. It is a tenable argument that such display is not original, but amounts to a copy, and is, therefore, inadmissible as evidence. Indian law does not resolve this issue. An alternative route could be using the evidence for corroborative purposes. Oral evidence can be introduced if it relates to a relevant fact. Further, if the oral evidence refers to the existence or condition of any material thing other than a document, the court may require the production of such material thing for inspection. Thus, if oral evidence as to the existence of a contract is adduced, then computer evidence may become admissible as it can be termed a material thing. Therefore, computer evidence may be allowed to corroborate the oral evidence extended. Indian courts have allowed tape recordings to be admissible in this manner.

---

4 Section 3 defines “document” to include any matter expressed or described upon any substance by means of letters, figures, or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter.
5 Indian Evidence Act, Section 64
6 Ibid, Section 59
7 Ibid Second Provision of Section 60
8 M.P. Verma v. Surinder Kaur, AIR 1982 SC 1043
ii. **UNCITRAL Model Law**

The Model law mandates that if there is a legal requirement of an original, this requirement will be met by a data message if it satisfies the following two tests:

i. there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

ii. where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

Digital signatures can also be used to ensure the integrity of messages or information. The Model law states that information in the form of a data message shall be given due evidential weight, after considering the reliability of the manner in which the data message was generated, stored or communicated, reliability of the manner in which the integrity of the information was maintained, the manner in which the originator was identified, and any other relevant factor.

iii. **Information Technology Act, 2000**

The IT Act, through its amending section, brings in a new section into the Indian Evidence Act which reads as under: 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 shall be deemed to be also a document 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

---

9. Z.B. Bukhari v. B.R. Mehra, AIR 1975 SC 1788, which held, “tape recordings stand on the same footing as photographs and are documents per section 3 of the Evidence Act.”

10. R. v. Fellows; R. v. Arnold, (1997) 2 All ER 548 (557) where Evans, J., held “….We conclude that there is no restriction on the nature of the copy, and that the data represents the original photograph, in another form.”

11. UNCITRAL Model Law, Article 13

12. *Ibid* Article 8 (1) (a), (b)

13. *Ibid* Article 9 (2)
admissible. The conditions referred above in respect of a computer output shall be following:

- 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;
- 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;
- 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
- 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. Thus, an electronic document can for all practical purposes have the same legal effect as a paper based original document.

b. RULE AGAINST HEARSAY

The rule against hearsay is an important evidential tool in common law countries, and has been often used to exclude a large amount of evidence. “Evidence from any witness which consists of what another person stated (whether verbally, in writing, or by any other method of assertion such as a gesture) on any prior occasion is inadmissible, if its only relevant purpose is to prove that any fact so stated by that person on that prior occasion is true. Such a statement may, however, be admitted for any relevant purpose other than proving the truth of facts stated in it.” Hearsay Evidence is a weak evidence. Weaknesses within a hearsay statement may include defects in the declarant’s perception; defects in the declarant’s memory; lack of the declarant’s sincerity or veracity; and

---

14 The Indian Evidence Act, Section 65B(1)

15 Ibid, Section 65B(2)

16 Peter Murphy, Murphy on Evidence, 5th Edn., 1997, Universal Law Publishing Co. Pvt. Ltd., New Delhi, p. 172
defects in the declarant’s narration or transmission of the statement. The underlying assumption of the hearsay rule is, therefore, that the untested nature of such evidence justifies its exclusion.

The question that arises in the context of electronic documents is that: Since the document is subject to traceless tampering (because of electronic format) and does not state the truth of the matter contained therein, should not the rule against hearsay apply, and thus exclude the admissibility of electronic documents?

\[i. \text{ In United States Of America (U.S.A)}\]

As defined by the Federal Rules of Evidence, ‘hearsay’ is “a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted.”

A ‘statement’ for purposes of hearsay is defined as, “an oral or written assertion, or non-verbal conduct of a person, if it is intended by the person as an assertion.”

The Americans have had a history admitting computer-generated evidence as an exception to the hearsay rule. The Federal Rules prescribe certain exceptions to the hearsay rule. Thus, if it can be proved that the evidence sought to be adduced falls under

---

17 G. Lilly, An Introduction to the Law of Evidence, 2nd Edn., 1987, p. 182
18 Id at p. 183
19 It is not a matter of contention that documents too attract the hearsay rule. In this context see Myers v. DPP, [1964] 2 All ER 881, where a companies business records were treated as hearsay; R v. Patel, [1981] 3 All ER 94, where the Immigration Records at the Home Office were treated as hearsay; Laksmi Raj Shetty v. State of Tamil Nadu, AIR 1988 SC 1274, where the Indian Supreme Court held newspaper reports to be hearsay evidence.
20 Fed. R. Evid. 801 (c)
21 Fed. R. Evid. 801 (a)
23 Art. VIII (Hearsay), Rule 803 (Hearsay Exceptions)
an exception, it can be made admissible. The most relevant exception in the case of E-Commerce is the Records of Regularly Conducted Business Activity.24

Monotype Corporation Plc v. International Typeface Corporation25 involved admissibility of an E-mail message under the business record exception to hearsay rule. The court held that the E-mail is not a regular, systematic record meeting the foundational requirements of the business records exception.96 As computers are being used widely in the public sphere as well in the US, there will be a need to introduce them under one of the other exceptions to hearsay. However, the issue of Internet evidence as a public record is well settled in the United States. In Armstrong v. Executive Office of the President,27 the court unequivocally held that government E-mail is a record as per the Federal Records Act, and it is insufficient for the Government only to preserve a print-out.

ii. In United Kingdom (U.K)

The hearsay rule has been formalized by the House of Lords in a number of cases.28 The position regarding hearsay in England today is still governed by the landmark case in 1965 of Myers v. DPP29 that concerned an alleged conspiracy to deal in stolen cars. The defendant would buy a wrecked car and it’s log-book, and then steal an almost identical car. He would then convert the stolen car so that the details matched the logbook and proceed to sell it for a profit. Evidence produced by the car manufacturers at the time of

24 Fed. R. Evid. 803 (6); See Rosenberg v. Collins, 624 F. 2d 659, 665 (5th Cir. 1980)
25 Monotype Corp., Plc. v. International Typeface Corp., 43 F.3d 443 (9th Circuit)
26 However, in U.S. v. Catabran, 836 F.2d 453 (9th Cir. 1988), the court held that computerized printouts of accounting and other booking keeping records are admissible as business records. Critical to admissibility of the computer records was testimony establishing the foundational requirements of Federal Rule of Evidence 803(6); See also Quality Auto Serv. v. Fiesta Lincoln-Mercury Dodge, Inc. No. 04-96-00967-CV, 1997 WL 563176 (Tex. App. Sept. 10, 1997) holding that computer generated compilations of original invoices qualified as business records; U.S. v. Kim, 595 F.2d 755 (D.C. Cir. 1979), where discussing the admissibility of a telex, the court explained that the “critical factor in determining whether the document satisfied the ’business purpose’ requirement lies in the reason that the message was prepared and sent, not the means by which it was transmitted.”
27 1F.3d 1274 (DC Circuit, 1993)
28 Taper v. Regiman, 1952 All ER 447; Myers v. DPP, (1964) 1 All ER 877; R. v Patel, (1981) 3 All ER 94
29 Myers v. DPP, (1964) 1 All ER 877
the production of the cars was critical to the prosecution’s case. As the cars moved along the production line, workers recorded details of the serial numbers of the various components fitted to a particular car. The worker responsible recorded these details on a card. Eventually, the completed card was photographed and recorded on microfilm. The prosecution sought to put the microfilm in evidence at the trial under the exception to the hearsay rule which covered business records in the Evidence Act, 1938.\textsuperscript{30} The Act did not mention microfilm as a type of business record because the product was not in common use by the businesses in the 1930s. The House of Lords held the evidence to be inadmissible as hearsay, because any exception to the hearsay rule had to be construed restrictively.

\textit{iii. In Canada}

if a record is created in the ordinary course of business and is relied on in the business, then it is admissible.\textsuperscript{31} Some rules require that it be created more or less at the same time as the event recorded, and sometimes by a person with a duty to record it. These circumstances give the record sufficient assurances of the truth of its contents that it may be admitted.\textsuperscript{32} The rule does not require separate proof of the truth of a record’s contents. The making and the use of the record in the course of business provides sufficient guarantee of the truth of the record’s contents to support admission.\textsuperscript{33}

In R. v. Weir,\textsuperscript{34} the question involved was whether an E-mail carried a reasonable level of privacy. The evidence sought to be adduced were user logs and Email messages supplied by the Internet Service Provider. The Court held that, “The Crown relies on an unseen process of extraction of non-visual information from a CPU. Further, the Crown had the diskettes which contain the extracted copies of what was on the CPU, again non-visual information, made exhibits at the voir dire. Although visual representations (i.e. printouts)

\textsuperscript{30} This statute has been repealed and replaced by the Civil Evidence Act, 1968 and is thus defunct.
\textsuperscript{31} Canadian Evidence Act; Section 30
of the data were made exhibits, they were made exhibits only for ease of reference. In other words, to be consistent with the alleged offence in which computer generation of the images is alleged (i.e. no hard copy), the hard copy was entered only to allow me to consider the evidence outside the courtroom without the need to use a computer. The use of unseen procedures to extract information is not new. Blood analyses, breathalyzer tests and photo radar are examples of processes of information extraction which have been subjected to reliability tests over the years. Because computer data can be manipulated, extraction reliability may arise in another case. It did not arise in this one. Second, because the evidence extracted from the CPU to diskette is not something I can see without the use of a computer, exhibit control is exceedingly important. The exhibits in this case were well controlled. The police were careful to keep the confirmatory evidence of the tip separate from the evidence extracted from Mr. Weir’s CPU. Although some of the attachments extracted from both sources look the same, their source has been identified, they have been kept separate, and their continuity ensured.” Thus, a positive judicial attitude, coupled with an effort to create a “Law of Electronic Evidence” has ensured that Canada is in the lead in the development of such jurisprudence.

iv. In India

The idea that hearsay is applicable to documentary evidence is applicable in India, currently stands as law.\textsuperscript{35} The Indian Evidence Act, 1872,\textsuperscript{36} has been interpreted as containing the statutory rule against hearsay in this country.\textsuperscript{37} This mandates all oral evidence to be direct. Further, it is clear that the real evidence as regards computers is admissible. There has been no case in India challenging the admission of computer evidence under Section 32 (2). Section 34 also allows for evidence made in books of accounts. It may be noted that the IT Act has amended Section 34 to include books of accounts kept in electronic form. Thus, there is no difficulty in admitting electronic evidence in India, and any arguments as to hearsay will not stand unless there are compelling reasons, such as the electronic record under examination indeed falling into the hearsay category. Electronic evidence does not demand any change to the rules on

\begin{itemize}
  \item \textsuperscript{35} Laksmi Raj Shetty v. State of Tamil Nadu, AIR 1988 SC 1274 (1290)
  \item \textsuperscript{36} The Indian Evidence Act, 1872; Section 60
\end{itemize}
hearsay. The character of the record can be sufficiently demonstrated under existing law to meet the exceptions, regardless of the medium of the record.

- **Authenticity**

A document’s admissibility is one thing, its probative value quite another. The traditional rationale for authenticating a document is to ascertain that the document is, in fact, what it purports to be in order to prove a relationship between it and an individual. An example of authentication is the establishing of a relationship between a monthly computer-generated summary of account activity and its corresponding customer. The summary of account must be shown to be an authentic statement of transactions between the customer and the plaintiff before the writing may be deemed relevant to an issue raised in litigation. For the document to be carrying any evidential weight and conviction, it must be shown to be authentic. The means of doing this would be through an identification of the person the document relates to. Now, everybody who reads a writing can relate it to its issuer and signer and determine, without any reasonable doubt, the origin of the text. Thus, a signature can be used to identify a person and to associate the person with the content of that document.

- **Electronic Signature**

It is possible to accord the same legal treatment to an electronic signature, if such signature can perform the same function as a conventional signature. This electronic signature is not a written or embossed statement at the end of a document endorsing it. It is not a password to access the document. What it is, is the result of applying encryption to specific information. Countries like Malaysia, Singapore, Germany and several States in the US were early in having enacted specific laws to deal with Electronic Signature. The Indian IT Act not only gives legal validity to electronic signatures but also sets up a public-key infrastructure for asymmetric key encryption digital signatures.

---

40 Ford Motor Credit Co. v. Swarens, 447 S.W. 2d 53 (Ky. 1969)
PRIMARy OR SECONDARy EVIDENCE

If the document is shown to be authentic, the next query for the adducer is to look into whether it constitutes primary evidence\textsuperscript{42} or secondary evidence.\textsuperscript{43} Internet technology, as with computer technology, at every stage of the transaction, transmits only a copy of the data package. There is no original. Primary evidence envisages the existence of a single original, and this is an impossible proposition as regards computer documents. Since the glaring dangers of “manufactured evidence” are inherent in computer documents, and the divisive benchmark between primary and secondary evidence is the issue of original versus copy, presently, computer evidence should not be regarded as primary evidence.\textsuperscript{44}

\textsuperscript{42} The Indian Evidence Act, 1872; Section 62, It only restricts itself to the document in its original form.
\textsuperscript{43} Ibid., Section 63, The common thread running through the different types of secondary evidence throughout sub-sections 1 to 5 are that they are all not the original document, that is, they are all copies.
\textsuperscript{44} However, Indian law has not resolved the issue as to original versus copies. However, in the American case of King v. State ex rel. Murdock Acceptance Corp., 222 So. 2d 393 (Miss., 1969), the issue was whether a printout satisfied the requirement of being an original record. It was held that the printouts were admissible evidence of a permanent record on magnetic tape. This was because of the obvious fact that records stored on magnetic tape were unavailable and useless except by means of printouts.
ADMISSIBILITY OF ELECTRONIC EVIDENCE : CHALLENGES FOR LEGAL FRATERNITY

Due to enormous growth in e-governance throughout the Public & Private Sector, Electronic Evidence have involved into a fundamental pillar of communication, processing and documentation. These various forms of electronic evidence are increasingly being used in both Civil & Criminal Litigations. During trials, Judges are often asked to rule on the admissibility of electronic evidence and it substantially impacts the outcome of civil law suit or conviction/acquittal of the accused. The Court continue to grapple with this new electronic frontier as the unique nature of e-evidence, as well as the ease with which it can be fabricated or falsified, creates hurdle to admissibility not faced with the other evidences. The various categories of electronic evidence such as website data, social network communication, e-mail, SMS/MMS and computer generated documents poses unique problem and challenges for proper authentication and subject to a different set of views.

In the significant judgment Anvar P.V. Versus, P.K. Basheer &Others, the Supreme 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 anti-corruption 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. It was further observed that all these safeguards are taken to ensure the source and

45 MANU/SC/0834/2014

Admissibility of Electronic Evidence- A Legislative Analysis.
by Rishabh Raj, Managing Partner QUADLegal
authenticity, which are the two hallmarks pertaining to electronic records sought to be used as evidence. 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.

In the anti-corruption cases launched by the CBI and anti-corruption/Vigilance agencies of the State, even the original recording which are recorded either in Digital Voice Recorders/mobile phones are not been preserved and thus, once the original recording is destroyed, there cannot be any question of issuing the certificate under Section 65B(4) of the Evidence Act. Therefore in such cases, neither CD/DVD containing such recordings are admissible and cannot be exhibited into evidence nor the oral testimony or expert opinion is admissible and as such, the recording/data in the CD/DVD’s cannot become a sole basis for the conviction.

In the aforesaid Judgment, the Court has held that Section 65B of the Evidence Act being a ‘not 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 65A and 65B of the Evidence Act.

The Constitution Bench of the Supreme Court overruled the judgment laid down in the State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru\(^46\) by the Divisional Bench of the Supreme Court. The court specifically observed that the Judgment of Navjot Sandhu, to the extent, the statement of the law on admissibility of electronic evidence pertaining to electronic record of this Court, does not lay down correct position and required to be overruled.

\(^46\) (2005) 11 SCC 600
Other Relevant Cases

Relying upon the judgment of Anvar P.V. supra, while considering the admissibility of transcription of recorded conversation in a case where the recording has been translated, the Supreme Court 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.

In *Sanjaysinh Ramrao Chavan Vs. Dattatray Gulabrao Phalke*\(^{47}\) the Hon’ble High Court of Delhi, while deciding the charges against accused in a corruption case observed that since audio and video CDs in question are clearly inadmissible in evidence, therefore trial court has erroneously relied upon them to conclude that a strong suspicion arises regarding petitioners criminally conspiring with co-accused to commit the offence in question. Thus, there is no material on the basis of which, it can be reasonably said that there is strong suspicion of the complicity of the petitioners in commission of the offence in question.

In *Ankur Chawla Vs. CBI*\(^{48}\) the Hon’ble High Court of Calcutta while deciding the admissibility of email held that an email downloaded and printed from the email account of the person can be proved by virtue of Section 65B r/w Section 88A of Evidence Act. The testimony of the witness to carry out such procedure to download and print the same is sufficient to prove the electronic communication.

In *Abdul Rahaman Kunji Vs. The State of West Bengal*\(^{49}\) in the recent judgment 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 u/s 65B Evidence Act, the court observed that the secondary electronic evidence without certificate u/s 65B Evidence Act is inadmissible and cannot be looked into by the court for any purpose whatsoever.

---

\(^{47}\) MANU/SC/0040/2015

\(^{48}\) MANU/DE/2923/2014

\(^{49}\) MANU/WB/0828/2014
The admissibility of the secondary electronic evidence has to be adjudged within the parameters of Section 65B of Evidence Act and the proposition of the law settled in the recent judgment of the Apex Court and various other High Courts as discussed above. The proposition is clear and explicit that if the secondary electronic evidence is without a certificate u/s 65B of Evidence Act, it is not admissible and any opinion of the forensic expert and the deposition of the witness in the court of law cannot be looked into by the court.

However, there are few gaps which are still unresolved as what would be the fate of the secondary electronic evidence seized from the accused wherein, the certificate u/s 65B of Evidence Act cannot be taken and the accused cannot be made witness against himself as it would be violative of the Article 19 & 20(3) of the Constitution of India.

“*No person accused of any offence shall be compelled to be witness against himself.*” - Article 20(3) of The Constitution of India
CONCLUSION & SUGGESTIONS

Thus, it has thus been seen that with the increasing impact of technology in everyday life, the production of electronic evidence has become a necessity in most cases to establish the guilt of the accused or the liability of the defendant. The shift in the judicial mindset has occurred mostly in the past twenty years and most legal systems across the world have amended their laws to accommodate such change. Further, when society is largely utilized computers and even investigation seeks help of gadgets which product of modern electronic technology prosecution is need to be armed with latest technological knowledge and basics of admissibility of electronic evidence as well.

The objective, to keep pace with the changing face of globalization, should be to facilitate the use of information and telecommunication technologies not only in the context of E-commerce, but also on a more individual, personal level. Technology is rapidly expanding at speeds too fast for society. The statute drafters should thus be careful in applying strict rules, definitions and interpretations to the subject matter. Yet, the framework must be broad and clear as to its content.

With the enactment of the IT Act, some of our fundamental issues are solved – the law recognizes electronic counterparts of paper documents and signatures, they are admissible in court and may be proved with few barriers such as requirement of originals. This is, however, only the first stage of moving into the secure electronic environment that the Act envisages. We must acknowledge that electronic records are vulnerable to tampering and there is no foolproof way of authentication and the acceptance and reliance on such forms of evidence should be tailored to the needs of each case. Judges ought to exercise careful discretion as to testing the integrity of the data. There must not be any strict method of deciding this, as integrity depends on system of system. 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 digital forensics training needs to be imparted to them so as to crack cyber crimes.50

In India, all electronic records are now considered to be documents, thus making them primary evidence. At the same time, a blanket rule against hearsay has been created in respect

of computer output. These two changes in the stance of the law have created paradigm shifts in the admissibility and relevancy of electronic evidence, albeit certain precautions still being necessary. However, technology has itself provided answers to problems raised by it, and computer forensics ensure that manipulations in electronic evidence show up clearly in the record. Human beings now only need to ensure that electronic evidence being admitted is relevant to the fact in issue and is in accordance with the Constitution and other laws of the land.