ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 12, Iss 01, 2023

ELECTRONIC EVIDENCE AND ITS JUDICIAL APPRECIATION IN INDIA IN THE LIGHT OF DUE PROCESS NORM AND RULE OF LAW

Dr. Pandhare Balasaheb Dashrath*
(Associate Professor & Recognized Ph.D. Research Guide at PES)
AJMVP'S New Law College, Ahmednagar and Modern Law College, Pune affiliated to Savitribai Phule Pune University Pune

1. Introduction

The rapid use of information technology by human beings in every walk of life is inevitable. At the same time it creates a kind of proof of the every act which is done by using one of the several modes of informant technology. This leads to the situation today that all cases either civil or criminal revolve around at least some sort of electronic information which has a potential to sue or to be sued in a court of justice as a proof. It is hard to delete those from the digital age due to the unique scientific technology involved in this phenomenon. One can erase a fingerprint but cannot permanently erase digital foot prints emitted in electronic environment. In this context it is a positive opportunity for the crime investigation agencies to retrieve and collect electronic evidence, preserve it and produce before the court in order to secure convictions on the basis of great evidentiary value possessed by the electronic evidence. This paper seeks to analyze the increased use of information technology due to its importance in almost all sectors of human life. It also decodes the concept of electronic evidence which was not defined under the Indian Evidence Act, 1872 however its meaning was generated from the judgments delivered by the courts. It further attempts to list out the stages of collecting the electronic evidence, the mode and manner in which it is preserved till the trial and ultimately how it is produced before the court. This paper also tries to answer a crucial question that how to establish the authenticity of electronic evidence before courts. The present paper also discusses about the appreciation of electronic evidence and evidentiary value accorded to it by the courts. At the end this article along with concluding remark provides for certain suggestion to be implemented by the agencies dealing in administration of justice in order to enhance the evidentiary vale of electronic evidence.

2. Importance of Information Technology in administration of Justice

Justice delayed is a justice denied this maxim receives a jolt up to some extent due the increasing use of information technology in court procedures. It saves time, expenses and energy.

* Associate Professor at AJMVP'S New Law College, Ahmednagar and Recognized Ph.D. Research Guide at PES Modern Law College, Pune affiliated to Savitribai Phule Pune University Pune.

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 12, Iss 01, 2023

It is more effective and efficient to deliver justice by implementing tools developed through information technology. Some of those tools can be stated as Video Conferencing,[1] issuing process through electronic mail systems[2] and automation in the court system like development of website of each court to make it easily accessible for all stakeholders. By taking into account all these importance Parliament of India enacted Information Technology Act, 2002 and conferred legal recognition on electronic records. In the context of this article due to increasing importance of information technology it is obligatory on the courts to recognize and accept electronic evidence produced by the litigants. In this context it is desirable to discuss the concept of electronic evidence so that one can understand that what electronic or digital material constitute electronic evidence.

3. Concept of Electronic Evidence

As per the norms of drafting statutes prevailing in almost all legal systems the concepts are defined in the interpretation clause created separately in the statute if it is a codified law. In Indian scenario also all concepts are defined under definition or interpretation clause generally under Sec. 2 of the Act. However in case of Indian Evidence Act, 1872 these are defined under Section 3 of the Act. After extensive scrutiny of Section 3 it was revealed that it does not defined the term Electronic Evidence instead it defined the concept of evidence covering only oral and documentary evidence with a mentioned of electronic record inserted by way of an amendment. The second source of legal concepts is General Clauses Act, 1897, wherein Section 3 to 4-A talks about the definition used in different legal statutes. This act is also salient on the concept of evidence as well as electronic evidence. As the term electronic evidence is of a recent origin and is recognized only by Information Technology Act, 2000 it is desirable to look into it. Even this act also does not expressly define the term electronic evidence however it refers the words electronic evidence and electronic form of evidence. In order to trace the concept of electronic evidence certain other concepts requires a mentioned here which will leads towards the decoding of the concept of electronic evidence. These concepts are as under

[1] The State of Maharashtra v. Dr. Praful B. Desai AIR 2003 SC 2053 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 Twentieth Century Fox Film Corporation Vs. NRI Film Production Associates (P) Ltd. (AIR 2003 KANT 148), certain conditions have been laid down for video recording of evidence. Amitabh Bagchi Vs. Ena Bagchi (AIR 2005 Cal 11), the court held that the physical presence of person in Court may not be required for purpose of adducing evidence and the same can be done through medium like video conferencing. Suvarana Musale vs Rahul Musale [2015 (2) Mh.L.J. 801] Petitioner-wife was working in U.S. and has a minor daughter aged 6 years, traveling to India for being present physically was expensive and she may face difficulty in getting leave and hurdles in obtaining VISA. An application for recording evidence through video conferencing was therefore allowed

[2] Central Electricity Regulatory Commission v National Hydroelectric Power Corporation Ltd. & Ors. (2010) 10 SCC 280 See also Dr. Madhav Vishwanath Dawalbhakta v M/s. Bendale Brothers 2018 SCC OnLine Bom 2652, Tata Sons Limited & Ors. v John Doe(s) & Ors 2017 SCC OnLine Del 8335, SBI Cards & Payments Services Pvt. Ltd. v Rohidas Jadhav 2018 SCC OnLine Bom 1262

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 12, Iss 01, 2023

4. Examiner of Electronic Evidence

This provision was added to the Act by way of Amendment in the year 2009 which came into force from 27th October 2009. This amendment added a new chapter i.e. Chapter-XII-A entitled as Examiner of Electronic Evidence. This chapter consists of only one section which enables the central government to notify examiner of electronic evidence in order to provide expert opinion on electronic form of evidence before any court. The section further appended with an explanation which decode further the term electronic form of evidence means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, and digital fax machines. From this explanation an illustrative list of electronic evidence can be gathered and this explanation is to be considered as the express mentioned of the concept of electronic evidence.

4.1 Electronic Record

One another reference to the term electronic record is traced to clause 2 of Sec. 3 of Indian Evidence Act, 1872 as it says that all documents including electronic records produced for the inspection of court such documents are called documentary evidence. This section suggests that electronic evidence is produced for the inspection of court it is to be treated as documentary evidence. However the concept of document as defined under Indian Evidence Act, 1872, Indian Penal Code 1860 and General Clauses Act, 1897 never suggest a reference that document includes electronic record. However an illustration first appended to the definition of document under Section 3 of Indian Evidence Act provided that "A writing is a document" and definition of writing is given under Section 3(65) of General Clauses Act, 1897 states that writing shall be construed as other modes of representing of reproducing words in a visible form, this gives rise to the meaning that an electronic record in a visible form is a writing and thereby a document. Although the word "document" under Sections 61-65 of the Evidence Act, 1872 have not been replaced with electronic documents but for all the practical purposes, it is meant to include 'electronic records' as well. The importance of electronic evidence is such that a previous statement, made by a person and recorded on tape, can be used not only to corroborate the evidence given by the witness in Court but also to contradict the evidence given before the Court, as well as to test the veracity of the witness and also to impeach his impartiality[3]

Further this theory was also supported by Section 4 of Information Technology Act, 2000 which confers legal recognition on electronic record. It provides that, if any information is required in writing, typewritten or in a printed form then such requirement is satisfied if it is made available or rendered in electronic form and accessible so as to be usable for a subsequent reference.

However this definition is not practicable because the term document and illustration writing is given with intent to documents required in writing as to transfer immovable property under transfer of property Act and requires registration of documents as per Indian Registration

[3] Shri N. Sri Rama Reddy Etc vs Shri V. V. Giri ,1971 AIR 1162

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 12, Iss 01, 2023

Act. Second reason is Information Technology Act, 2000 is not applicable to certain documents based transactions such as Negotiable instruments, Trust deeds, Will, Power of Attorney, Sale deed etc. transactions. Therefore one has to look again into Information Technology Act, 2000 itself to trace the term Electronic record. This act not only defines the term electronic record but also makes regulatory provisions in respect of electronic records such as authentication, legal recognition, use, retention, attribution, acknowledgement, and dispatch of electronic records. It also makes provision for secure electronic records. The scope of present article is confined only to the electronic evidence therefore all aspects of electronic records are not discussed herein at length. Section 2(t) of the IT Act, 2000 defines the term electronic record as data, record or data generated, image or sound stored, received, or sent in an electronic form or micro film or computer generated micro fiche.

Therefore the first ingredient of electronic record is data it means representation of information, knowledge, facts, concepts or instructions which are intended to be processed on a computer system or network and stored internally in the memory of computer or printouts. The second ingredient of electronic record is record is image or sound and the qualifier for all ingredients is it must be generated, stored, received or sent in an electronic form or micro film or computer generated micro fiche. The next step to understand the concept of electronic record is electronic form and reason is data as mentioned above must be generated, stored etc. in electronic form.

According to Section 2 (r) of the IT Act, 2000 electronic form means, a platform on which information is generated, received, sent or stored. These platforms are media which is magnetic, optical, computer memory, micro film or computer generated micro fiche or similar device.

After holding a detailed conceptual discourse of electronic evidence one can list out some material from which one can gather electronic evidence. Those materials are e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories, databases, contents of computer memory, computer backups, computer, computer printouts, global positioning system tracks, logs from a hotel electronic door, locks, digital video or audio file etc.

5. Collection and preservation of Electronic Evidence

The most important step in any criminal proceeding is the collection and preservation of evidence. In civil cases it is the responsibility of concern person who wish to submit the evidence in court to collect and preserve the evidence till the stage of evidence could arrived in a particular suit. However in criminal prosecution it is the duty of prosecution to collect the evidence and preserve till the filing of charge sheet before the appropriate court. As it is governed by the provisions of Criminal Procedure Code, 19973 which define investigation is a measure taken by a police officer or any other person authorized by magistrate for collection of evidence. Therefore in order render justice in true manner the prosecution has to take care of the evidence right from the stage of collection to the production before court. Due to the peculiar

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 12, Iss 01, 2023

nature of electronic evidence it become technical for the investigating officer to collect and preserve electronic evidence as it is more voluminous, difficult to destroy, can be modified and duplicated easily. A special training is to be given to the investigation officer so that the evidentiary value of the electronic evidence could be reserved till the trial. Let's observe this phenomenon from the perspectives of judicial decisions where in the collection and preservation of electronic evidence in involved.

The first step in to the investigation of any crime is arrest of a person if a case is cognizable in nature. In case of non-cognizable case no arrest is to be made until authorized by the magistrate. Presuming the offence as cognizable for the purpose of this article after arrest of suspects police gather relevant information from him/her and proceeds to the scene of crime and collect relevant evidence. To enable it the procedure of search and seizure is followed, the concern legislature empowers authorities to conduct search and seizure to collect evidence.

5.1 Collection of Hard Drive

The issue of seizure of hard drive as an electronic record arose in **State of Punjab V Amritsar Beverages Ltd.**[4] Wherein as per the requirement of Section 14 of the Punjab General Sales Tax Act, 1948 Sale Tax Department searched and seized a computer hard disk from the dealers premises. As per Clause 3 of Section 14 after examination the sales tax authority was required to return all documents seized within sixty days. However sales tax department did not return a hard disk on the pretext that it is not a document. The Supreme Court while applying the principle of purposive interpretation held that hard disk is also a document and suggested the course of action to follow while making seizure of hard disk and returning it. It suggested for making copies on a paper of the data stored in a hard disk and to take signature and official seal on the hard copy and furnish a copy to the dealer and or a person concerned. High Court of Delhi in **Dharambir Vs. CBI**[5] observed that the words "document" and "evidence"' in the amended Section 3 the Evidence Act, read with Sections 2(o) and (t) of the IT Act, there can be no doubt that an electronic record is a document, therefore Hard Disk of a computer system is a document.

5.2 Collection of Electronic Mail as Evidence

In **Abdul Rahaman Kunji Vs. The State of West Bengal**[6] 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.

Apart from this while collecting the electronic evidence the investigation authorities shall take care of three important things i.e. firstly the evidence collected by them is not tempered with, secondly The hardware and software used to reading, downloading, interpreting, seeing or storing was functioning according to set standards and there was no deviation or its corruption

[4] 2006 IndLaw SC 391
[5] 148 (2008) DLT 289
[6] MANU/WB/0828/2014

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 12, Iss 01, 2023

and lastly The system used to access such electronic record was secured, and during the particular course of period it was not accessed by any unauthorized person, so as to rule out the possibility of its tampering or malfunctioning

5.3 Collection of CCTV Footage

The investigating authorities should ensure to take following measures while collecting CCTV footage having potential evidence[7]

1. To identify all the video cameras covering the spot of incidence
2. To find out the owner of concern CCTV cameras and issue letter to him about preservation of CCTV footage.
3. To obtain login and passwords from the custodian of the system
4. To record the model of the CCTV system and the number of cameras and other technical details.
5. To verify whether system have video footage and record it after playing on one's cell phone or a camera.
6. To obtain exact specification and memory capacity of the storage device in order to avoid overwriting.
7. To obtain photo graph of the system and its wiring to restore the system at lab.
8. To perform the time-check in order to understand the difference between the system time and real time
9. While converting the footage into standard video format its hash value must be obtained as it will change its metadata.
10. If any decision is which is taken and can be objected on any logic then it must be written down in a chain of custody form.
11. All the cameras and their peripherals should be collected duly labeled, exhibited and entered into a record.
12. The person In-charge of the system must be asked to give a certificate as required under Sec. 65B of the Indian Evidence Act, 1872

5.4 Disclosure of Password Usernames

Every kind of electronic device is protected by the unique password which is known to the person who is having lawful control of such device, in such circumstance it is a challenging task for the authorities to open such device and collect the data having potential evidentiary value. Therefore the question is whether it is obligatory on the person to disclose passwords to the authorities and if they refuse to disclose then how access can be made. In this context it is desirable to study the existing jurisprudence over this issue.

[7] In the book "Electronic Evidence in the Court room", authored by Mr. Yuvraj P. Narvankar, a checklist for the acquisition of the CCTV footage has been suggested and this Court feels that the same can be taken into account and which can be followed in cases involving CCTV footages and the same is extracted hereunder: Checklist for the acquisition of CCTV footage

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 12, Iss 01, 2023

As per Section 139 of the Indian Evidence Act, 1872 a person may be summoned by a court to produce a document and the term document includes electronic record. Password being a key to open electronic record a court after following a due process can order any person to disclose password. Further as per Sec.54-A of the Criminal Procedure Code, 1973 court can subjects any person who is arrested for any crime to identification by any person as the court may deem appropriate, in the context of electronic records establishing identity is equivalent to disclose password of the device. This disclosure can also be ordered under Section 311-A of the Criminal Procedure Code, 1973. It is in the nature of giving specimen signature to establish identity of handwriting. Even voice sample can be ordered by the court in corruption cases to establish the identity of voice. This question was settled by the apex court in **Ritesh Sinha V State of Uttar Pradesh**[8] by relying upon **Sudhir Chaudhary V. State (NCT of Delhi)**[9] the court deeply discuss the issue of testimonial compulsion envisaged under Article 20 (3) and the absence of express provision for collection of voice sample and held that having regard to the existing realities and imminent necessity of present situation magistrate could order the collection of voice sample under section 311-A of Cr.PC. While dealing with testimonial compulsion court held that, the purpose of a voice sample is to facilitate the process of comparing it with a recorded conversation. The voice sample is not a testimony in itself since it only constitutes what was described as "identification data".

In **Mr. Virendra Khanna V. State of Karnataka**[10] the Karnataka High Court decided several questions regarding the disclosure of password by the accused and the measure to be taken by the authorities if password is not given by the accused. The answers given by the court those questions can be listed as under.

1. Investigation officer is having ample powers under the Cr.PC, 1973 to issue direction or make request to the accused or any other person connected with the device to furnish password or other biometrics to open the electronic device.
2. The Court cannot issue any direction unless an application made by the either party to disclose the password. Disclosure of password is the part of investigation hence court should not order it on its own motion.
3. If the accused refuses to furnish a password even after directed by the investigating officer, such officer is free to approach the court to seek necessary directions in the form of search warrant to carry out a search of electronic devices.
4. The order of search warrant can be made in two situations one is emergent circumstances[11] and another is regular ordinary course of investigation[12]

[8] (2019) 8 SCC 1
[9] (2016) 8 SCC 307
[10] Writ Petition No. 11759 of 2022 Decided by High Court of Karnataka At Bengaluru on 12th March 2021
[11] Section 102, 165 of Code of Criminal Procedure, 1973
[12] Ibid Section 91,92,93,94. And Sec.69 (1) of Information Technology Act, 2000

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 12, Iss 01, 2023

5. The data gathered would have to be proved during the course of the trial as done in any other matter
6. By providing of password, passcode or biometrics, there is no oral statement or a written statement being made by the accused, therefore it cannot be said to be testimonial compulsion
7. The responsibility of safeguarding the information or data which could impinge on the privacy of the person will always be that of the investigating officer, if the same is found to have been furnished to any third party the investigation officer would be proceeded against for dereliction of duty or such other delinquency as provided.
8. In the event of the manufacturer and the service provider not facilitating the opening of the smartphone, email account or computer equipment, then the Court on an application being filed in that regard permit the Investigating Officer to hack into the smartphone and/or email account by engaging the service of experts.
9. In the event of the investigating agency is unsuccessful in hacking into the smartphone and or the e-mail account and during the course of such a procedure, if the data on the smartphone and or the e-mail account being destroyed then, the Investigating agency/prosecution would be free to rely upon the notice by which the accused was warned of adverse inference being drawn.

CONCLUSION

After extensive review of the prevailing legal provisions relating to electronic evidence it can be sad that, the entire gamete of electronic evidence is depend upon the judicial decisions delivered by the constitutional courts and manuals prepared by the executive authorities. Therefore a lack of express statutory authority by the Indian legislature is the need of the day. Even the judicial decisions are not reached to the level that it confers a complete clarity over the subject. The existing practice followed by the investigating agencies results into the gross violations of the fundamental rights of the accused such as right to privacy and protection against self -incrimination. In order to avoid these lacunas there must be the express and comprehensive framework in the form of competent sovereign legislation to deal with the issue of electronic evidence. This legislation will definitely comply with the due procedure norm and rule of law as required under the constitutional spirit of India.