IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Challenges to the Admissibility of the Electronic Evidence

Pankaj Padam(Author)

Neha Gadgala (Co-Author)

Abstract

The exposure or emergence of digitalisation has not only affected our daily life but it has affected legal aspects and legal philosophy also. It has become quite difficult to connect with people without the help of technology because technology is playing a major role in our daily lives. Everyone is depending upon technology for work, entertainment, connecting with different people. It is playing a vital role in the field of law. The researcher shall will try to define types of electronic evidence. Also a close look on guidelines of Legality of Electronic evidence shall be drawn along with challenges that Electronic Evidence faces. An elaborative look shall be given along several Case Laws in Relation to electronic evidence. And finally the necessity and importance of Electronic evidence shall be explained briefly.

Introduction:

The exposure or emergence of digitalisation has not only affected our daily life but it has affected legal aspects and legal philosophy also. It has become quite difficult to connect with people without the help of technology because technology is playing a major role in our daily lives. Everyone is depending upon technology for work, entertainment, connecting with different people. It is playing a vital role in the field of law.

"Electronic Evidences" are evidences which are in the form of digital evidences which any party involved in a suit can use at the time of the trial. These evidences are kind of information comprised in the form of electronic media. Electronic evidences are also known as "Digital Evidences".

Electronic evidence is one of the kinds of evidences which are significantly being accepted or admissible in the court of law to decide any case. So other kinds of evidences are Physical evidences, documentary evidences and those documents which comprise testimony, Character Evidence, Hearsay Evidence etc. as follows:

Circumstantial Evidence:

These are a kind of indirect evidences. These evidences always depend upon the series of facts, it is mostly relevant at the workplace of investigation or where investigation is going on related to any case. These evidences also play an important role in a trial.

Direct Evidence:

It is the most important evidence and it becomes direct proof in itself. Basically this can be the testimony of a witness who witnessed a sexual harassment in any place.

Documentary Evidences:

Generally the documentary evidences are in the form of documents which are written in nature for example- letters, wills etc. but sometimes it also includes photos and videos also.
So this is also an important kind of evidence.

Exculpatory Evidence:

Generally these kinds of evidences absolve defendants in criminal cases. Tbyhese evidences are opposite to inculpatory evidences.

Forensic Evidences:

Forensic evidences are very reliable evidences. These are kind of scientific evidences such as DNA and fingerprints etc. they play great role to help in convicting the criminals, and the court of law also rely on the admissibility of these evidences.

Hearsay Evidence:

Hearsay evidence is such evidences which is made by the witness who is not present. These evidences are rarely admissible in the court of law.

Physical Evidences:

Any evidence which is in the tangible form is known as a physical evidence.for example it can be a gun, rope and knife etc. generally they are known as Real Evidences.

Testimonial Evidences:

Testimony evidence can be in written or in oral form usually given by the witness under oath.

What is mean by Electronic Evidence?

Here we are dealing with Electronic form of Evidences. These evidences are also known as Digital Evidence, Electronic Evidence and "Computer Evidence". Digital or Electronic evidences are meant to be those evidences I which the information which is of probative value is transmitted or stored. The parties to case use these evidence in the court of law in their trial.

What are the Guidelines for handling electronic or digital evidence?

A plethora of projects and a large number of guidelines have been made for handling and preserving electronic evidence or digital evidence. So here some guidelines have been given for handling these types of evidences as follows:

1. Identifying Electronic Evidence
2. Gathering Electronic Evidence
3. Preserving Electronic Evidence
4. Storing and Transporting Electronic Evidence

1. Identifying Electronic Evidences:

This is one of the important guideline to handle electronic evidence. Since we know that electronic evidences are quite admissible in the court of law, so an investigation is required to be done of all electronic evidences which are going to be used in the trial between the parties in the court of law. So identification of electronic evidence is tremendously necessary.

2. Gathering Electronic Evidences:

When it becomes necessary that the evidences that are collected are to be gathered in the electronic form, then some important guidelines must be made for securing and handling electronic evidences. For example the tempering with electronic evidences should not be allowed except the electronic evidence specialists. Because the important data stored in electronic form of evidences could be lost just by a small mistake.

If a copy of the original form is being made, even then the original should also be kept along with the copy of that original form. So electronic evidences specialists are required to gather such kinds of evidences properly. Basically means if copying of an image is being done, the original image should not be altered.

It is quite important that no one should be allowed to disturb electronic evidences, because data is stored mostly in computers in this form of evidences, so the whole data can be erased in seconds.

3. Preservation of electronic evidences:

Electronic Evidences are those evidences which have some probative value in it. So once the information is gathered in electronic or digital form, an electronic evidence specialist should store the data of any floppy or other storage devices in a storage device itself.

An authentic copy should also be made by that specialist, and once the copy of all the data has been made in electronic form, it should be proved that the copy of that information has not been altered and it is the same as the original one.

So the preservation of electronic evidences is very necessary. Because these kind of evidences are used in both civil and criminal nature of matters in the courts of law.

4. Storing and Transporting Electronic Evidences:

There should be appropriate methods by which all the information stored in electronic form going to be transported and stored. The computers in the information is stored should be protected from any kind of virus or other defaults and they should be properly working.

Because these kinds of evidences have very great probative values.

The computers should be properly equipped like the modems, hard disk, keyboard etc. should be properly working without any problem. Electronic evidences should be stored in a proper place.

A proper check is need to be maintained when electronic evidences are being transported. No tempering should be allowed with electronic evidences while transportation process is going on. These evidences should be protected from dampness and dust or clay etc.

Challenges to the Electronic Evidences:

So the challenges to the authenticity and admissibility of electronic evidences in the court of law are as follows:

1. First of all the claim regarding the tempering of electronic evidences may be made by the parties in a trial. Since the evidences are stored in electronic form, so parties can also allege that the electronic evidences have been altered or manipulated since they have been taken.

   This is one of the basic challenges to the authenticity of the electronic evidences that the parties and courts are facing nowadays relating to admissibility of electronic evidences in the courts. Because tempering is something which can be easily done by anyone if there are not proper cautions are not being followed. That is why tempering with electronic evidences is one of the major challenge that electronic evidences are facing.
2. The computer program in which the electronic evidences have been framed, its reliability can also be challenged in the court of law. The parties and court can question the reliability of the computer program which has generated the data in electronic form to formulate evidence.

This is also a major challenge to the admissibility of electronic evidences and its admissibility in the court of law.

3. It can also become a major ground of challenge that whether the person who has used his Password, Pin or option of I accept is the same person who has actually carried out the action or performed the actual function.

   So this is an easy ground of challenge which questions the admissibility of the electronic evidence in the court of law. It also raises the question upon the authenticity of an electronic evidence which is going to be used in a trial by the parties.

4. The author, who has been responsible for writing word files or email or an SMS, his identity can also be challenged in lieu of the electronic evidences. The ground of challenge in this perspective can be whether the author himself or herself has written that particular word file or email or an SMS.

   It can become a great challenge if sufficient evidence has not been found to show the nexus or connection between the original evidence and the person who has written those things. So the identity of the author can also be questioned in relation to the electronic evidences.

5. Social media websites and authentication of information available on them is itself a major ground of challenge of admissibility of the electronic evidence. Firstly, on social media websites, it is not necessary to prove one's identity to operate particular account. People are using fake accounts on social websites. So it would become difficult to judge or identify author.

   Secondly, it could be difficult to identify the original author of the particular document, because the people on social media websites have access to one page and they write to it. So it will become difficult to judge the original author of that document or content.

6. When many people have access to the same device for example mobile phone, it becomes quite difficult to prove that the message or content has been directed to which particular person.

   No doubt it can be agreed that the act was being carried out and also have been recorded but the issue or dispute arises when the party fails to prove that the content or message has been directed to which particular person.

   So this becomes a serious challenge to the admissibility and authenticity of the Electronic Evidence or Digital Evidence.

7. Any evidence which has been gathered from any social networking website might also be questioned in relation to its dependability or reliability.

   Because everyone is depending upon social websites for example- Facebook, Instagram, WhatsApp and Twitter etc. human beings are social animals and they cannot live alone, they have to depend upon each other.

   People nowadays have become so addicted to the social websites and they are much curious about their reputation in online world. They post everything they are doing, to some extent these types of things or activities have become not so appropriate to be admissible in a trial as an evidence.

That is why the reliability of evidences gathered from social websites can be questioned or their admissibility and authenticity can be challenged in the court of law in an ongoing trial between the parties.

8. The next ground of challenge to the electronic evidence can be data on the local Networks. If many computers are connected with each other on a same network it could be quiet difficult to know that the action has arisen on which computer and at what time.

   So the data on local data networks is a major ground of challenge on the admissibility of electronic evidence and it put a check on the authenticity of the Digital Evidence or Electronic Evidence.

9. The next ground of challenge is the data available on the internet. Sometimes it can be differ from devices to devices like data from a remote computer, the computer of an investigator.

   So such process can create hurdles in the way of admissibility and authenticity of Electronic Evidence or Digital Evidence.

10. When data is constantly getting updated on the for example transactional data bases, and those websites which are consistently being updated. This is a major ground of challenge on the admissibility of the Electronic Evidence. Because data on the internet plays a major role in the forming the evidences in electronic form and to store and for their transactions also.

    So at the end the data which is time to time getting updated can be a ground of challenge and it can also be a ground of authenticity of the Electronic Evidence or Digital Evidence.

11. The other ground of challenge to electronic evidence can be mechanical damages, virus etc. these things can destroy whole information stored in electronic devices in seconds if not properly taken care.

    So these are the various grounds of challenges to the admissibility and authenticity of Electronic Evidence or Digital Evidence.

Case laws:

"**State v. Mohd. Afzal and Ors**."[1] In this case it was held that "computer generated electronic records is specified by section 65B of the Indian Evidence Act, 1872". It was also held that electronic evidence are admissible as evidence. If someone challenges the accuracy of a computer evidence or electronic record on the grounds of misuse of system or operating failure or interpolation, then the person challenging it must prove the same beyond reasonable doubt"[2]

[1] (2003) DLT 385, 2003 (71) DRJ 178, 2003 (3) JCC 1669

[2] State v Mohd. Afzal & Ors. Judgement, *Available at* https://indiankanoon.org/doc/1031426/ (Visited on March, 18, 2019)

"**Anvar PV v. PK Basheer**"[3], In this particular case it was held by the court that "Section 65B of Indian Evidence Act has been inserted by way of an amendment by the information Technology Act, 2000. Inasmuch it is a special provision which governs digital evidence and will override the general provisions with respect to adducing secondary evidence under the Evidence Act"[4].

"**State of Maharashtra v. Dr. Praful B Desai**"[5], it was held in this case by Supreme Court that "video conferencing could be resorted for the purpose of taking evidence of a witness"[5].

"**Jagdeo Singh v The State and Ors.[7]",** it was held by the Hon'ble High Court of Delhi that "while dealing with the admissibility of intercepted telephone call in a CD which were without a certificate u/s 65B Evidence Act, the court [6]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"[7].

"**R.M Malkani v. State of Maharashtra**"[89], it was held in this particular case that "Tape recorded conversation is admissible, provided first the conversation is relevant to the matters in issue, secondly there is identification of the voice and thirdly, the accuracy of the tape recorded conversation is proved by eliminating the possibility of erasing the tape recorder. The tape recorded conversation is therefor, a relevant fact under section 7 of Indian Evidence Act, 1872"[10].

"**Ram Singh and Ors. v Col. Ram Singh**"[1112], It was held in this case that "It will be wrong to deny the law of evidence advantages to be gained by new techniques and new devices. Provided the accuracy of the recording can be proved. Such Evidence should always be regarded with some caution and assessed in the light of all the circumstances of each case. Electronic evidence was held to be admissible subject to safeguards adopted by the court about the authenticity of the same".[13]

[3] AIR 2015 SC 180

[4] Anvar PV v. PK Basheer and Ors. Judgement, *Available at* https://www.casemine.com/judgement/in/5609af58e4b01497114161f4 (visited on March, 18, 2019) [5] (2003) 4 SCC 601

[5] State of Maharashtra v Dr Praful B Desai, Judgement, *Available at* https://indiankanoon.org/doc/560467/ (Visited on March, 18, 2019)

[6] MANU/DE/0376/ 2015

[7] Jagdeo Singh v The State and Ors. Judgement, *Available at* https://indiankanoon.org/doc/35565129/ (Visited on March, 25, 2019)

[8]

[9] AIR 157, 1973 SCR (2) 417

[10] R.M. Malkani v State of Maharashtra, Judgement, *Available at* https://indiankanoon.org/doc/1179783/ (visited on March, 28, 2019)

[11]

[12] AIR, 3 1986 SCR

[13] Ram Singh and Ors. v Col. Ram Singh, Judgement, *Available at* https://indiankanoon.org/doc/22898/ (Visited on March, 28, 2019)

"**Tomaso Bruno and Anr. v. State of Uttar Pradesh**"[14], It was held that "Scientific and Electronic Evidence can be a great help to an investigation agency".[15]

What are the points which are helpful in dealing with Digital Evidence or Electronic Evidence?

There are various points which could become helpful in dealing with the evidences which are in digital form or electronic form. And they can also be helpful in curbing the challenges which electronic evidences are facing in relation to its admissibility and authenticity. Some of these points are as follows:

1. Use of Machine
2. About the user
3. Connection with the internet
4. Deletion of data
5. Investigation authority

1. **Use of Machine:**
   - It must be to the knowledge that where the electronic media or information is stored for example- Floppy Disks, Hard Disks, Pin Drives etc.
   - At what time and at which place the computer was bought. Basically it must be known that whether the computer was new or it was second hand.
   - Who is having access to that particular computer software or hardware
   - There are total how many people who are using that particular computer and for how many number of times

2. **About the user:**
   - There are how many users names and what are the user names on that computer. And what are the different programs that they are using or operating
   - What is the level of experience of using computer of each user
   - If that computer is protected with user name and password, and if yes then what is the user name and password

3. **Deletion of Data:**
   - Is there any programs which have been used to clean the data available on that computer
   - What have been the changes made in the data available on that computer

[14] (2015) 7 SCC 178

[15] Tomaso Bruno and Anr. V. State of Uttar Pradesh, Judgement, *Available at* https://indiankanoon.org/doc/193239104/ (Visited on March, 29, 2019)

4. **Investigation Authority:**

- Who has been the investigation authority in the case and what actions did he take to collect and preserve the data available on the computer and the devices which are involved in that action
- What was the process through which the electronic evidence was collected by the investigating authority
- Identification of all those persons who have control over the digital evidence or electronic evidence after and before it was examined
- Identification of the methods or ways which have been used to collect and store evidence

So these are the some points which can be considered to deal with the evidences in electronic form or digital form. These points can also be helpful to escape from the challenges available to the admissibility of the electronic evidence or digital evidence.

Conclusion:

In the end, the electronic evidences are though admissible in the court of law but they are not free from the challenges that challenge the admissibility and authenticity of the electronic evidence or digital evidence for example- the data available on the social media websites. Tempering with the electronic evidence can also be an issue to the admissibility of the electronic evidence. The reliability of the computer program can also be challenged. So these are the various challenges that are available to the authenticity and admissibility of the Electronic Evidence or Digital Evidence.