SCOPE OF ELECTRONIC EVIDENCE IN INDIA: A COMPARATIVE STUDY (UK, USA & CANADA)

By Shiv N.S.
From KSLU's Law School, Karnataka

INTRODUCTION

In this digital era, we almost cannot live without using digital devices. It helps us to communicate locally and globally. Due to which reliance on electronic means of communication, E-commerce and storage of information digitally is rapidly increasing.[1]It has led to the evolution of laws concerned to information technology and admissibility of electronic evidence both in civil and criminal matters. It is not limited only to computers but also extends to include evidence on telecommunication and multinational communication tools. The e-evidence can be found in e-mails, digital photographs, ATM transaction logs, digital documents, instant message histories, GPS system tracks, digital video and audio files etc., digital evidence are more difficult to destroy, easily modified, easily duplicated, potentially more expressive and more readily available.[2]The definition of digital evidence has three elements. First, it is intended to include all forms of evidence that is created, manipulated or stored in a product that can, in wide sense be considered as computer. Secondly, it aims to include the various forms of devices by which data can be stored or transmitted including analogue devices that produce an output we presently understand. Ideally, this definition will include any form of device. Thirdly, the element restricts the data to information that is relevant to the process by which a dispute, whatever the nature of disagreement, is decided by the adjudicator. This part of the definition includes one aspect of admissibility - relevance only - but does not use 'admissibility' in itself is a deciding criterion, the inadmissibility is well within the authority of the adjudicator. The last criteria, however restricts the definition to those items offered by the parties as part of the fact-finding process.[3]

ORAL EVIDENCE TAKEN BY REMOTE LINK

Oral evidence taken by remote link is considered to be electronic evidence. However pre-recorded oral evidence is not covered under oral evidence taken by remote link. It relates to the oral evidence taken through videoconferencing. It may be carried out by using analogue or digital technical devices to transmit oral evidence. If testimony requires confidentiality, it may be necessary to apply measures or technical solutions to restrict the access to the intelligible form of the secure communication to authorized persons only. Oral evidence has practical difficulties such as economic consideration and procedural difficulties. If a person resides in a different country, it may be more appropriate to question him or her remotely. It is important that judges, professionals, including legal practitioners are well versed with the remote link technology.[4]

[1] Tauseef Ahamad, *Relevancy and Admissibility of Digital Evidence: Comparative Study*, 2 IJMH, Issue I, ISSN: 2581-5369 (2018).
[2] Vivek Dubey, *Admissibility of electronic evidence: An Indian Perspective*, 4 FRACIJ (2017).
[3] Council of Europe, *Electronic evidence in civil and administrative proceedings*, ISBN 978-92-871-8929-5 (JUL 2019).
[4] Supra note 3.

In India, recently Supreme Court issued guidelines permitting videoconferencing for ensuring robust functioning of the judicial system across the country, this is a welcome step. Videoconferencing is not a new thing for the judiciary but it would be for the first time during this COVID 19 pandemic that videoconferencing would connect the bench directly to the bar. Earlier videoconferencing was used in deposition of witness in several cases.[5] Supreme Court guidelines regarding videoconferencing have been issued taking recourse under Art.142 have been of the constitution of India.[6] The provisions passed by invoking this article becomes law of the land and enforceable throughout the country. CJI Sharad Bobde very aptly has said "*This cannot be seen as a temporary issue. Technology is here to stay*". The Supreme Court has held in *State of Maharashtra v. Praful Desai*[7] that the recording of evidence by the way of videoconferencing might be done in cases where the attendance of witness cannot be ensured without delay, expense and inconvenience. On the contrary in the family law case *Santhini v. Vijaya Venkatesh*[8], the Supreme Court held 'Physical presence of both parties in a matrimonial proceeding held in camera is essential as it creates environment of trust, confidentiality, privacy and emotional bond.' As per Chandrachud, J.(dissenting), videoconferencing does not negate the postulates of in-camera proceedings.

In United Kingdom, The Access of Justice Act,1999[9] allows videoconferencing to be used for civil hearings. Criminal case hearings are generally done in courtroom and not via videoconferencing as there exist a chance that the witness could be intimidated from a position of power.

In United States of America videoconferencing is a very common in legal system and is used to conduct both administrative and civil proceedings, as well as pre-trial release and sentence hearing. One argument claims that the use of videoconferencing would be in violation of one's sixth amendment clause[10], where they have a constitutional right to face their accuser. Since the defendant is not able to confront witness in a face to face meeting. The court in *Maryland v. Craig* [11] case decided that confrontation clause that 'Reflects the preference for face to face confrontation trial…a preference that must be occasionally given away to the consideration of public policy'. Both substantive and procedural due process concerns also arises due to the remote and sometimes perceived impersonal nature of videoconferencing proceedings. Such arguments stress that the defendant's physical presence in courtroom is critical for making judgements of his or her credibility and competence, as well as physical and psychological wellbeing as held in *United States v. Algere*[12],2005.

---

[5] *Standard Operation Procedure for Advocates/Litigants for attending urgent matters through videoconferencing*, available at https://min.sci.gov.in/notices-circulars, last visited on 25 JUN 2020.

[6] The Constitution of India, 1949.

[7] *State of Maharashtra v. Praful Desai*, (2013) 4 SCC 601: 2003 SCC(Cri)815.

[8] *Santhini v. Vijaya Venkatesh*, (2018) 1 SCC 1: 1 SCC(Civ)1.

[9] The Access of Justice Act,1999(UK).

[10] United States Constitution, 6th Amendment (1791).

[11] *Maryland v. Craig*, 497 U.S. 836(1990).

[12] *United States v. Algere*, 457 F. Supp.2d 695 (E.D.La.2005).

In Canada, the courts and administrative tribunals have connected to digital proceedings and have concluded that proceedings by way of videoconferencing is not considerably different than proceeding with in person hearing. In *Bradley v. Bradley*[13], the court concluded that proceedings through videoconferencing has fairness and natural justice principles. In *X* (2004)[14] case, counsel for the claimant objected to the Refugee Protection Division proceeding by the way of videoconferencing, he contended that credibility could not be properly assessed. But the court held that videoconference does not substantially differ from a in person hearing.

USE OF ELECTRONIC EVIDENCE

The use of electronic evidence has increased in the past few decades as courts have allowed the use of e-mails, digital photographs, ATM transaction logs, digital and audio files etc., courts should be aware of the importance of electronic data being submitted by the parties as evidence in its original format. If a printout of the electronic evidence is filed, the court may order, at the request of a party or on its own initiative its authenticity, the original of the electronic evidence have significant importance in resolving as issue, provided it is presented in its original format.[15] Most jurisdictions around the world have already expressly provided in their law for the use electronic evidence in legal proceedings. In principle, courts should not deny the legal effect of electronic evidence only because it lacks an advanced, qualified or similarly secured electronic signature. Courts should be aware of the probative value of meta data and the potential consequences of it.[16]

In India sec.65A of the Indian Evidence Act[17] provides that the contents of the electronic evidence records may be provided in accordance with the provisions of sec.65B of the Act which provides that notwithstanding anything contained in the Act, any information contained in electronic record, whether it be the contents of document or communication printed on a paper, recorded, copied in optical or magnetic media produced by a computer, it is deemed to be a document and is admissible as evidence without further proof of the production of the original which is subjected to the conditions set out in sec. 65B(2)-(5) of the Act. In *Anvar P.V. v. P.K. Basheer*[18] held that undoubtedly an evidence electronic evidence shall not be admissible as evidence until it has been certified by the expert authority as stipulated under sec.65B of the Evidence Act. On the contrary in the case of *Shafi Mohammad v. State of Himachal Pradesh*[19] observed that a party who is not in possession of a device which has produced an electronic document, cannot be required to produce certificate under sec.65B. It was further held that the requirement to produce certificate can be relaxed by the court. Later on, 14 July 2020 in the case of *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal & Ors.*[20], the 3-judge bench, holding the Shafi Mohammad judgment to be incorrect said, *"the major*

[13] *Bradley v. Bradley*, B.C.J No.2116(1999).
[14] *X* (2004), Can L II 56771(CA IRB).
[15] Supra note 3.
[16] Mason S., *The use of Electronic Evidence in Civil and Administrative proceedings and its effect on the Rules of Evidence and Modes of Proof: A Comparative Study and Analysis*, 14 CDCJ, (27 JUL 2016).
[17] The Indian Evidence Act, 1872.
[18] *Anvar P.V. v. P.K. Basheer and Ors*., 10 SCC 473(2014).
[19] *Shafi Mohammad v. State of Himachal Pradesh*, AIR 2018 SC 714(4).
[20] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal & Ors.*, 2020 SCC OnLine SC 571.

premise of Shafi Mohammad (supra) that such certificate cannot be secured by persons who are not in possession of an electronic device is wholly incorrect. An application can always be made to a Judge for production of such a certificate from the requisite person under Section 65B (4) in cases in which such person refuses to give it."

In United Kingdom, evidence is admissible when it is offered to prove the facts of the case and does not violate the constitution or other statutes.[21] Illegally obtained evidence, obtained in violation of the constitution is inadmissible because it violates privacy, a human right that is protected under the constitution of UK.[22] Only if there is a court order such evidence can be obtained. Evidence may not be admitted in court if it has been obtained without authorization.

In United States, the admission of electronic evidence requires navigating a number of hurdles by the Federal Rules of Evidence. The first hurdle any proffered evidence must leap is authentication.[23] The electronic evidence must not be hearsay.[24] If the electronic evidence is not original but a duplicate then it automatically does not fulfil the original writing requirement. However, it is admissible unless a genuine question is raised about original's authenticity.

In Canada, the Canada Evidence Act[25] and Ontario Evidence Act[26] states that provisions relating to admissibility of electronic records. Both statutes explicitly state that these provisions in Acts do not modify any other rules relating to admissibility such as authentication and best evidence rules of evidence.

COLLECTION AND TRANSMISSION OF ELECTRONIC EVIDENCE

Electronic evidence by its very nature is fragile and can be altered, damaged or destroyed by improper handling or examination. For these reasons, special precautions must be taken to collect this type of evidence. In principle the parties are responsible for the proper collection of evidences. In matters of considerable importance electronic evidence should be collected with the support of IT specialist, Notary services, Judges and professionals. Collection and seizure of electronic evidence may require states to adopt special tools of procedures so that we can ensure the integrity, confidentiality and security of such data.[27] The efficiency of the proceedings is improved when it is possible for electronic evidence to be transmitted in its original format rather than printing and sending it. Facilitation of the transmission of electronic evidence by electronic means can be achieved through implementation of common technical standards and file formats.[28]

In India, the conservative surroundings, substances are put in storage in physical form. However, in the technological era of electronic devices, India has protocol for collection, seizure and transmission of e-evidence. The investigating officer essentially search in a place where it is

[21] Takis Iliadis & Nicolas Santis, *Evidence Law* (2nd edition, 2016) p.66.
[22] *Demetris Shiamishis v. The Police*, 2 CLR 308(2011).
[23] The Federal Rules of Evidence, 1975(sec. 901-902).
[24] The Federal Rules of Evidence, 1975(sec.401-402).
[25] Canada Evidence Act, R.S.C.1985, C-5.
[26] Evidence Act, R.S.O, 1990, C.E.23.
[27] Supra note 3.
[28] Supra note 1.

alleged that crucial electronic devices and data can be found. It is prudent to call computer forensic expert along with the investigation team. It is very significant to safeguard that doubtful suspect is not permissible to trace any electronic evidence.[29] According to sec.166A of CrPC[30] if superior rank officer finds that evidence may be available outside India, any criminal court may issue a letter of request to a court or an authority in that country.

In United Kingdom, the planning and preparation process should be significantly rigorous to identify the level of forensic support that would be required at the scene. Once the initial planning is conducted the preparation for the actual entry takes place, the premises and seizure of e-evidence has been properly authorised in law. Ensuring that rapid and safe entry is arranged. The team is briefed about their tasks and how to perform them. Necessary seizure of tools and equipment to be done. All these activities comply with state and local laws. Transmission of collected e-evidence is done in antistatic bags and antistatic bubble wraps.[31]

In United State, the first responders should also have radio frequency-shielding material such as Faraday isolation bags or aluminium foil to wrap cell phones, other communication devices after they have been sealed and seized, this prevent devices from further receiving any communication which may alter the evidence. The investigation scene should be sealed with no unauthorized entries.[32]

In Canada, the procedure is similar to that of UK, recent case from Supreme Court of Canada has demonstrated that courts will not take privacy interest in digital devices lightly. The SC of Canada has enhanced protection to digital devices as opposed to other items to be searched. In this case *R v. Vu*[33], a computer was found in the house that police were searching with a warrant. But court held that the warrant did not specify electronic devices which is violative of privacy.

RELEVANCE OF ELECTRONIC EVIDENCE

There is a large amount of unnecessary electronic evidence, which can be provided all to easily by a party, will make it difficult or impossible for the court and the other parties to handle it effectively. Therefore, active management of electronic evidence by the court, with a view to restricting its provision to what is strictly required in the case is essential.[34]

In India in the case *R.M. Malkani v. State of Maharashtra*[35], it was held that the tape is primary and direct evidence of what has been said and recorded. The court made it clear

[29] *Collection & Seizure of e-evidence*, available at https://cbi.nic.in/-aboutus/manuals/chapter-18.pdf, last visited on 30 JUN 2020.
[30] The Code of Criminal Procedure, 1973.
[31] Electronic Evidence Guide: A basic guide for the police officers, prosecutors and judges, available at https://au.int/sites/-default/files/newsevents/workingdocuments/34122=wd-annex-4-electronic-evidence-guide-2.0-final-complete.pdf, last visited on 30 JUN 2020.
[32] U.S. Department of Justice, National Institute of Justice report, available at https://www.ncjrs.gov/pdffiles1/njj/219941.pdf, last visited on 30 JUN 2020.
[33] *R v. Vu*, 3 SCR 657(2013).
[34] Supra note 3.
[35] *R.M. Malkani v. State of Maharashtra*, AIR 1973 SC 57.

that electronically recorded conversation is admissible in evidence, if the conversation is relevant to the matter in issue and the voice is identified and the accuracy of the recorded conversation is proved by eliminating the possibility of erasure, addition or manipulation. The court held that a contemporaneous electronic recording of the relevant fact as comparable to a photograph of a relevant incident and is admissible under sec.8 of the Indian Evidence Act.[36]

In United Kingdom, principles related to the effectiveness, usefulness and legitimacy play a relevant role in different legislations. The need for obtaining evidence, the transparency while gathering it and the respect for the freedom of expression are the principles reflected in the Europe. The principles of legitimacy, relevance and the use of such evidence have greater influence.[37]

In United States, while digital evidence exploitation is relatively new tool for law enforcements investigation, law enforcement relies extensively on the digital evidence for important information about both victims and suspects. Due to the potential quantity of digital evidence available, cases where such evidence is lacking are more difficult to develop leads and solve.[38]

In Canada, the common law requirement asks a litigant offering a disputed electronic record into evidence to preface its admissibility. Usually a witness with personal knowledge of the record would fulfil such requirement by recognizing the record and explaining its relevance to the dispute.[39]

STORAGE AND PRESERVATION OF ELECTRONIC EVIDENCE

Storage and preservation for the judicial proceedings. Electronic evidence may be stored by the courts, for example in server backup system, including cloud computing. Cybersecurity should adopt proactive approaches to protect the integrity of electronic evidence from cyberthreats, including damage or unauthorized individuals should not be given access to the electronic evidence. Stored electronic evidence can be associated with standardised metadata describing the context of the creation and the existing links with other electronic evidence. The implementation of international standards for metadata ensures a level of consistency in storage of electronic evidence. As the creation of standardised metadata can be difficult and time consuming, courts may use tools that help generate standardised metadata.[40]

In India, there is no standard procedure for storage and preservation of electronic evidence. Its upto the client and lawyer to take necessary care to preserve the electronic evidence.[41]

[36] Indian Evidence Act, 1872.

[37] Elias Neocleous & Co LLC, *Admissibility of digital evidence in court*, available at https://www.lexology.com/library/detail.pdf last visited on 30 JUN 2020.

[38] Sean E. Goodison et al, *Digital evidence and the U.S. criminal justice system*, available at https://www.ncjrs.gov/pdffiles /nij/grants/248770.pdf last visited on 30 JUN 2020.

[39] Heather MacNeil, *Providing grounds for trust: Developing conceptual requirements for preservation of e-evidence*, Archivaria 50 pp.52-78.

[40] Supra note 3.

[41] S. Murugan, *Electronic Evidence: collection, preservation and appreciation*, available at https://www.nja.nic/2017-18.PPT last visited on 30 JUN 2020.

In United Kingdom, procedural standards do not include any specific procedure to regulate the collection, preservation and presentation of electronic evidence in court.[42]

In United States, for centuries lawyers and their clients have a legal duty to take reasonable steps to preserve potentially relevant evidence from spoliation.[43]

In Canada, Canadian courts opened up the possibility of an independent tort of spoliation. Courts have imposed sanctions to impose an evidentiary presumption that the destroyed evidence would have been unfavourable to the party responsible for destruction.[44]

CONCLUSION

Due to the rapid development of public, private and e-commerce activity electronic evidence has evolved into a fundamental pillar of communication, processing and documentation. Electronic evidences are increasingly been used in judicial proceedings. The court continues to grapple with this new frontier of evidence as it can be fabricated with ease and creates a hurdle for admissibility. The admission of electronic evidence along with advantages can also be complex at the same time. It is relied upon 3 essentials that is authenticity, reliability and integrity.[45]

In India, the law relating to electronic evidence cannot be termed as rigid nor flexible, the law does not really take into account an individual's privacy even while issuing a warrant for search, usually the warrants issued in India are for open search and seizure of evidence whereas in other countries prior to the search the police should provide the Court with the list of things to be seized for issuance of warrant.

The latest landmark 3-judge bench Arjun Panditrao Khotkar's case held the Shafi's case to be incorrect by stating "An application can always be made to a judge for production of such a certificate from the requisite person under sec.65B(4) in cases were the person refuses to give it", now there exist an ambiguity relating to the practical applicability such as what happens when an application seeking directions against the concerned person to file certificate is made, what happens to the progress of the trial? Will the trial abruptly stop till this issue is sorted first? Won't that be a slap on the face to *Bipin Shantilal Panchal v. State of Gujarat & Anr.*[46] which recommended deciding all the objections during the evidence stage at the end of the process in a bid to save time? What happens if a person does not know who the concerned person ought to be?[47] All this is sure to consume a lot of time which would delay securing justice. These questions should be addressed by a larger bench to solve the ambiguity.

In United Kingdom, the law relating to electronic evidence is rigid and takes into account the privacy of an individual seriously, authenticity of digital evidence is

[42] Fredesvinda Insa, *The admissibility of electronic evidence in court*, Journal of digital forensic practice, Vol.1, Issue 4 (2007).
[43] Supra note 37.
[44] Luciana Duratni et al, *Electronic records and law of evidence in Canada*, 70 Archivaria 95(2010) p.97.
[45] Supra note 1.

[46] *Bipin Shantilal Panchal v. State of Gujarat & Anr.* AIR 2001 SC 1158.
[47] Abinav Sekhri, *The Supreme Court, 65-B Certificates, and Electronic Evidence*, available at https://criminallawstudiesnluj.wordpress.com/2020/07/20/the-supreme-court-65-b-certificates-and-electronic-evidence/ last visited on 12 SEP 2020.

assessed vigorously and the whole chain of custody is checked to ensure integrity of the electronic evidence.

In United States, the law relating to electronic evidence is rigid yet flexible, privacy of an individual can be invaded without a warrant. But with only a few specifically established and well defined exceptions, one of which is exigent circumstances which require two conditions "An objectively reasonable basis for concluding that the loss or destruction of evidence is imminent, and that the governmental interest being served by the intuition has been weighed against the individual interest that would be protected if warrant were required."[48]

In Canada, the law relating to electronic evidence is rigid and takes privacy of an individual seriously, same as United Kingdom not surprising as it was earlier a British colony, admissibility of the electronic evidence is only after vigorous scrutiny of the evidence produced and the chain of custody.

*****

[48] Rothstein et al, *Managing discovery of electronic information: A pocket guide for judges*, available at http://federalevidence.com/pdf/2008/09-Sept/FJC_\%20Managing\%20Discovery\%20of\%20Electronic\%20Information. pdf. Last visited on 12 SEP 2020.