A COMPARATIVE ANALYSIS OF ADMISSIBILITY AND RELEVANCE OF ELECTRONIC AND DIGITAL EVIDENCE IN CRIMINAL CASES

Prajwal Vasuki, BA LLB, School of Law, CHRIST (Deemed to be University), Bangalore

ABSTRACT

Evidence may be defined as "any material items or articles of fact that may be submitted to the court as a vehicle to ascertain the truth of any matter of fact alleged under investigation."[1]

Under Indian Law, a defendant is considered to be innocent until proven guilty [2]. If the Court has a reasonable doubt about the defendant's guilt, it may acquit him of all charges. Thus, the prosecution's evidence presented before the Court must establish the defendant's guilt so clearly that they need to be accepted as a fact by any rational, sane person. Relevance and Admissibility are considered as the foundations of Evidence Law. They are the conceptual building blocks of evidentiary scholarship and the practice of trial [3]. This Paper examines the various laws that govern the investigators' access to electronic evidence; In the present age of technological advancements, it has been increasingly noticed that the outcome of Civil and Criminal trials turns to digital evidence. Digital evidence such as e-mails, text messages and social media posts can be most persuasive when issues of intent, motive, and other such aspects are proven[4].

The author will be comparing the Common law and the Indian Law to draw his conclusions, is limiting the Paper to the critical analysis of the due diligence mechanisms present in India by comparing them to the instruments present in the Countries that follow the Common Law system, such as the USA.

Keywords: due diligence, electronic evidence, intent, motive, evidence, hearsay

INTRODUCTION

Historically, the legal system has viewed evidence electronically stored as a form of hearsay evidence. There were no scientific techniques to ascertain or certify that the data stored in the electronic or digital form is factual in historical times. In the present time, with the consistent boom in the Information Technology sector, with the increasing reliance on the electronic means of communications, e-commerce and storage of information in the digital form have caused a need for the law to transform concerning the Information Technology and the Rules of relevance and Admissibility of the same in both civil and criminal matters in the Indian state.

The influence of information technology and computers on society as a whole and the ability to store and amass information in the digital form have necessitated amendments in the Indian legal framework to incorporate the provisions on the appreciation, relevance and Admissibility of digital forms of evidence. Thus, the Information Technology (IT) Act, 2000 was amended to allow digital evidence's Admissibility. With this change in the law, the Indian Courts have developed case laws regarding the reliance on electronic/digital evidence. In various instances, the Judges have also demonstrated perceptiveness towards the intrinsic 'electronic' nature of the evidence, including the Admissibility and the interpretation of the law about the electronic/digital evidence.

Before accepting digital evidence, the Court must ascertain its relevance, veracity, and authenticity and establish if the fact is hearsay or a copy is preferred to the original. Digital Evidence is "information of probative value that is stored or transmitted in the binary form"[5]. Digital evidence includes computer evidence, digital audio, digital video, cell phones, digital fax machines, etc. The digital/electronic evidence can be found in 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 printouts, Global Positioning System tracks, Logs from a hotel's electronic door locks, Digital video or audio files. Digital Evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive and more readily available [6].

THE BEST EVIDENCE RULE

The best evidence rule was that a party must produce the best evidence that the case's nature

would permit. At a certain time in history, this rule was an important part of the law of evidence. The only vestige of this rule that now remains in the modern legal jurisprudence concerns the availability of the original document. The Court, in the modern-day, admits all evidence irrespective of it is best or not. [7]

TYPES OF DIGITAL EVIDENCE

IN THE USA

In the older times, the absence of scientific tests to authenticate the genuineness of the digital evidence led to it being classified as hearsay. However, in modern times, when Digital Evidence has become more prevalent with the global adoption of technology and motivated by the use of technology in committing crimes [8]. As digital evidence gained more prominence, there began a rise of exceptions to the inadmissibility of digital evidence or electronically stored information in the United States. [9]

For Example, the Federal Rules of Evidence 803(6), an exception to the viewing of electronically/digitally stored information as hearsay evidence exists, whereby, thedigital evidence is admissible in the American Court. The US has put in place a criteria for what type of data can be admissible, they are namely, (a) Background evidence (b) foreground evidence. (a) is any electronically or digitally stored information/evidence that have created as part of normal business operations that are used to establish facts and conclusions during an investigation, this includes but is not limited to information retrieved from Network devices such as routers, authentication records such as physical access systems, Data management solutions which in itself includes but is not limited to backups, archives, or classification engines, etc and audit information such as system, application and security logs. (b) is any electronically or digitally stored information/evidence that have been created as a result of objects (human, application, or system), interactions or activities that directly support an investigation or identify perpetrators. This type of evidence includes but is not limited to: Real time monitoring systems, IPS systems, application softwares such as file integrity monitoring, business process systems, address books, electronic communication channels, etc. [10]

IN INDIA

"The definition of evidence as given in the Indian Evidence Act, 1872 covers:

a. the evidence of witness i.e. oral evidence, and

b. documentary evidence whichs includes electronic record produced for the inspection of the court"[11]

Section 65A and 65B were added to the Indian Evidence Act, 1872 to incorporate the Admissibility of the electronic and digital forms of evidence. Traditionally, the fundamental rules of evidence are considered, i.e., direct oral evidence may be used to prove all the facts, except for documentary facts and issues. The hearsay rule suggests that any oral oral evidence that is not direct cannot be relied upon unless it is saved by one of the exceptions as outlined in sections 59 and 60 of the Evidence Act dealing with the hearsay rule.

It is to be noted that the hearsay rule [12] is not as restrictive or straightforward in India, in the case of documentary evidence as it is in the case of oral or physical evidence. This is because it is settled law that oral evidence cannot prove the contents of a document, and the document speaks for itself [13]. Therefore, where a document is absent, oral evidence cannot be given as to its accuracy, and it cannot be compared with the contents of the document. While primary evidence of the document is the document itself, it was realized that there would be situations in which primary evidence may not be available. Thus secondary evidence in the form of certified copies of the document, copies made by mechanical processes and oral accounts of someone who has seen the document, was permitted under section 63 of the Evidence Act to prove the document's contents. Therefore, the provision for allowing secondary evidence dilutes the principles of the hearsay rule and is an attempt to reconcile the difficulties of securing the production of documentary primary evidence where the original is not available [14].

Relevance and Admissibility of Electronic/Digital Evidence in the Indian Courts

In the case of Som Praksh v. State of Delhi, the Supreme Court rightly observed that "in our technological age nothing more primitive can be conceived of than denying discoveries and nothing cruder can retard forensic efficiency than swearing by traditional oral evidence only thereby discouraging the liberal use of scientific aids to prove guilt."[15]

So when Parliament contemplated notice in writing to be given we cannot overlook the fact that Parliament was aware of modern devices and equipment already in vogue."[16] Again in

the case of State v. Mohd. Afzal and Ors. the Supreme Court held that the Computer-generated electronic data is admissible in a trial if proved in the manner as prescribed under section 65B of the Indian Evidence Act. [17]

In the case of State v. Navjyot Sandhu [18], the Court held that merely because a certificate containing the details in sub-Section (4) of Section 65B is not filed in the instant case, does not mean that secondary evidence cannot be given even if the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely Sections 63 & 65 [19]. The Supreme Court's finding in Navjot Sandhu case [20] raised various uncomfortable questions about the integrity of prosecution evidence, especially in trials related to national security or in high-profile cases of political importance. The state's investigation of the Parliament Attacks was shoddy concerning the interception of telephone calls [21].The Indian Evidence Act mandates a special procedure for electronic and digital evidence because the printed copies of information are highly vulnerable to manipulation and abuse.

The Court, in the case of Ratan Tata v. Union of India [22] was another case where a CD containing intercepted telephone calls was introduced in the Supreme Court without following the procedure laid down under section 65B of the Evidence Act [23]. In Anvar vs. Basheer [24], the court held that Section 65B of the Evidence Act has been inserted by way of an amendment by the Information Technology Act, 2000. In as much, 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. In 2007, the United States District Court for Maryland handed down a landmark decision in Lorraine v. Markel [25] that clarified the rules regarding the discovery of electronically stored information. In American federal courts, the law of evidence is set out in the Federal Rules of Evidence. Lorraine held when electronically stored information is offered as evidence, the following tests need to be affirmed for it to be admissible:

1. Is the information relevant.

2. Is it authentic?

3. Is it hearsay?

4. Is it original or, if it is a duplicate, is there admissible secondary evidence to support it; and

5. Does its probative value survive the test of unfair prejudice?

In a small way, Anvar [26] does for India what Lorraine [27] did for US federal courts. In Anvar, the Supreme Court unequivocally returned Indian electronic evidence law to the special procedure created under section 65B of the Evidence Act. It did this by applying the maxim generalia specialibus non derogant ("the general does not detract from the specific"), which is a restatement of the principle lex specialis derogat legi generali ("special law repeals general law"). The Supreme Court held that the provisions of sections 65A and 65B of the Evidence Act created special law that overrides the general law of documentary evidence. Proof of electronic record is a special provision introduced by the IT Act amending various provisions under the Evidence Act [28]. The very caption of Section 65Aof the Evidence Act, read with Sections 59 and 65B is sufficient to hold that the special provisions on evidence relating to electronic record shall be governed by the procedure prescribed under Section 65B of the Evidence Act. That is a complete code in itself. Being a special law, the general law under Sections 63 and 65 has to yield [29].

In the recent judgment, Jagdeo Singh vs. The State and Ors46 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. [30]

CRITICAL ANALYSIS

Strict compliance with section 65B is now mandatory for persons who intend to rely upon e-mails, web sites or any electronic record in a civil or criminal trial before the courts in India. This outlook of the Supreme Court of India is to ensure that the credibility and evidentiary value of electronic evidence is provided for, since the electronic record is more susceptible to tampering and alteration. In its judgment, Kurian J observed, that: '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.4' Therefore, the computer generated electronic record cannot be solely relied upon, because there is a possibility of it being hampered. The Indian Evidence Act could be further amended to rule out any manipulation - at least for the purposes of presuming prima facie authenticity of the evidence of the electronic record - by adding a condition that the record was created in the

usual way by a person who was not a party to the proceedings and the proponent of the record did not control the making of the record. By ensuring that the record was created by a party who was adverse in interest to the proponent of the record, and the record was being used against the adverse party, the risk of the manipulation of the records would be reduced significantly.

This is because, it is argued, no disinterested party would want to certify the authenticity of the record which to his knowledge had been tampered with. The law also needs to creatively address the requirement of the burden being on the proponent to provide testimony as to the author of a document to determine whether there was any manipulation or alteration after the records were created, the reliability of the computer program that generated the records, 20 and whether the records are complete or not. The courts also have to be mindful that data can be easily forged or altered, and section 65B of the Evidence Act does not address these contingencies.

For instance, when forwarding an e-mail, the sender can edit the message. Such alterations are often not detectible by the recipient, and therefore a certificate of a third party to the dispute may not always be a reliable condition to provide for the authenticity of the document. Serious issues have been raised in the digital world due to malpractices such as falsification of information and impersonation, in relation to the authenticity of information relied upon as evidence. It raises queries as to how it is possible to prove the creation and transmission of electronic communication by one party when the party's name as the author of the post could have been inserted by anyone. Perhaps, it may be prudent for the courts or the government to set up a special team of digital evidence specialists who would assist the courts and specifically investigate the authenticity of the electronic records.

The challenges with respect to the admissibility and appreciation of electronic evidence, India still has a long way to go in keeping pace with the developments globally. Although the amendments were introduced to reduce the burden of the proponent of records, they cannot be said to be without limitations. It is clear that India has yet to devise a mechanism for ensuring the veracity of contents of electronic records, which are open to manipulation by any party by obtaining access to the server or space where it is stored.

The admission of electronic evidence along with advantages can also be complex at the same time. It is upon the courts to see that the whether the evidence fulfils the three essential legal

requirements of authenticity, reliability and integrity. After the Anvar v. Basheer case decision,with the Supreme Court laying down the rules for admissibility of electronic evidence it can be expected that the Indian courts will adopt a consistent approach, and will execute all possible safeguards for accepting and appreciating electronic evidence.

Still there is a lacuna in the law in India with regard to the initiation of an investigation against individuals by the law enforcement authorities based on a simple production of a chat or an image, without verifying the relevance or originality of the content of a digital evidence to even start a prima facie case of criminal nature. For example, in the recent episode of the Delhi Boys Locker Room case, the police had arrested the boys said to be involved even before the forensic report was issued by the authority, later when the report revealed that the boys arrested were not the offenders but it was the girl who had complained herself who was responsible for the whole episode. Thus, there is a need for a genuine, expert verification of the digital evidence even before it is considered by the police/ law enforcement to build a prima facie case. This is relevant for the civil cases as well, with regard to consumer protection cases, digital contracts, etc, there needs to be expert verification of the facts and circumstances to ascertain the authenticity of the evidence and its relevancy in the cases before the court. In the opinion of the author, there requires to be an independent authentication and verification authority for the examination of the electronic/digital evidence which shall provide extensive reports with regard to the evidence being real, i.e. organic or created by making use of relevant technologies such as mixing of sounds, photoshop, etc.

CONCLUSION

Even though the digital evidence has been accepted as relevant real evidence by the courts, there is a lacuna in the law in India with regard to the initiation of an investigation against individuals by the law enforcement authorities based on a simple production of a chat or an image, without verifying the relevance or originality of the content of digital evidence to even start a prima facie case of criminal nature. The challenges with respect to the admissibility and appreciation of electronic evidence, India still has a long way to go in keeping pace with the developments globally.

Although the amendments were introduced to reduce the burden of the proponent of records, they cannot be said to be without limitations. Thus, there is a dynamic need for the proposal of a law that needs to stay relevant for the future with the tech-age being in the prime focus for

the following decades, we need to understand that the law needs to dictate the standards that need to be adhered to irrespective of circumstances in the interest of justice equity and good conscience.

ENDNOTES

[1] Ajay BhargavA , Aseem Chaturvedi , Karan Gupta and Shivank Diddi, Use Of Electronic Evidence In Judicial Proceedings, 2020, available at

[2] <https://www.mondaq.com/india/trials-appeals-compensation/944810/use-of-electronic-evidence-in-judicial-proceedings >

[3] 2 Ajay BhargavA , Aseem Chaturvedi , Karan Gupta and Shivank Diddi, Use Of Electronic Evidence In Judicial Proceedings, 2020, available at

[4] https://www.mondaq.com/india/trials-appeals-compensation/944810/use-of-electronic-evidence-in-judicial-proceed

[5] 4 Paras Jain and Others. v State of Rajasthan 2015 SCC OnLine Raj 8331.

[6] 5 Kundan Singh v The State 2015 SCC OnLine Del 13647.

[7] Section 3, Indian Evidence Act, 1872

[8] Article 20(3), Constitution of India, 1950

[9] Paul Roberts, Adrian Zuckerman, (2004). Criminal evidence. Oxford Univ. Press.

[10] James Byrne and Gary Marx, "Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact"(Cahiers Politiestudies, 2011).

[11] Dholam, Swarupa. (2017). Electronic evidence and its challenges Electronic evidence and its challenges.

[12] Prashant Mali, Electronic Evidence/Digital Evidence & Cyber law in India,

[13] May, Richard, and Steven Powles. 2007. Criminal evidence. London: Thomson/Sweet & Maxwell.

[14] Martin Novak, Jonathan Grier, and Daniel Gonzalez, "New Approaches to Digital Evidence Acquisition and Analysis," NIJ Journal 280, January 2019, https://www.nij.gov/journals/280/pages/new-approaches-to-digital-evidence-]acquisition-and-analysis.aspx

[15] Rule 803(6), The Federal Rules of Evidence, 2019 (UNITED STATES OF AMERICA)

[16] Eoghan Casey, Handbook of Digital Forensics and Investigation, 2009, Academic Press.

[17] Section 3, Indian Evidence Act, 1872 (INDIA)

[18] Hearsay evidence is anything said outside a court by a person absent from a trial, but

which is offered by a third person during the trial as evidence. The law excludes hearsay evidence because it is difficult or impossible to determine its truth and accuracy, which is usually achieved through cross examination. Since the person who made the statement and the person to whom it was said cannot be cross examined, a third person's account of it is excluded.

[19] 1Anvar v. Basheer and the New (Old) Law of Electronic Evidence - The Centre for Internet and Society, available at:

http://cisindia.org/internetgovernance/blog/anvarvbasheernewoldlawofelectronicevidence

[20] Section 62, Indian Evidence Act, 1872

[21] Som Prakash vs. State Of Delhi AIR 1974 SC 989, 1974 Cri. LJ 784

[22] SIL Import, USA v vs. Exim Aides Exporters, Bangalore MANU/ SC/0312/1999, (1999) 4 SCC 567

[23] State vs. Mohd. Afzal And Ors (2003) DLT 385, 2003(71)DRJ 17.

[24] State vs. Navjyot Sandhu AIR 2005 SC 3820

[25] Ibid

[26] Ibid

[27] Ibid

[28] Ratan Tata v. Union of India, Writ Petition (Civil) 398 of 2010 before Supreme Court of India.

[29] Ibid

[30] Anvar vs. Basheer AIR 2015 SC 180, MANU/SC/0834/2014