WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

The Role of Digital Evidence in Legal Proceedings: The Indian Perspective

Neelabh Rai Shanker

LL.M. (Criminal Law), Amity University, Noida
neelabhrai1@gmail.com
DOI: https://doi.org/10.55248/gengpi.5.0524.1321

ABSTRACT

This abstract examines how technology and law interact in Indian law, with a particular emphasis on seminal instances involving the admittance of digital evidence and the use of video conferencing for witness testimony. It explores how Indian courts are using new technology while maintaining justice and accuracy in court procedures. The abstract emphasizes the courts' dependence on digital evidence and witness testimony, and it also supports video conferencing as an acceptable method of questioning witnesses. It also emphasizes how crucial it is to protect digital evidence's integrity and guarantee the dependability of video conferencing equipment.

Keywords: Digital evidence, Indian judiciary, Legal proceedings, Video conferencing, Witness testimony, Admissibility, Technological advancements, Fairness.

Introduction

The introduction of computers and the increasing impact of information technology applied to people existence, along with the transition to digital information storage, compelled modifications to Indian laws to enable the management of digital evidence. The IT Act, which was passed by the Indian Parliament in 2000, amended several Indian laws to guarantee the admission of digital evidence. “The IEA, 1872, the IPC, 1860, and the Banker's Book Evidence Act, 1891 were amended by the IT Act, which took inspiration from the UNCITRAL Model Law on Electronic Commerce.” It also acknowledged transactions conducted via other electronic communication methods including electronic data exchange. The Evidence Act has been in place for a long time, but it hasn't stayed that way; instead, it has undergone recurrent revisions to reflect important developments. The Evidence Act has also undergone amendments to allow electronic records to be admitted in addition to traditional paper-based materials.

Evidence

Section 3(a) of the Evidence Act amended the definition of "evidence" to include electronic records. The two main categories of evidence are oral and written. Any document meant for judicial inspection—including electronic records—is now included in the concept of documentary evidence. “Data, record, or data created, picture, or sound saved, received, or communicated in electronic form, microfilm, or computer-generated microfiche” is the definition of 'electronic records' as given in the IT Act, which is adopted here.

Admissions

The Evidence Act's definition of admission (section 17) now includes any statement oral, written, or electronic—that suggests a conclusion about a relevant fact or a fact in dispute. In addition, the Evidence Act now contains a new provision, 22A, that addresses the applicability of oral testimony with reference to electronic record contents. Oral confessions about the contents of electronic records are not considered significant, according to this clause, unless the validity of the electronic records being submitted is being questioned.

Proof must be provided if the assertion is included in an electronic record

When a statement found in an electronic record is being considered, it is covered by Section 39 of the Evidence Act. In these situations, the court is required to provide evidence pertaining to the portion of the electronic record that it determines is necessary to fully comprehend the nature, ramifications, and context of the statement. This clause covers remarks that are made alone, as part of a discussion, as part of a broader statement, or as part of a document included in a book, correspondence series, or other collection of documents.

Admissibility of Digital Evidence

Subsequent to the IT Act's Second Schedule, the Evidence Act saw the addition of new sections 65A and 65B. Section 5 of the Evidence Act limits evidence to facts directly pertinent to the case at hand. Section 136 grants judge the authority to determine the admissibility of such evidence. Section 65A, a recent amendment to the Evidence Act, delineates procedures for verifying the information included in electronic documents in compliance with the rules outlined in Sec. 65B. "According to Section 65B, information contained in electronic records—whether in printed documents, communications, or stored, recorded, or copied using optical or magnetic media generated by a computer (referred to as computer output)—is deemed a document and admissible as evidence without further proof of the original, provided the criteria outlined in Sections 65B(2) to (5) are met. This stands regardless of any provisions within the Evidence Act."

Requirements for the acceptance of digital evidence

According to Section 65B(2), a computer output cannot be admitted as evidence unless certain requirements are met.

(a) The information was produced by the computer when it was being frequently used to store or process data for activities carried out on a regular basis by the person who had legal control over how the computer was used.

(b) As part of the regular course of these activities, throughout this period, data of the kind included in the electronic record, or from which such data is generated, was consistently input into the computer..

(c) The computer was operational for the most of this time, or if it wasn't, any malfunctions or downtime had no effect on the accuracy of the electronic record.

(d) The data entered into the computer during regular operations is reflected in or the source of the information included in the electronic record.

Furthermore, Section 65B (3) states that all computers used for data processing or storage in continuous activities over a predetermined period of time will be considered a single entity for the purposes of this section, regardless of whether they were used simultaneously, consecutively, or in different combinations.

Sec. 65B (4) states that a responsible official's signed authenticity certificate is necessary to meet the aforementioned conditions. This certificate needs to verify the data it contains and state unequivocally that the computer did, in fact, create the electronic record. It should provide the electronic record's name, describe how it was created, list any tools that were utilized, and cover all requirements for entry.

Presumptions with reference to digital evidence

A confirmed fact is not always the same as a relevant and acceptable fact. The judge's job is to evaluate the evidence and determine whether the fact is proven or not. The Evidence Act does, however, include several exceptions were the court may infer certain facts. "Indian Evidence Act", has been amended to include a number of digital evidence presumptions, which are discussed in more detail below.

E-Gazettes

In accordance with Section 81A, "the court will presume, without question, that any electronic record produced from appropriate custody and maintained substantially in compliance with legal requirements is authentic, even if the record purports to be the Official Gazette or any other electronic record required by law."

E-Agreements

"When digital signatures from all parties are added to an electronic document that signifies an agreement," Section 84A creates an assumption that a contract has been created.

Safe digital signatures and electronic documents

According to Section 85B, an electronic record that has a security method applied to it at a certain time is deemed secure until it is verified. Until shown otherwise, the court considers a secure electronic record to have not been changed since the designated time. "According to Sec. 15 of the IT Act, a secure digital signature must meet the following requirements in order to be applied through a predetermined security procedure:

(a) solely owned and managed by the subscriber;

(b) able to uniquely identify the subscriber; and

(c) connected to the relevant electronic record in such a way that any modification to the record renders the digital signature void."

It is assumed that in the case of secure digital signatures, the subscriber attached the signature with the intention of endorsing or approving the electronic document. When it comes to digital signature certificates (as defined by Section 85C), the court will assume that the data stated in the certificate is accurate, with the exception of subscriber information that hasn't been confirmed, provided that the subscriber approved the certificate.

E-Messages

Section 88A creates an assumption that a message entered into the sender's computer for transmission matches the message transmitted by the sender to the intended recipient via an electronic mail server. That being said, this clause makes no assumptions about the sender's identity. It assumes only that the electronic communication itself is valid, not that Whom does the message belong to.

5-year-old electronic records

According to Sec. 90A, "it can be assumed that the digital signature attached to an electronic record belongs to the person whose signature it is or to any person authorized by them when the record is presented from a custody that the court has determined is appropriate for a particular case and is purported to be or proven to be at least five years old. An electronic record in proper custody is assumed to be in its natural environment and to be in the hands of the person it would normally be with. If custody can be demonstrated to have a lawful origin or if the specific circumstances of the case make the origin likely, it is not deemed inappropriate. The electronic version of the Official Gazette is likewise subject to this requirement."

Modifications to the 1891 Banker's Book Evidence Act

The definition of "banker's book" now encompasses the printing of data from a floppy disk, disc, or other electromagnetic device, as outlined in section 2(3). Section 2A mandates the provision of a certificate confirming that a print version of a copy or an entry thereof is indeed a faithful reproduction of the stated entry. This certificate must be issued either by the branch manager or the chief accountant. Furthermore, a certificate from the individual overseeing the computer system is required, detailing the precautions taken by the system and providing a concise description of the system itself.

Amendments to the Indian Penal Code, 1860

In order to address offenses relating to the production of papers, which now include electronic records, a number of offenses were added to the First Schedule of the IT Act, which modified the IPC. These extra offenses consist of:

1. Running away from a court summons in order to avoid having to produce a paper or electronic record (section 172, IPC).
2. Willfully stopping a summons, notice, or proclamation to appear in court with a paper or electronic record (section 173, IPC).
3. Willfully obliging a public official to produce or turn over a paper or electronic record (section 175, IPC).
4. Fabricating false evidence with the intention of using it as evidence in court either adding misleading information to an electronic record or creating a fake electronic record (sections 192 and 193, IPC).
5. Destruction of an electronic record, defined as when someone conceals, destroys, modifies, or renders unreadable any portion of an electronic record with the goal of avoiding its use as evidence (section 204, IPC).
6. Producing a fraudulent electronic document (IPC sections 463 and 465).

Indian courts' recent decisions on digital evidence

1. Search and Seizure

Documents and hard drives from the dealer's location were seized by the Sales Tax Department during a search in the State of Punjab v. Amritsar Beverages Ltd. (2006) 7 SCC 607 case. The computer hard drive was seized in accordance with the guidelines provided in Punjab General Sales Tax Act, 1948, section 14. Section 14(3) of the Act mandates that the authorities restore the confiscated papers to the dealer or the individual in question within a certain amount of time, as long as they give a receipt for the seized material.

2. Evidence recorded on to CD

A member of the State of Haryana's Legislative Assembly was removed by the Speaker for turning against the state in the case of Jagjit Singh v. State of Haryana (2006) 11 SCC 1. Transcripts from a variety of television networks, including Zee News, Aaj Tak, and Haryana News of Punjab Today, were reviewed by the Supreme Court as digital evidence during the hearings. In paragraph 25 of the ruling, Chief Justice Y.K. Sabharwal described the scope of the pertinent digital items.

On June 23, 2004, the original Zee Telefilms CDs were sent in, along with translated transcripts of the channel's interviews and a letter from Zee Telefilms. Similarly, the original proceedings of the Congress legislative party held on June 16, 2004, together with English translations and original CDs from the Haryana News channel were also filed with signatures from three of the four independent members.

Chief Justice Sabharwal stated in paragraphs 26 and 27 that both parties were offered the chance to examine the papers, but they chose not to.

It is significant to remember that the respondent was one of the six independent members of the Haryana Vidhan Sabha that were interviewed for the original CDs, which were presented by the petitioner, from Zee News and Haryana News (Punjab Today Television station). Both television networks officially authenticated these CDs, attesting to their contents and June 14, 2004, New Delhi, recording date. Furthermore, as attested in Ashwani Kumar's evidence (Annexure - P-8), letters from both channels, signed by their designated representatives, verified that the original CDs were sent to Ashwani Kumar with the petitioner's consent. The letters also said that both networks aired the interviews on June 14, 2004. The interview, conducted by journalist Shri Amit Mishra on June 14, 2004, took place at Mr. Ahmed Patel's apartment at 23 Mother Teresa Crescent in Delhi, as confirmed by the certificate from Haryana News (Punjab Today Television Channel). The CLP meeting that was conducted by reporter Mr. Rakesh Gupta on June 16, 2004, in Chandigarh, was likewise verified to have been covered by this same certificate (P-12).

The admissibility of the electronic evidence was decided by the court. It confirmed that the individuals whose voices were captured on the CDs were, in fact, those engaged, upholding the Speaker's reliance on the interview recordings on the CDs. The Speaker's use of digital evidence was deemed appropriate by the Supreme Court, and the judgments reached by Chief Justice Y.K. Sabharwal—explained in paragraph 31—were fully upheld.

3. Admissibility of Intercepted Phone Calls

Following the assault on the Indian Parliament on December 13, 2001, an appeal was filed in the matter of State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600. During this tragic event, five heavily armed assailants breached the Parliament House Complex, resulting in the deaths of nine individuals—eight security officers and one gardener—and injuring sixteen others, thirteen of whom were security personnel. The admissibility and authentication of mobile phone call records emerged as significant issues in this case. The accused raised concerns in their appeal regarding the prosecution's failure to procure the requisite certificate under section 65B(4) of the Evidence Act, asserting that this omission rendered the mobile phone call records unreliable. The Supreme Court, however, ruled that the validity of the call records could only be substantiated through the testimony of a qualified witness familiar with the operation of the computer system during the relevant period and the methodology employed in obtaining the printouts of the call records.

4. Examination of witnesses *via* video conferences

The question at hand in The State of Maharashtra v. Dr. Praful B. Desai (2003) 4 SCC 601 was whether a witness might be questioned virtually. The Supreme Court observed that video conferencing is an example of a technical development that replicates the sense of being physically there by enabling people to see, hear, and speak with others afar. A witness's physical presence is not always necessary for their attendance to be required by law. The Court came to the conclusion that, as video conferencing is an essential component of electronic technologies, it is not prohibited for a witness to be questioned through this medium.

High Court verdicts have mirrored this Supreme Court decision in other cases. “In the cases of Amitabh Bagchi v. Ena Bagchi AIR 2005 Cal 11 and Bodala Murali Krishna v. Bodala Prathima 2007 (2) ALD 72, for example, the Andhra Pradesh High Court stressed the significance of implementing the appropriate safety measures to guarantee the identity of the witness and the precision of the video conferencing equipment. It was also specified that the party choosing video conferencing will be responsible for covering all associated costs.”

Conclusion

Technology's advancements have had a significant influence on the judicial system, especially when it comes to evidence and witness testimony. Indian courts have wrestled with the acceptance of digital evidence and the use of video conferencing for witness examination via seminal decisions like State (NCT of Delhi) v. Navjot Sandhu and The State of Maharashtra v. Dr. Praful B Desai. The Supreme Court upheld Navjot Sandhu's decision, holding that mobile phone call records are not always inadmissible if a certificate under section 65B(4) of the Evidence Act is missing. Rather, the validity of the documents can be established only by the evidence of a qualified witness who is acquainted with the procedure for acquiring them. Similar to this, the Supreme Court supported the use of video conferencing for witness examination in the case of Dr. Praful B. Desai, acknowledging it as a valid and effective technique that complies with contemporary technological improvements. This ruling demonstrates how the courts can keep up with technological advancements while maintaining the standards of justice and accuracy.

Furthermore, the decisions rendered in these instances have established guidelines that other courts have adopted, highlighting how crucial it is to confirm the witness's identity and the reliability of the video conference apparatus. Furthermore, the party that chooses to use video conferencing capabilities is responsible for covering the associated costs. To sum up, these instances demonstrate how the Indian judiciary has come to understand how technology may revolutionize judicial operations. They emphasize how the courts are dedicated to using technology developments to provide justice access while maintaining the honesty and equity of the judicial system.

REFERENCES

1. " A Case Study in Admissibility: The Science of Expert Testimony in Forensic Handwriting Analysis " by Good, Jonathan, and Daniel G. McAuley Jurimetrics [59, 3], 299–328, [2019].
2. "Computer Evidence: Collection and Preservation," by Gary C. Kessler [1992] 357–363, Computers & Security [11, 4].

3. "Digital Evidence and the New Criminal Procedure," by Samuel J. Rothstein, Notre Dame Law Review Notre Dame Law Review [94, 3], 1209–1270, [2019].
4. " Acceptability of evidence produced electronically: A dispute resolution approach" by John Zeleznikow Law [28, 1], 51–66; 2019 Information & Communications Technology Law.
5. " A novel approach to the admission of digital evidence in criminal trials," by J. Schwartz and D. Ball [2017] 21:2–52 in Virginia Journal of Law and Technology.
6. Amanda Zelechoski, "Digital Evidence's Admissibility in Criminal Cases" [2019] 567–612 in American Criminal Law Review [56, 3].
7. "The Emerging Admissibility of Snapchat Evidence," by Alisha Kohn Journal of Information Technology & Privacy Law John Marshall [32, 1], 153–171. [2016].
8. " The US Federal Rules of Evidence and Digital Evidence," by Mary Casey [2005] 281-287 in Digital Investigation [2, 4].
9. " Comparing judicial viewpoints across national borders regarding digital evidence in court " by Rasinger and Sebastian M. Digital Investigation [30], 48–S56, [2019].
10. " An overview of the admissibility of electronically produced evidence in Nigeria " by Oke, Gbenga, and Akinkunmi Akintunde [2019] 719-729 in Computer Law & Security Review [35, 6].
11. " An overview of the legal admissibility of digital evidence in criminal trials," by Darren Quick Digital Investigation [18] [2016], pp. 29–37.