International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

HANDLING OF ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATION: THE ROLE OF LAW ENFORCEMENT AGENCIES IN INDIA

CANDIDATE NAME= VISWANATHA K.N
DESIGNATION= RESEARCH SCHOLAR SUNRISE UNIVERSITY ALWAR
GUIDE NAME = DR. GAYATRI SANJAY PATIL
DESIGNATION= ASSOCIATE PROFESSOR
SUNRISE UNIVERSITY ALWAR RAJASTHAN

ABSTRACT
The research team behind this project hopes their findings will help improve law enforcement agencies' ability to investigate crimes, maintain law and order, and collect important intelligence. In order to maintain and improve one's competence, specialized training facilities are essential. At least one forensics laboratory per 3–4 million people needs to be set up in each district or cluster of districts. Only by having access to such sophisticated forensic laboratories will law enforcement be able to keep up with the rising crime rate in our more urbanized society. Insufficient resources, such as outdated cameras, prevent the police from conducting thorough investigations. There is a severe lack of forensic science labs, and not a single one exists at the district level that can provide prompt help to the investigating Police. It is also well-known that many different states' law enforcement agencies lack forensic and cyber expertise. As a result, law enforcement agencies place less emphasis on scientific and circumstantial evidence and more on testimonial testimony. There is an immediate need to assign considerable importance of CCTV Recordings in light of the Information Technology Act, 2000 for use in the Court of Law in light of the rising prevalence of electronic gadgets in the commission of crimes. For the best possible use of CCTV recordings as evidence in a court of law, the investigating officials must comprehend the science behind them. The judicial system's track record in dealing with electronic evidence has not been very reassuring, and for good reason: protecting the authenticity of digital evidence is difficult. The judiciary often misinterprets evidence because it is not technically savvy enough to understand it. In numerous cases, forensic specialists have also had trouble getting courts to grasp the technical details of the evidence they had gathered.

KEYWORDS: Electronic Evidence, Criminal Investigation, Law Enforcement Agencies, India, CCTV Recordings

INTRODUCTION

In response to a question from the Rajya Sabha (India's Upper House of Parliament) about the number of cases registered in Delhi over the past two years (2017 and 2018) and the number of cases where investigation has been completed, the Minister of State in the Ministry of Home Affairs, Government of India, said that the Cyber Crime Cell of the Delhi Police registered 160 cases in 2018. However, only 26 of those cases had their investigations concluded.

The last few decades have seen a meteoric rise in the common usage of scientific and technological terms. As a result, criminal activity has gotten increasingly complex and technical. The key role players in the

entire criminal investigation process in India, from the collection of evidence until they are produced before the court, are already facing a number of challenges due to the proliferation of cyber-crime and other traditional crimes involving the use of computers and other electronic devices. When the evidence to be gathered is intangible and requires technical skills to investigate further, such as when dealing with electronic records, their job becomes more vital. In some cases, Indian law enforcement has failed to acquire electronic evidence in a legally compliant manner, a critical step in any cyber forensic investigation. When faced with crimes that need a highly sophisticated investigation technique, authorities in cyber-crime cells have often admitted their powerlessness. Officials often have to rely on forensic laboratories or private detectives when a case involves computer forensics. For prompt action in most computer-related matters, it is necessary to quickly retrieve electronic evidences from places like e-mails, websites, chat rooms, databases, etc., as well as information saved in portable electronic devices like laptops, desktops, and mobile phones

In 2015, just 47% of those accused with breaking the Indian Penal Code of 1860 were found guilty One of the main causes for India's low conviction rate of crime is the poor quality of investigation by police, according to the Law Commission of India's 239th Report (2012) When it comes to technologically-based investigations, the police force is woefully unprepared for the challenges of the modern era. Due to a lack of legal expertise, these organizations are unable to perform a thorough inquiry. In light of these gaps, the Second Administrative Reforms Commission (2007) suggested that governments establish dedicated investigation units inside the police force.

After compromising the email account of a company situated in Delhi, India, hackers in Turkey believed to be working for the terrorist group Islamic State stole six crore rupees (about $1.1 million) in December 2015. The inquiry put the Delhi Police in a bind, as they needed to look into things like emails, email accounts, the origin and source of transactions, and more Forensic science laboratories are used by law enforcement authorities to help solve a wide range of criminal cases that call for specialized knowledge. Evidence in the aforementioned cases needed to be quickly retrieved from electronic devices such as laptops, desktops, mobile phones, etc. In many cases, law enforcement organizations lack the resources necessary to effectively deal with emergencies involving electronic evidence. Problems with the admissibility of digital evidence in court and a lower conviction rate can stem back to irregularities in the gathering phase. Without a standard computer forensics technique, investigating authorities may improperly seize or acquire digital evidence.

GROWING IMPORTANCE OF ELECTRONIC EVIDENCE: THE ROLE OF COMPUTER FORENSICS

With the advent of the internet and other forms of digital communication, the field of information technology has seen a dramatic transformation in the twenty-first century, leading to a proliferation of online activities. The misuse of data in cyber space, whether in the form of cyber-crimes or more traditional computer-based crimes,

is a direct result of our growing reliance on electronic means of communication. The significance of electronic evidence has increased greatly as a result of the prevalence of crimes that involve the use of technology in their commission.

Keeping electronic evidence secure throughout an investigation and trial is more challenging than dealing with more traditional forms of evidence like physical documents, as discussed in the previous chapter on electronic evidence. The particular qualities of electronic evidence provide special difficulties in the process of admitting such evidence before a court of law. To begin, it is important to note that electronic or digital evidence cannot be seen by the naked eye, necessitating the adoption of specialized instruments and technology before it can be used in a court of law. Second, the nature of such evidence makes it vulnerable to manipulation. Therefore, it does not conform to the fundamental requirements of admission under the rules of evidence. Thirdly, special equipment and methods are needed to gather, store, and examine the evidence. In other words, the admissibility of electronic evidence in legal proceedings depends on the testimony of experts

Evidence found on digital equipment, such as telecommunication or electronic multimedia devices, may also be considered electronic evidence. They can be found in a wide variety of media, including electronic mail, digital photographs, ATM transaction logs, documents, IM histories, internet browser histories, databases, CDs, DVDs, GPS tracks, digital cameras, memory sticks and memory/SIM cards, personal digital assistants, cell phones, and so on. They are typically larger in size, harder to destroy, more malleable, more reproducible, potentially more expressive, and more widely available

The rise of computer forensics as a field of study reflects the growing importance of digital evidence in securing criminal convictions. To ensure that justice is served in society, forensic science makes it possible to apply physical science principles in court cases. Emerging in recent years, the field of computer forensics examines digital data found on computers and other electronic storage devices. It's the use of computer science and the law together to solve crimes more efficiently. Expert forensic investigators will make copies, or "images," of the original digital evidence, then store it, analyze it, and offer it to the court for a ruling. Since information has been saved on computers, computer forensics (also known as "digital forensics") has been practiced Data science is the study of locating, extracting, and analyzing information stored in digital form. Computer forensics is a relatively new scientific discipline that involves the recovery of inaccessible digital evidence, such as deleted emails, text messages, and files containing documents

In order to ensure the admissibility of evidence gathered via computer systems in court, it is crucial that investigative authorities follow the proper legal procedure when doing so. Regrettably, pre-computer forensics rules were not designed to evaluate the sophistication of computer systems. Poor admissibility of computer-based evidence has often been the result of a lack of proper mechanisms

to appreciate such evidence. The use of computer forensics technologies to gain access to data has been met with intense opposition from privacy advocates who fear it could violate people's fundamental human right to privacy. The proliferation of encryption and anonymization techniques also increases the risk of criminals abusing the internet. The use of computer forensics in criminal investigations may be limited by legal constraints

The courts have repeatedly made references to the use of scientific methods in the investigation of complex crimes, recognizing that conventional physical evidence may not be adequate to establish guilt beyond a reasonable doubt in light of the increasing sophistication of criminal activity in recent years. Case Concerning Tomaso Bruno et al. v. State of Uttar Pradesh , The court remarked that the inquiry process should be permeated by a scientific outlook and the development of relevant information technologies.

FUNDAMENTAL PRINCIPLES OF ELECTRONIC/ DIGITAL EVIDENCE

One of the most important parts of any criminal investigation involving computer-related offenses is the handling of electronic or digital evidence at the crime scene. Recognizing, identifying, seizing, and securing all electronic evidence at the scene, documenting the site of the crime, collecting and preserving the evidence, and lastly packing and transporting the evidence for further forensic investigation are all standard steps in the procedure

The following principles form the basis of any case involving digital or electronic evidence:

For purposes of admissibility in court, it is first and foremost the responsibility of law enforcement to preserve the integrity of any digital evidence they acquire.

When original data stored on a computer or other storage media must be accessed in a hurry, the individual doing so must be qualified to do so and explain the relevant evidence and its implications.

Thirdly, the computer-based evidence must have an audit trail or other related processes that are created and kept. A third party should be able to look at those procedures and come to the same conclusion.

Fourth Principle: The investigating officer is ultimately responsible for upholding the integrity of the rules of evidence and these principles.

Electronic evidence generated by a computer is governed by the same standards as paper documents. This evidence must be produced in a way that clearly demonstrates how it was recovered, with clear documentation of each step. To be admissible in court, evidence must be kept in such a way that it can be reproduced by a third party and used to confirm the authenticity of the results given.

INVESTIGATION OF COMPUTER-RELATED CRIMES AND HANDLING OF ELECTRONIC EVIDENCE

1. Role of Investigation in Criminal Proceedings

In the administration of criminal justice, the role of investigation is crucial. A criminal trial's overarching goal is to ensure that the accused, the victim, and society as a whole are all treated fairly. In a criminal case, the investigation plays a crucial role in determining whether or not

the accused will be found guilty. When investigating a crime, the team has the heavy responsibility of making sure everything is done as thoroughly and accurately as possible so that the charge sheet can be filed and the trial can begin. Jamuna Chaudhary et al. v. State of Bihar, Supreme Court of India decided that the investigators' job is to uncover the whole truth, not just the pieces that will help the prosecution win in court, and not only the pieces that will help the prosecution win. An investigation is defined as "all the proceedings under this Code for the collection of evidence conducted by a police officer or by any person (other than a Magistrate) who is authorized by a Magistrate in this behalf" in Section 2 (h) of the Code of Criminal Procedure, 1973. Definitions in the Criminal Procedure Code are intended to be both comprehensive and flexible.

2. Investigation in Computer-related Crimes

It's common knowledge that crimes can only be committed if the right people are on the scene, the right opportunities present themselves, and no one is keeping an eye on things All three elements necessary for the commission of a crime in cyberspace are made easier in a digital environment, and this is especially true of cyber-crimes and other computer-related crimes. The investigation of crime, especially cybercrime, which involves the use of computers and other electronic means of communication, has benefited and been hindered by technological advancements. One way in which computers have made a significant impact on the ICT sector is by hastening both the collection of data and its processing and dissemination. However, investigators are having trouble accessing encrypted files and sifting through gigabytes of data to retrieve the necessary information because of the interplay of massive amounts of electronic data on cyberspace It goes without saying that the issue of jurisdiction poses significant difficulties for law enforcement and the judicial system when dealing with this type of criminal activity. Identification of the crime, collecting of evidence, preservation of evidence, and guaranteeing the presence of the accused in court are the basic goals of an investigation

Law enforcement is an essential part of any functioning legal system. The process of criminal law, which begins with the investigation of a crime, is said to begin at the moment a case is recorded with the police. Therefore, efficient investigating apparatus is required for the application of criminal legislation. The Code of Criminal Procedure, 1973 is India's major piece of legislation governing the investigation of crimes.

Despite the existence of well-established procedural law to regulate the process of investigation in criminal proceedings, cybercrime and other computer-related crimes have proven more difficult to investigate due to the highly technical nature of the evidence involved. Therefore, the law and the judiciary must adapt to the shifting dynamics of crime.

Col. Ram Singh v. Ram Singh and Others , The three-judge bench of India's highest court recently discussed the necessity of scientific inquiry. For further reading, see R. v. Maqsud Ali. and R. v. Robson to stress that new technologies and gadgets should be allowed to contribute to the law

of evidence if there is a way to show the reliability of the recording. However, such evidence needs to be carefully analyzed or used. The courts in those cases agreed that electronic evidence should be accepted, if certain measures were put in place to ensure its validity.

3. Handling of Electronic Evidence and Law Enforcement Agencies

Forensic knowledge and abilities are essential to the process of crime scene investigation. It goes beyond the simple accumulation or storage of material evidence. It is the most important part of any forensic examination of a probable crime. The foundation of any forensic investigation is the crime scene investigator's ability to recognize the significance of physical evidence. The crime scene can be reconstructed more accurately with the help of a thorough investigation. When investigating crimes committed on a computer, any electronic device that may have been used in the commission of the crime is considered part of the crime scene, regardless of its proximity to the actual act of crime. This includes computers, mobile phones, and other similar devices. The integrity of any potential evidence, whether physical or digital, depends on the methodical processing of both the physical and digital crime scenes. A digital investigation is built on the phases of preparation, collecting, and preservation of digital evidence, including computers and networks. An investigation into a digital crime can be severely hampered by a lack of integrity at the outset, whether it be due to the omission of critical details or the improper preservation of digital evidence. However, even the most thorough plan for dealing with evidence might not account for every possible obstacle or contingency. Therefore, law enforcement agencies that deal with evidence need to have sufficient training and expertise to both follow processes and deal with situations that aren't covered by the rules. In addition, when formulating rules and processes for dealing with computer-related crime scenes, it is crucial to bear in mind that legal concepts relating to such investigation process vary among jurisdictions. The investigation of computer-related crimes has become more standardized thanks to the gradual development of international standards. To guarantee that a certain material, product, process, or service is up to par and serves its intended purpose, a set of guidelines called "standards" is issued. Safety, dependability, and effectiveness (ISO 2009a) are all addressed in this agreement. The formulation of international standards is a major step in achieving cross-border consistency in results and mutual compliance.

CONCLUSION

As the criminal landscape shifted, lawmakers enacted the Information Technology Act in 2000, which was updated in 2008 to account for the rise of cybercrime. Rules pertaining to electronic evidence were included in amendments made to the Indian Evidence Act, 1872 (hence referred to as the Evidence Act) by the same Act. To highlight the importance of forensic science in criminal investigations, Section 45A of the Evidence Act was added to allow the court to weigh the expert opinion of a computer forensic examiner or Examiner of Electronic Evidence on any issue

involving information transmitted or stored in any computer resource or any other electronic or digital form. However, despite the fact that Section 45A of the Evidence Act was added in 2009 and Section 79A of the Information Technology Act, 2000 provided for the notification of Examiner of Electronic Evidence, the Central Government did not make any rules or issue a notification for giving recognition to any agency/laboratory in India as Examiner of Electronic Evidence until 2017, at which point the Government came up with a scheme for the same and six laboratories were recognized as Examiners of Electronic Evidence. The process of determining whether or not electronic evidence is admissible has been hampered by this delay in facilitation.

Traditional methods of acquiring evidence and coercing a confession from suspects persist in the Indian criminal justice system. The police have no idea how to conduct a modern criminal investigation or how to collect scientific data to present a solid case in court. This is why there is still a delay between when a crime is reported, when an arrest is made, and when the accused is brought to justice. Law enforcement agencies and computer forensic experts face difficulties in collecting, preserving, and analyzing electronic evidence, but a different set of difficulties arises when the question of admissibility of such evidence arises before the judiciary, which is typically unfamiliar with the technicalities of computer-related crimes. Various aspects of the admissibility rules under Sections 65A and 65B have been the subject of judicial pronouncements, including the importance of the certificate to be produced before the court along with the evidence as one of the conditions under Section 65B, the qualifications of the certifying agencies for the same, and the possibility of producing electronic evidence as secondary evidence under Section 63. In this study, the author analyzes the difficulties experienced by different parties involved in the criminal justice process when interacting with law enforcement during investigations, the role of Computer Forensic laboratories, the presentation of forensic examination findings by experts, and the judicial approach to admissibility. With their interests in mind, an empirical investigation was carried out.

REFERENCES

- V. NAGESWARA RAO, THE INDIAN EVIDENCE ACT (2015)
- V. P. SRIVASTAV, AN INTRODUCTION TO CYBER CRIME INVESTIGATION (2003)
- VEPA P.SARATHI, LAW OF EVIDENCE (2017)
- W. BLAKE ODGERS. PRINCIPLES AND PRACTICE OF THE LAW OF EVIDENCE (1911)
- WALTER P. SIGNORELLI, CRIMINAL LAW, PROCEDURE, AND EVIDENCE (2011)
- Adam Wilson, *Expert Evidence*, 70 J. CRIM. L. 292 (2006)
- Amitai Etzioni, *Implications of Select New Technologies for Individual Rights and Public Safety*, 15(2) HARV. J. OF L. & TECHN (2002)
- Anne Wallace, *Using Video Link to Take Forensic Evidence: Lessons from an Australian Case Study*, 17(3) INT.

J. OF EVIDENCE & PROOF 221 – 49 (2013)

- Arunima S Kumar, *Cyber Forensics in Kerala*, INT'L J. OF COMP. SCI. & MOBILE COMPUTING 74 (2013)
- Ashwini Vaidialingam, *Authenticating Electronic Evidence: S. 65B, Indian Evidence Act, 1872*, NUJS L. REV. 43 (2015)
- Asou Aminnezhad, *A Survey on Privacy Issues in Digital Forensics*, 1 (4), INT. J.OF CYBER SEC. & DIG. FORENSICS (IJCSDF) 1(4): 311-323
- B. Carrier, DEFINING DIGITAL FORENSIC EXAMINATION AND ANALYSIS TOOLS USING ABSTRACTION LAYERS, 1(4), INT. J. OF DIGITAL EVIDENCE, (2003).
- Barry Chen, *Computer Forensics in Criminal Investigations*, DARTMOUTH UNDERGRAD. J. OF SCI. (2013)
- Carrie Morgan Whitcomb, *A Historical Perspective of Digital Evidence: A Forensic Scientist's View*, 1 (1), INT'L J. OF DIGITAL EVIDENCE (2002)
- Christopher Wall & Jason Paroff, *Cracking the Computer Forensics Mystery*, 17 (7) UTAH BAR JOURNAL (2015)
- Confluence of Digital Evidence and the Law: *On the Forensic Soundness of LiveRemote Digital Evidence Collection*, 2005 UCLA J.L. & Tech. 5
- Dale A. Nance, *Reliability and the Admissibility of Experts*, 34, SETON HALL LAW REVIEW (2003)
- Daniel Capra, *Authenticating Digital Evidence*, FORDHAM LAW ARCHIVE OF SCHOLARSHIP & HISTORY (2017)
- David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STANFORD L.REV. 1357(1996).