LUJ | Legal Upanishad Journal
www.lujournal.com
info@lujournal.com

CYBER FORENSICS AND ELECTRONIC EVIDENCE: CHALLENGES IN ENFORCEMENT & THEIR ADMISSIBILITY IN INDIA

Legal Upanishad Journal

Vol 1 Issue 1 | March 2023 | pp- 15-21

Shudhi Malhotra, 4th Year Law Student, Shri Guru Nanak dev Khalsa College, Delhi

ABSTRACT

In the 21st century, there has been a technological revolution that has taken over India and the rest of the world. Computers are not limited to any established organization or institution, and everyone can use them with one finger. Information technology has simplified almost all human behaviour. The evolution of information technology (IT) has given rise to cyberspace, where the Internet provides all people with equal opportunities to access all information, store data, analyse it, and more—using advanced technology. The growing reliance on electronic communications, e-commerce, and digital storage has clearly changed information technology laws and the admissibility of electronic evidence in both civil and criminal cases in India. The prevalence of computers and the impact of information technology on society have required Indian law to be amended to include a provision for the evaluation of digital evidence, along with the ability to store and accumulate information in digital form. In this paper, the author tries to analyse the concept of Electronic evidence and cyber forensics. The paper focuses on the legal framework regulating digital evidence and also sheds light on the challenges faced in its enforcement in India.

Keywords: Cyber forensics Cyberspace, Data, Electronic Evidence, Information technology.

1. INTRODUCTION

The spread of information technology has left society in a tumultuous state. It now occupies a crucial space in our lives. Technology's never-ending pursuit of advancement has bred a variety of social vices. With the development of modern technology, criminal activity has taken on a new dimension and aspect. We cannot completely rule out the role that such exciting technology will play in our lives, both personally and professionally. We struggle to balance both situations on the scale, though[1].

These sophisticated technologies are being used by criminals to perform crimes that are beyond the comprehension and capability of the average person. A person who is untrained in this art cannot imagine tracing the criminal activity's origins. Cybercrime is a new phrase that has emerged in recent years as a result. It is a crime where a computer (or, more broadly, cyber) is either a tool or a target.

2. CYBER FORENSICS

Cyber forensics is the process of obtaining data as evidence of a crime (using electronic equipment) while adhering to the correct investigative procedures to catch the offender by presenting the evidence to the court. Computer forensics and cyber forensics are similar terms. The basic goal of cyber forensics is to keep the trail of evidence and documentation, going so that it may be determined who committed the crime digitally[2].

2.1 Different Legal Aspects Using Cyber Forensics

Criminal prosecution: In cases when incriminating material is present, use electronic evidence. Criminal prosecution includes examples of child pornography, homicide, financial fraud, drug use, embezzlement, and harassment.

[1] Mohit Kumar, A Detailed Study to Examine Digital Forensics and Cyber Security: Trends and Pattern in India, 5 INT'L J. FORENSIC SCI. (2020)
[2] Prashant Saurabh & Amrit Jay Kumar Roy, Role of Cyber Forensics in Investigation of Cyber Crimes, 4(3) INT'L J. L. MGMT. & HUMAN. 786, 787-789 (2021)

Civil prosecution: Electronic evidence may be used in civil prosecution to compel the production of the company and individual records. Examples include agreements, separation, lawsuits, harassment, and defamation cases.

Cases involving insurance: Insurance firms may be able to successfully refute any claim by supplying electronic records of potential fraud in accident and arson trials.

Companies: They also utilize this evidence to determine whether there are any connections between extortion, fraud, theft of trade secrets, misuse of other internal and external information, and blackmail.

Revenue, enforcement, and regulation: These are terms frequently used to describe post-seizure safeguards for computer assets.

Advisors: They occasionally use skilled cyber forensic investigators to manage and establish sophisticated electronic documents in diverse situations.

2.2 Admissibility of Forensic Evidence in the court of law

- The correctness, reliability, and relevance of forensic evidence are the three fundamental criteria used to determine its admissibility. To be considered admissible in a court of law, the evidence must meet these fundamental requirements[3].

- The court found it challenging to assess the scientific data because it is constantly evolving. Only that evidence will be taken into consideration by the court after a thorough evaluation of its admissibility in the trial.

- The admissibility of evidence is a complex issue in our nation. The admissibility of forensic evidence is constantly subject to the whims of the court; hence its use is never predictable throughout time.

[3] Varsha, Electronic evidence and its admissibility in Indian Courts, B&B ASSOCIATES LLP (Feb. 25, 2023, 8:00 PM), https://bnblegal.com/article/electronic-evidence-and-its-admissibility-in-indian-courts/#:~:text=Digital%20evidence%20plays%20a%20vital,the%20Indian%20Evidence%20Act%2C%201872

- One of the fundamental issues that the law has with the admissibility of forensic evidence is that the Indian Evidence Act makes no mention of the crucial requirements that the court must adhere to while considering forensic evidence.

- The only reference to the act is in section 45, which states that if someone gains expertise in a certain sector, the law should consider it while evaluating their testimony.

- Similar to the previous point, section 51 of the Evidence Act states that evidence will be considered significant if it is provided by a subject-matter expert. Other than this, the legislature has not created any other rules to handle the admissibility of forensic evidence or to evaluate its trustworthiness.

2.4 Challenges for law enforcement

Due to the constant development of new data storage formats, methods, and technologies, cyber forensics has grown more difficult. The legal system is one of the biggest obstacles that investigators and courts must overcome. Electronic records are now acceptable evidence in India following the passage of the Information and Technology Act of 2000[4] and related revisions to the Indian Evidence Act of 1872[5] and the Indian Penal Code of 1860[6]. The jurisdictional question, however, is the main concern. The issue of enforcement arises when a certain act is classified as a crime under the laws of one country but not under the laws of another. Not to mention the assistance and support that must be provided by the other country are also very important.

When carrying out a cyber forensics examination, special precautions should be followed. It must be remembered that gathering proof alone is not sufficient. The agency must determine whether or not the evidence they have collected is admissible in a court of law. They must make

[4] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[5] The Indian Evidence Act, 1872, No. 1, Acts of Parliament, 1872 (India).
[6] The Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India).

arrangements to ensure that the evidence is not tampered with or altered for the sake of admissibility. Evidence must pass a rigorous admissibility test. As a result, they must paint a precise picture of the circumstances leading up to the only conviction of the accused.

3. ELECTRONIC EVIDENCE

Data recorded on computer systems or devices that can be recovered by digital forensic professionals and utilized as admissible evidence in court is known as electronic evidence, also more frequently known as digital evidence. Due to the widespread usage of smartphones and computers, a significant amount of actual data is produced by these tools. As a result, it is possible to anticipate that practically any inquiry will require finding electronic evidence. This digital evidence may be essential to how criminal, civil, and business investigations turn out if it is properly recognized, gathered, and analysed using forensic standards.

3.1 What Factors Determine If Evidence Is Admissible?

To demonstrate the contents of electronic documents by Section 65B's requirements, Section 65A of the Indian Evidence Act[7] has been added. Hence, the process for justifying any documented evidence by way of an electronic record is outlined in Section 65B of the Evidence Act[8].

The four fundamental categories of evidence consist of:

- Evidence that displays or proves a fact at issue in a case is known as demonstrative evidence. Demonstrative evidence, such as a picture of a wrecked car from a collision, demonstrates the effects of the collision on the vehicle.
- Documents that are pertinent to a case's issue are considered documentary evidence. The contract, for instance, would be required proof in a case of contract breach.

[7] The Indian Evidence Act, 1872, § 65A, No. 1, Acts of Parliament, 1872 (India).
[8] The Indian Evidence Act, 1872, § 65B, No. 1, Acts of Parliament, 1872 (India).

- The actual evidence is a tangible item or thing connected to the case. Real evidence would include, for instance, the bullet that was removed from the corpse of a gunshot victim.
- Statements made by a witness who attends court to share their knowledge of the relevant facts are considered testimonial evidence.

3.2 What Legal Rules Apply to Electronic Evidence?

The Fourth Amendment and statutory privacy regulations are the two main legal sources that control the gathering of electronic evidence.

1. The Fourth Amendment serves to safeguard the rights to an individual's privacy by forbidding arbitrary searches and seizures. If law enforcement gets a legitimate search warrant, they are allowed to seize and search a person's computer by the Fourth Amendment. Law enforcement can grab a person's laptop and search it with a valid search warrant[9].

2. Several federal rules that regulate when and how electronic evidence may be gathered are included in statutory privacy laws. The Electronic Communications Privacy Act (ECPA) governs how the information sought by law enforcement may be obtained[10].
    a. Account data saved by network service providers;
    b. Providers of internet services (ISPs).
    c. Telephone providers.
    d. Providers of mobile phone services.
    e. Providers of satellite services.

[9] Varsha, Electronic evidence and its admissibility in Indian Courts, B&B ASSOCIATES LLP (Feb. 25, 2023, 8:00 PM), https://bnblegal.com/article/electronic-evidence-and-its-admissibility-in-indian-courts/#:~:text=Digital%20evidence%20plays%20a%20vital,the%20Indian%20Evidence%20Act%2C%201872

[10] Mohit Kumar, A Detailed Study to Examine Digital Forensics and Cyber Security: Trends and Pattern in India, 5 INT'L J. FORENSIC SCI. (2020)

Moreover, the ECPA places restrictions on the methods that can be used for electronic surveillance. The Patriot Act, which broadens law enforcement's ability to gather electronic evidence, is another federal statute addressing electronic evidence. This law made it easier for law enforcement to access ESI while easing the constraints that were imposed on investigators.

4. SUGGESTIONS

For handling different kinds of criminal investigations, investigative agencies have created standard operating procedures (SOPs). Such methods must follow the fundamental tenets of forensic science to guarantee that evidence is gathered, preserved, and analyzed consistently. Such uniformity is necessary to prevent inadmissibility brought on by mistakes in the process of gathering and preserving the evidence. Also, by using the finest methods for evidence collection and preservation, it will be more likely that two forensic investigators will reach the same findings about the evidence.

5. CONCLUSION

It is crucial to comprehend how law enforcement organizations handle electronic evidence and the challenges they encounter. Police personnel frequently lack the knowledge necessary to conduct a proper search in a computerized environment, particularly in a networked ecosystem. They consequently miss out on important information and hints. Because of this, offenders are exonerated, defeating the main goal of the criminal justice system. Considering the multiple issues that crop up throughout the gathering of evidence, creating an international standard is a time-consuming procedure that requires the utilization of numerous resources. The need for specialized problem standardization frequently doesn't become apparent until after new technology has been made widely accessible[11].

[11] Prashant Saurabh & Amrit Jay Kumar Roy, Role of Cyber Forensics in Investigation of Cyber Crimes, 4(3) INT'L J. L. MGMT. & HUMAN. 786, 794-796 (2021)