THE LAWWAY WITH LAWYERS JOURNAL
VOLUME:-29 ISSUE NO:- 29 , NOVEMBER 26, 2025
ISSN (ONLINE):- 2584-1106
Website: www.the lawway with lawyers.com
Email: thelawwaywithelawyers@gmail.com
Digital Number : 2025-23534643

Authored By :- Ms. Aditi Prasad

THE RISE OF CYBER CRIME - HOW DIGITAL EVIDENCE IS CHANGING INVESTIGATION

Abstract:

The rapid growth of digital technology has led to a significant rise in cybercrime, including offences such as hacking, identity theft, and online fraud. This transformation has altered traditional methods of criminal investigation, making digital evidence—such as emails, electronic records, and online data—central to modern law enforcement. However, the use of digital evidence presents several challenges, including risks of data tampering, privacy concerns, and lack of technical expertise. In India, the admissibility and regulation of electronic evidence are governed by the Information Technology Act, 2000 and Section 65B of the Indian Evidence Act, 1872. This paper examines the role of digital evidence in contemporary investigations and highlights the legal and practical challenges associated with its use.

The digital evidence used in this case creates multiple problems which include data tampering risks, privacy issues and the absence of necessary technical skills. The Indian legal system controls electronic evidence through the Information Technology Act 2000[1]and Section 65B of the Indian Evidence Act[2].

Keywords- Cyber Crime, Digital Evidence, Electronic Evidences, Information Technology Act, 2000, Section 65B.

Introduction:

The digital era has created a situation where more people use the internet which has resulted in increased cyber crime activities that include hacking, phishing and online fraud. Criminals today use advanced technology methods because people depend on technology more than before which makes traditional investigation methods less effective.

[1]Information Technology Act, 2000, https://blog.ipleaders.in/information-technology-act-2000/ (last visited Apr. 4, 2026).

[2] Section 65B, Indian Evidence Act, 1872, https://corporate.cyrilamarchandblogs.com/2020/07/section-65b-of-the indian-evidence-act-1872-requirements-for-admissibility-of-electronic-evidence-revisited-by-the-supreme-court/ (last visited Apr. 4, 2026).

The growth of cyber crime is effected from three main factors which include people having easy access to technology, people not knowing about it and people being able to hide their identity online. Digital evidence has become essential for contemporary investigations because it enables law enforcement to track down and establish proof of criminal activities. Cyber crime has created a new investigation process which requires more technological tools and electronic documents for solving cases.

This paper aims to analyse the growing role of digital evidence in cybercrime investigations and evaluate the adequacy of the existing legal framework in India.

Cyber Crime: Meaning

Cyber crime[3]encompasses any illegal act involving the use of computer systems or networks, either directly or indirectly. In simple terms, Cyber crime exists when people use digital systems to perform illegal activities which include unauthorized entry into systems, stealing data, executing fraud, abusing personal identification and disrupting online services.

The current digital world faces a serious legal and social problem because cyber crime has increased with the growing use of electronic communication, online banking, e-commerce, cloud storage and social media services.

Cybercrime can be broadly classified into cyber-dependent crimes (such as hacking and malware attacks) and cyber-enabled crimes (such as online fraud and identity theft).

Types of Cyber Crime:

1. **Hacking –** Unauthorized access to the network or system to obtain personal data or to change the present information. It is punishable under IT Act Section 66
2. **Phishing –** Fraudulent messages or emails to deceive individuals into disclosing their confidential information including passwords and banking details. (Section 66D IT) 3. **Identity Theft –** Stealing personal data without their permission to commit a fraud or a crime. (Section 66C IT)

-[3] Cyber Crime, https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention (last visited Apr. 4, 2026).

4. **Online Fraud –** Involves cheating individuals by using false website, internet scams and digital payment scams.
5. **Cyber Stalking –** Involves individuals who use social media, emails and other online platforms to stalk and threaten their targets.
6. **Ransomware Attacks –** Uses malicious software to block access to files until payment is made for their release.
7. **Malware Attacks –** Use dangerous software to either destroy systems or enable unauthorized access to them.

Rise of Cyber Crime:

The rise in cyber crime occurs because people use the internet and digital technologies more than before. The growing need for online platforms to handle banking and communication and transaction needs creates additional chances for cyber crimes to occur. Users lack understanding of security risks while organizations possess ineffective protection systems which create security weaknesses. The development of cyber crime occurs because people can easily access technology and authorities fail to enforce laws effectively.

According to NCRB reports, cybercrime cases in India have shown a consistent upward trend, reflecting the growing vulnerability of digital systems.

Concept of Digital Evidences:

Digital evidence[4]refers to any information or data of probative value that exists in electronic form and can be used as evidence in court. It includes all electronic records generated through computers, mobile devices, networks or other digital systems. Digital evidence has become essential for both cyber crime investigations and their subsequent prosecutions.

The concept of digital evidence is based on the idea that every digital activity leaves behind a trace, often referred to as a *"digital footprint*[5]*."* These traces can be collected, preserved and analyzed to reconstruct events, identify suspects, and establish intent. Digital evidence exists as

[4] Digital Evidence, https://blog.ipleaders.in/all-about-digital-evidence/ (last visited Apr. 4, 2026). [5] Digital Footprint, https://www.ibm.com/think/topics/digital-footprint (last visited Apr. 4, 2026).

an intangible asset which requires special tools and methods to begin its process of extraction and examination.

Emails, Chat messages, Digital documents and CCTV Footages are some types included in digital evidences.

Digital evidence is inherently volatile and requires careful handling, preservation, and analysis using specialised forensic tools.

The admissibility of electronic evidence has been clarified in ***Anvar P.V. v. P.K. Basheer***, where the Supreme Court held that compliance with Section 65B of the Indian Evidence Act is mandatory for the admissibility of electronic records.

Changing nature of Investigations:

The progress of digital technology has created new investigation methods which are used to

solve not only criminal investigation but also civil, administrative and corporate investigations. Earlier, investigators used to depend on physical proof and manual methods to solve cases but with the enrolment of modern technology the investigators can now use digital equipment and electronic records for the investigating process

Digital evidence which includes emails, electronic records, financial transactions and online communications is now widely used across various types of investigations. The system enables users to track activities, confirm information and determine who is responsible for events with higher precision and faster output.

The current investigative processes use technology together with data analysis methods to investigate all situations which require evidence collection and fact verification. Modern investigations increasingly rely on digital forensics, data analytics, and cyber intelligence tools.

Information Technology Act, 2000 and Section 65B of Indian Evidence Act:

The Information Technology Act, 2000[6]together with *Section 65B of the Indian Evidence Act, 1872*[7]establishes the fundamental framework for cyber law and digital evidence in India. The IT Act establishes electronic records and digital signatures as legally valid entities and it contains rules for fighting cyber crimes which include hacking and identity theft and online fraud. The framework establishes digital environment accountability through its definition of offenses which have corresponding punishment requirements.

On the other hand, *the Indian Evidence Act Section 65B* functions as an essential legal component because it establishes the rules for presenting electronic evidence in judicial proceedings. The system requires digital evidence to have a certified document which proves its authenticity and reliability.

Both the provisions together exist to establish a connection between legal requirements and technological advancements which enable proper usage of digital evidence during investigations and court cases.

Challenges in Digital Evidences:

Digital evidence has become increasingly important for investigations but its implementation faces multiple difficulties. The main problem arises from electronic evidence which can be altered or deleted through unauthorized access that occurs when proper security measures and preservation techniques are not followed. The process requires both secure protection methods and complete evidence verification to maintain its validity. The absence of required technical skills and equipment to conduct investigations represents another major obstacle.

Digital evidence needs to be collected and secured before analysis because it requires specialized training and dedicated equipment which may not exist in all situations. Investigations create

[6]Information Technology Act, 2000, https://blog.ipleaders.in/information-technology-act-2000/ (last visited Apr. 4, 2026).

[7] Section 65B, Indian Evidence Act, 1872, https://corporate.cyrilamarchandblogs.com/2020/07/section-65b-of-the indian-evidence-act-1872-requirements-for-admissibility-of-electronic-evidence-revisited-by-the-supreme-court/ (last visited Apr. 4, 2026).

privacy and data protection problems when they need to access personal or sensitive information. Cyber crimes create challenges because they cross international boundaries which lead to difficulties in accessing foreign data because of existing legal and procedural restrictions.

Conclusion:

Cyber crime has developed into a new form of threat which continues to increase and develop because technology now controls all parts of human existence. The investigation process now achieves better results because digital evidence provides investigators with a powerful tool which creates more accurate results through advanced technological methods.

The Information Technology Act of 2000 together with Section 65B of the Indian Evidence Act, establishes a legal framework which enables effective control of cyber offenses while securing strong judicial recognition for electronic evidence.

The existing problems which include data manipulation and privacy issues together with technical constraints need to be addressed through the establishment of stronger legal systems,

better public understanding and improved investigative methods. The justice system requires digital evidence as its essential foundation because criminal activities develop alongside technological advancements.

There is a need for specialised cybercrime units, enhanced technical training for investigators, and stronger international cooperation to effectively combat cybercrime. Additionally, continuous updates to legal frameworks are essential to keep pace with technological advancements.

****