Quest Journals
Journal of Education, Arts, Law and Multidisplinary
Volume 15 ~ Issue 4 (Jul. – Aug. 2025) pp: 01-09
ISSN(Online): 2347-2895
www.questjournals.org

Research Paper

Cybercrime and The Role of Forensic Investigation in India in the Digital Era: An Analytical Legal Study

Priya Gupta and Dr. Abhay Chand Mall Visen
Research Scholar, Department of Law, Deen Dayal Upadhyaya Gorakhpur University, Gorakhpur. U.P.
Assistant Professor, Department of Law, Deen Dayal Upadhyaya Gorakhpur University, Gorakhpur. U.P.
Email id: pg.priya90@gmail.com, abhaycmv@gmail.com

Abstract:
With the rise of the information and technology era, the global landscape is confronting a new type of crime known as Cybercrime. Cybercrime is a transformed version of traditional crime that manifests in the digital realm. It is a highly perilous crime that can affect anyone worldwide through its various online forms. The most vulnerable targets of this crime are often children and women. Identifying and apprehending these criminals is quite challenging because the offenses occur in the digital space. This article talks about how after India entered the digital era, it is crucial to establish stringent laws to combat this crime, and cybercriminals can be apprehended and penalized by utilizing forensic techniques to investigate their IP addresses and other identifying data. Through this, the foundation of a healthy and safe digital era can be laid in India.

Keywords: *Cybercrime , Digital crime, Technology crime, Internet crime, Cyber space crime, Forensics Investigation, Investigation by Forensics, Investigation in Digital era by Forensics, Forensics, Technology era, Information and Technology era*

I. INTRODUCTION

As Internet technologies proliferate into everyday life, we come close to realizing new and existing online opportunities. One such opportunity is in Cyber forensics, unique process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally accepted. The American Heritage Dictionary defines forensics as "relating to the use of science or technology in the investigation and establishment of facts or evidence in a court of law". Cyber forensics involves the identification, documentation, and interpretation of computer media for using them as evidence and/or to rebuild the crime scenario. According to computer forensics defined as the process of identifying, collecting, preserving, analysing and presenting the computer-related evidence in a manner that is legally acceptable by court. More recently, computer forensics branched into several overlapping areas, generating various terms such as, digital forensics, data forensics, system forensics, network forensics, email forensics, cyber forensics, forensics analysis, enterprise forensics, proactive forensics etc. Cyber forensics is the investigation of what happened and how. System forensics is performed on standalone machines. Network forensics involves the collection and analysis of network event in order to discover the sources of security attacks. The same process applied on Web is also known as Web forensics. Data forensics major focuses on analysis of volatile and non- volatile data. Proactive forensics is an ongoing forensics and there is an opportunity to actively, and regularly collect potential evidence in an ongoing basis. Email forensics deals with one or more e-mails as evidence in forensic investigation.

1. Meaning

Cyber Crime and **Cyber Forensic Investigation** are two interrelated areas in the field of cybersecurity and digital law enforcement.

1) *Cyber crime encompasses* illegal activities carried out using computers, networks, or digital systems—ranging from hacking, identity theft, and online fraud to cyber terrorism. As digital threats increase in scope and sophistication, the role of cyber forensic investigation becomes critical.[1]

2) *Cyber Forensics involves* the systematic process of identifying, preserving, analyzing, and presenting digital evidence in a manner that is admissible in a court of law. Together, these domains form the backbone of

[1] *available at*: https://en.wikipedia.org/wiki/Cybercrime (last visited on July 2, 2025).

efforts to combat digital offenses, ensure accountability, and uphold justice in the rapidly evolving landscape of cyberspace.[2]

3) Computer forensics which is sometimes referred to as *computer forensic science* - essentially is data recovery with legal compliance guidelines to make the information admissible in legal proceedings. The terms digital forensics and *cyber forensics* are often used as synonyms for computer forensics.

4) Digital forensics starts with the collection of information in a way that maintains its integrity. Investigators then analyze the data or system to determine if it was changed, how it was changed and who made the changes. The use of computer forensics isn't always tied to a crime. The forensic process is also used as part to gather data from a crashed server, failed drive, reformatted operating system (OS) or other situation where a system has unexpectedly stopped working.

2. Connection Between Cyber Crime And Cyber Forensic:

- **Cyber crime** is the offence.
- **Cyber forensics** is the method to **investigate and solve** these offences.
- **Cyber Crime** and **Cyber Forensic Investigation** are two interrelated areas in the field of cybersecurity and digital law enforcement. Cyber crime encompasses illegal activities carried out using computers, networks, or digital systems—ranging from hacking, identity theft, and online fraud to cyber terrorism. As digital threats increase in scope and sophistication, the role of cyber forensic investigation becomes critical.[3]
- **Cyber Forensics** involves the systematic process of identifying, preserving, analyzing, and presenting digital evidence in a manner that is admissible in a court of law. Together, these domains form the backbone of efforts to combat digital offenses, ensure accountability, and uphold justice in the rapidly evolving landscape of cyberspace.[4]

3. Importance of computer or cyber forensics:

In the civil and criminal justice system, computer forensics helps ensure the integrity of digital evidence presented in court cases. As computers and other data-collecting devices are used more frequently in every aspect of life, digital evidence - and the forensic process used to collect, preserve and investigate it - has become more important in solving crimes and other legal issues. The average person never sees much of the information modern devices collect. For instance, the computers in cars continually collect information on when a driver brakes, shifts and changes speed without the driver being aware. However, this information can prove critical in solving a legal matter or a crime, and computer forensics often plays a role in identifying and preserving that information. Digital evidence isn't just useful in solving digital-world crimes, such as data theft, network breaches and illicit online transactions.[5] It's also used to solve physical-world crimes, such as burglary, assault, hit-and-run accidents and murder. Businesses often use a multi-layered data management, data governance and network security strategy to keep proprietary information secure. Having data that's well managed and safe can help streamline the forensic process should that data ever come under investigation.[6]

4. The Objective of Cyber Forensics:

To identify digital evidence for an investigation with the scientific method to draw conclusions. Examples of investigations that use cyber forensics include unlawful use of computers, child pornography, and cyber terrorism. The area of cyber forensics has become prominent field of research because; Forensics systems allow the administrator to diagnose errors, Intrusion detection, systems are necessary in avoiding cyber crimes, Change detection can be possible with proactive forensic.

5. Kinds of Cyber Crime

i. **Illegal Access (Hacking, Cracking)-** The offence which is described as "hacking "usually it refers to unlawful access to a computer system. This is the one of oldest computer-related crimes.[7]

ii. **Cyberbullying and Harassment** - Sending threatening or abusive messages, often targeting women and children.

[2] *available at*: https://www.splunk.com/en_us/blog/learn/cyber-forensics.html (last visited on July 2, 2025).
[3] *available at*: https://www.ebsco.com/research-starters/science/cyber-crimes-and-forensics (last visited on July 2, 2025).
[4] *Ibid.*
[5] *available at*: https://www.ecsbiztech.com/what-is-the-importance-of-cyber-forensics/ (last visited on July 2, 2025).
[6] *Ibid.*
[7] *available at*:https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention (last visited on July 2, 2025).

iii. **Phishing & Identity Theft** - Stealing personal data via fake emails or websites.[8]
iv. **Ransomware Attacks** – Encrypting data and demanding ransom for its release.
v. **Cyber Terrorism** - Using cyberspace to carry out or plan terrorist acts.
vi. **Online Financial Fraud** - Credit card fraud, UPI fraud, e-banking scams.
vii. **Erotic or Adult Pornographic Material (Excluding Child Pornography)-** Sexually-related content was among the first content to be commercially distributed over the Internet, which offers advantages to retailers of erotic and pornographic material including:
viii. **Child Pornography-** The Internet is nowadays being highly used as a medium to sexually abuse the children. The children are viable and soft victim to the cybercrime. Computers and internet having become a necessity of every household, the children have got an easy access to the internet. There is an easy access to the pornographic contents on the internet as well.
ix. **Cyber Stalking-** In general terms, stalking can be termed as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, vandalizing victim's property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim. Cyber stalking means repeated acts of harassment or threatening behavior of the cybercriminal towards the victim by using internet services.[9]

II. HISTORICAL DEVLOPEMENT

1. Cybercrime:

Sussman and Heuston first proposed the term "Cyber Crime" in the year 1995. Cybercrime cannot be described as a single definition, it is best considered as a collection of acts or conducts. These acts are based on the material offence object that affects the computer data or systems. These are the illegal acts where a digital device or information system is a tool or a target or it can be the combination of both. The cybercrime is also known as electronic crimes, computer-related crimes, e-crime, high technology crime, information age crime etc. In simple term we can describe "Cyber Crime" are the offences or crimes that takes place over electronic communications or information systems.[10] These types of crimes are basically the illegal activities in which a computer and a network are involved. Due of the development of the internet, the volumes of the cybercrime activities are also increasing because when committing a crime there is no longer a need for the physical present of the criminal. The unusual characteristic of cybercrime is that the victim and the offender may never come into direct contact. Cybercriminals often opt to operate from countries with nonexistent or weak cybercrime laws in order to reduce the chances of detection and prosecution. There is a myth among the people that cyber- crimes can only be committed over the cyberspace or the internet. New trends in computer crime and cybercrime continued to be discovered in the 21st century. The first decade of the new millennium was dominated by new, highly sophisticated methods of committing crimes, such as "phishing "botnet attacks" and the emerging use of technology that is more difficult for law enforcement to handle and investigate, such as "voice- over-IP (VoIP) communication and "cloud computing It is not only the methods that changed, but also the impact. As offenders became able to automate attacks, the number of offences increased. Countries and regional and international organizations have responded to the growing challenges and given response to cybercrime high priority.[11]

2. Cyber Forensics:

Until the late 1990s, what became known as Cyber forensics was commonly termed 'computer forensics. The first cyber forensic technicians were law enforcement officers who were also computer hobbyists. In the USA in 1984 work began in the FBI Computer Analysis and Response Team (CART). One year later, in the UK, the Metropolitan Police set up a computer crime unit under John Austen within what was then called the Fraud Squad. A major change took place at the beginning of the 1990s. Investigators and technical support operatives within the UK law enforcement agencies, along with outside specialists, realised that cyber forensics (as with other fields) required standard techniques, protocols and procedures. Apart from informal guidelines, these formalisms did not exist but urgently needed to be developed.[12] A series of conferences, initially convened by the Serious Fraud Office and the Inland Revenue, took place at the Police Staff College at Bram shill in 1994 and 1995, during which the modern British cyber forensic methodology was established.

[8] *Ibid.*
[9] *Ibid.*
[10] *available at*: https://arcticwolf.com/resources/blog/decade-of-cybercrime/ (last visited on July 2, 2025).
[11] *Ibid.*
[12] *available at*: https://www.cadosecurity.com/wiki/history-of-digital-forensics-how-it-evolved-over-time (last visited on July 2, 2025).

3. Aim of Cyber Forensics in Cyber Crime Investigation:

Key Aims of Cyber Forensics in Cyber Crime Investigation:

i. **Evidence Collection**-To retrieve digital evidence from electronic devices (computers, mobile phones, servers, etc.) without altering or damaging it and ensures that data is collected using legally approved and technically sound procedures.

ii. **Preservation of Evidence**-To securely preserve the integrity of digital evidence so it remains untampered from the point of seizure to presentation in court.

iii. **Analysis of Data**-To reconstruct the sequence of events leading to the cybercrime, and It includes examining file systems, emails, logs, deleted files, browser history, and more to identify incriminating activity.[13]

iv. **Attribution**-To trace the identity or location of the perpetrators using technical artifacts such as IP addresses, metadata, timestamps, and user profiles.

v. **Legal Admissibility**-To ensure that all digital evidence meets legal standards for admissibility in court (as per the Indian Evidence Act and the IT Act). This includes maintaining a clear chain of custody.

vi. **Supporting Law Enforcement**-To assist police, prosecutors, and judiciary in understanding complex cyber activities and presenting them clearly in legal proceedings.

vii. **Incident Response and Prevention**-Helps in identifying vulnerabilities exploited during the crime and aids in developing better cybersecurity measures to prevent future incidents.[14]

III. RIGHT TO PRIVACY IN CYBER FORENSICS AND CYBER SECURITY

When it comes to the development of Cyber- forensics in India, there is not even a single codified law which deals with this aspect of forensics. This can be due to the fact that technology law is still in its nascent stage in India. There are no regulations which are governing Cyber forensics, so if someone wants to become a cyber-forensic expert, he/she simply has to complete certified course on cyber forensics after finishing his graduation. There is no organization who governs the profession of cyber forensics in India. The primary use of cyber forensics in India is to deliver justice and solve the complicated cases, so it becomes very necessary to make a regulatory body which can check if the people in this profession are actually qualified enough to perform this task. Most of the time, the court of law has to rely on the data and evidences which are gathered from the investigation of digital media. This is due to the fact that most of the people now have access to internet which is also increasing the number of crime involving digital media. For example, if a girl is getting blackmailed on a messenger app, then the sole and most effective way of proving it in the court will be to give evidence, which in such cases, most of the time are in digital forms. Right to privacy is a fundamental right which is guaranteed under the Article 19 of constitution of India. There is a possibility of privacy infringement when the data in electronic forms are given to forensic science analyst. It is rational enough to consider that forensic investigators should have right to access everything which can be helpful in tracking down the accused so that victim can get justice. But most of the time, the investigator not only takes the required information, but also all that confidential information which are not useful for the case or which has nothing to do with the case. They use it for other purpose. So, the risk of exploiting the privacy is always there in case of cyber forensics investigation. This can be similar to controversial Aadhar Card case, When UDIAI used to collect all the information from the citizens of India on the behalf of government. So, in such cases, if any unauthorized person get access to the PIN, password, Username or such other required information because of the forensic science analyst, then it will not be difficult for them to manipulate the account and use it for illegal purposes. So, in a way we can say that if forensic investigators get access to that confidential information which is not required for the case in hand, then it should fall within the ambit of breach of right to privacy. There is a need of some regulatory authority in India which will come up with some code of conduct and give certifications to the forensic investigators. This code also give provisions for the breach of Right of privacy of individuals whose life can get affected because of the confidential information leak. There are already established international organizations which are regulating cyber forensics. Indian government and forensic science department can adopt the code of conduct of those organizations. It will help in speedy investigation process. One such organization which Indian forensic department should adopt is "*The International society of Forensic Computer Examiners" (ISFCE).* It is one of the most reputed organization in the field of cyber Forensics. In order to be a qualified forensic investigator one need to pass the examination and get certificate from the organization. Their certification is recognized in most of the parts of world. The cybercrime is also systematically addressed in the *National treaty of the Council of Europe's convention on crime.* It's a multinational treaty which has addressed the issue of cybercrime along with breach of the Right to Privacy. Moreover, it has also tried to harmonize and balance the step to gather cyber forensic evidences in Cybercrime as well as giving strong code

[13] *available at*: https://www.google.com/search?client=safari&rls=en&q=Aims+of+Cyber+Forensics+in+Cyber+Crime+Investigation&ie=UTF-8&oe=UTF-8 (last visited on July 2, 2025).

[14] *Ibid.*

and regulations for protecting the rights of privacy of individuals. The signatory nations provide for the common ground of laws, principles and procedures along with aiding international cooperation in the investigation of International cyber-crimes. The treaty's main aim is protection of Information technology and to provide for criminal penalties in the following scenario –

- Accessing a computer without authorization or using in excess of authorization.
- Blocking data without authorization
- Interfering with the data without permission
- Interfering with a system without any authority or permission
- Misusing devices.

In addition to the above treaty there are other bilateral treaties also which protect the right of individuals in case of Cyber forensics. Also the framework of the United States- India Cyber Relationships gives detailed cooperative, investigative and security principles which is consistent with various national and international responsibilities too.

IV. INTERNATION PERSPCTIVE

- **Budapest Convention on Cybercrime**:

This is the first international treaty addressing cybercrime, aiming to harmonize national laws, improve investigation techniques and foster cooperation among nations.[15]

- **The UN Cybercrime Treaty:**

Adopted by the United Nations General Assembly in November 2023, this treaty establishes a framework to combat the use of ICT for criminal purposes.[16]

- **Interpol Organization:**

Interpol plays a significant role in facilitating international cooperation on cybercrime, providing a platform for information sharing and coordinating investigations.[17]

V. INDIAN PERSPCTIVE

1. LEGAL PROVISIONS:

India addresses cyber crime and supports cyber forensic investigations through a combination of legislation, law enforcement frameworks, and digital evidence protocols:

i.Legal Provisions on Cyber Crime

1) Information Technology (IT) Act, 2000

This is the main primary law dealing with cyber crime and electronic commerce in India.

- Sec 43: Penalty for damage to computer systems-Hacking, virus attacks, data theft.
- Sec 66: Computer-related offenses- Dishonest or fraudulent actions- Penalty for accessing a computer system without permission
- Sec 66C: Identity theft- Fraudulent Using someone else's digital signature/password, or unique ID without authorization- Punishment for knowingly receiving stolen digital property.[18]
- Sec 66D: Cheating by impersonation Phishing, online fraud- Punishment for dishonest or fraudulent acts using a computer resource.[19]
- Sec 66E: Violation of privacy - Capturing, publishing private images without consent[20]
- Sec 66F: Cyber terrorism -Acts intended to threaten sovereignty, unity, or integrity of India[21]
- Sec 67: Obscene material- Publishing or transmitting obscene content in electronic form[22]
- Sec 67A: Sexually explicit material involving adults pornography
- Sec 67B: Child pornography

[15] *available at*: https://en.wikipedia.org/wiki/Budapest_Convention_on_Cybercrime (last visited on July 2, 2025).

[16] *available at*: https://visionias.in/current-affairs/news-today/2024-12-27/security/the-un-general-assembly adopts-the-convention-against-cybercrime (last visited on July 2, 2025).

[17] *available at*: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/IGOs/21COM1175-SRIUN_UseInformation_CriminalPurposes_complet.pdf (last visited on July 2, 2025).

[18] The Information Technology Act, 2000 (Act 21 of 2000), s. 66 C.

[19] The Information Technology Act, 2000 (Act 21 of 2000), s. 66 D.

[20] The Information Technology Act, 2000 (Act 21 of 2000), s. 66 E.

[21] The Information Technology Act, 2000 (Act 21 of 2000), s. 66 F.

[22] The Information Technology Act, 2000 (Act 21 of 2000), s. 67.

- Sec 69: Powers to intercept, monitor or decrypt information- Allows lawful interception by authorized agencies for national security.
- Sec 70: Protection of critical infrastructure- Declares certain systems as protected
- Sec 72: Breach of confidentiality and privacy- Unauthorized disclosure of information by lawful access- Applies to service providers or individuals handling sensitive data.

2) The Bhartiya Nyaya Sanhita, 2023

Cyber crime is primarily governed under the Information Technology Act, 2000 (IT Act) and also under certain provisions of the Bhartiya Nayaya Sanhita (BNS). Cyber crimes are often prosecuted in conjunction with relevant sections of the BNS:

- Sec 319: Cheating by personation- (e.g., phishing, online fraud)- Used in email/online identity impersonation.
- Sec 318: Cheating and dishonestly inducing delivery of property
- Sec 336(1), 336: Forgery of electronic records
- Sec 356: Cyber defamation
- Sec 75-78, 79: Online harassment of women (e.g., cyberstalking, voyeurism)
- Sec 61: Criminal conspiracy (often used with cyber terrorism cases)

ii.Legal Provisions for Cyber Forensic Investigation

India does not have a dedicated cyber forensic law, but legal backing comes from existing laws such as:

1) IT Act, 2000 (Investigation Powers)

- Section 69: Allows government agencies to monitor, decrypt, or intercept data for investigation.[23]
- Section 79A: Empowers the Central Government to notify certain agencies as Digital Evidence Examiner bodies.

2) The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023

Sec 94: Allows police or courts to demand production of digital documents/evidence.
Sec 95: Deals with obtaining records from telecom companies or ISPs.
Sec 185: Search and seizure of electronic evidence.[24]

3) The Bharatiya Sakshya Adhiniyam (BSA), 2023

Sec 3: Expands the definition of "evidence" to include electronic records.
Sec 62 & 63: Provide procedures for the admissibility of electronic evidence in court. Section 63 certificate is mandatory for digital evidence to be admissible.

2. AMENDMENTS FOR CYBERCRIME INVESTIGATION:

In the era of digital India, a lot of technology and many developments are taken place and many new inventions are still under process. With this increasing technology, the crimes related to technology are also increasing. Many cases are registered under IT Act 2008 and also got amended in 2010. Some of the cases registered are data theft, hacking, unauthorized access, pornography, intellectual property theft, cyber terrorism, viruses and many. Cybercrime becomes a large threat to the business, national security and for the common man. The following are the process of cybercrime investigation methodology.

3. ENFORCEMENT AGENCIES:

- Cyber Crime Cells (State Police & CBI)
- Indian Computer Emergency Response Team (CERT-IN)
- National Cyber Crime Reporting Portal (https://cybercrime.gov.in)
- Ministry of Home Affairs (MHA) – Cyber Forensic Lab (under Cyber Crime Prevention against Women and Children - CCPWC), National Cyber Crime Reporting helpline no. 1930

4. JUDICIAL DECISIONS:

A. Forensic Investigation in India

1) Selvi v. State of Karnataka[25]: Digital forensic techniques must also respect constitutional rights

In this case the was arise that Whether narco-analysis, brain mapping, and polygraph tests violate personal liberty and self-incrimination rights under Article 20(3). Supreme Court of India decided that these techniques cannot be

[23] The Information Technology Act, 2000 (Act 21 of 2000), s. 69.
[24] The Bharatiya Nyaya Suraksha Sanhita, 2023 (Act 46 of 2023), s. 185.
[25] (2010) 7 SCC 263

conducted without consent. Involuntary forensic tests violate fundamental rights. Digital forensic techniques must also respect constitutional rights.

2) Tomaso Bruno v. State of Uttar Pradesh[26]: Electronic evidence and use of cyber forensic tools in modern policing

In this case the issue is that Role of digital evidence (CCTV footage) in criminal trials? Supreme Court of India decision delivered that the non-production of CCTV footage by the prosecution when available creates doubt about the case. Court emphasized the importance of electronic evidence and use of cyber forensic tools in modern policing.

3) P. Gopalkrishnan @ Dileep v. State of Kerala[27]: Digital storage devices as crucial forensic exhibits

Here Issue raised that Accused requested access to forensic report and memory card in a sexual assault case. Supreme Court allowed access to digital forensic evidence, balancing fair trial rights of the accused with victim's privacy. Recognized digital storage devices as crucial forensic exhibits.

4) Mukesh & Anr. v. State (Nirbhaya Case)[28]: Forensic science in criminal investigation

The question of argument in trail is that forensic evidence like DNA testing, mobile phone data, GPS, and medical reports played a key role in conviction. The Supreme court upheld the validity and critical importance of forensic science in criminal investigation. Reinforced the role of forensic labs and cyber tools in justice delivery.

5) Anvar P.V. v. P.K. Basheer[29]: Section 65B certificate is mandatory for digital evidence to be admissible

The issues is that Admissibility of electronic records (emails, CDs, etc.) under the Evidence Act. Supreme Court laid down Section 65B certificate is mandatory for digital evidence to be admissible. strict procedure for forensic experts and investigating officers to follow.

6) Ram Singh v. Col. Ram Singh[30]: Admissibility of tape-recorded conversations as evidence

The arise topic is that Admissibility of tape-recorded conversations as evidence. Supreme Court held down Tape recordings are admissible if: they are authentic, not tampered, verified by expert evidence (forensics).

B. Forensic Investigation in Cyber Crime

1) Anvar P.V. v. P.K. Basheer[31]: Admissibility of Electronic Evidence in Court

Introduced a landmark precedent in cyber forensic law. Supreme court ruled that Section 65B certificate under the Indian Evidence Act is mandatory for the admissibility of electronic evidence. Overruled the earlier relaxed view from *State v. Navjot Sandhu*. Set a strict procedural framework for investigators and forensic examiners handling digital evidence. Its Relevancy is that forms the basis for presenting cyber forensic reports, emails, chats, CDs, mobile recordings in courts.

2) Sonu @ Amar v. State of Haryana[32] : Reaffirmed the necessity of 65B certificate

Supreme court held that digital evidence without proper certification is inadmissible, even if not objected to during trial. Relevance: Clarifies the legal threshold for cyber forensic admissibility. Reinforces chain-of-custody and proper digital investigation protocols.

3) P. Gopalkrishnan @ Dileep v. State of Kerala[33]: Memory card is a document under Section 3 of the Evidence Act

Supreme court said that the accused has the right to a copy of forensic evidence for a fair trial. But victim's privacy must also be protected (especially in cyber sexual assault cases). Relevancy of this case is that Balances cyber forensic access and privacy rights. Relevant in cases involving seized phones, chats, cloud storage, videos.

4) Dharambir v. CBI & Ors.[34]: Integrity and chain of custody of forensic digital evidence: Delhi HC Emphasized that digital evidence like hard drives and CDs must be properly cloned and preserved. Courts must ensure authenticity and avoid tampering or alteration. Relevancy of present case is that standardizes the handling of cyber forensic evidence in investigations and trials.

[26] (2015) 7 SCC 178
[27] (2020) 9 SCC 161.
[28] (2017) 6 SCC 1.
[29] (2014) 10 SCC 473.
[30] AIR 1986 SC 3.
[31] (2014) 10 SCC 473.

[32] (2017) 8 SCC 570.

[33] (2020) 9 SCC 161.

[34] 148 (2008) DLT 289.

5) Shamsher Singh Verma v. State of Haryana[35]: Importance of forensic reports andexpert testimony: Supreme court Clarified that forensic expert reports on electronic media (e.g., mobile phones) are critical. Delay in submitting them or improper collection weakens the prosecution's case. its Relevancy is Underscores the role of trained cyber forensic labs and timely digital analysis.

C. Legal Principle Established:

- Mandatory that the certificate made as per section 65B is digital evidence- *Anvar P.V. v. Basheer*
- No exception for uncertified electronic records- *Sonu v. State of Haryana*
- Accused's right to forensic digital copies; victim's privacy safeguarded- *Dileep v. Kerala*
- Importance of proper forensic cloning and chain of custody- *Dharambir v. CBI*
- Delays or lapses in cyber forensic procedures hurt credibility- *Shamsher Singh v.* Haryana

VI. CHALLENGES FACED BY CYBER FORENSICS

No matter however effective any technology or system may be. There always has been a drawback to the same. Similarly, preserving data or information for the purpose of serving as an evidence is beneficial to the court but on the other hand there may be certain technical and human barriers to such gathering of the information. Some of the limitations are as follows:

- Some facilities which are there within the browsers for the purpose of saving the WWW pages to disk are not perfect because it may save the texts but not the related images.
- There might be difference between what is there on the screen which can be seen and what is saved on the disk.
- The method which has been used to save a particular file might not carry individual labeling regarding when and where it was obtained. Such files can be easily forged or modified.
- Most times it becomes difficult for the system to locate the page which was acquired at last. If the entire series is examined, it becomes even difficult to point which one was later and which was earlier.
- Many ISPs use proxy servers in order to speed up their delivery of pages which are popular on web. Hence, the user might not be sure of what he has received from that particular website by his ISP.

VII. CONCLUSION

In the upcoming years computers are playing a major role. In our day to day life without computer we are not going to do any work. So the increase use of technology will also lead to increase in crime rate. The cyber-crime case has to be handled very carefully in order to cull out the truth. Giving training for the police and judicial officers is very important. India has to develop a lot in handling cyber-crimes cases.

VIII. SUGGESTIONS

There is a need to secure procedures connected with manpower for prosecution of computer- based crime cases to tackle them on a war footing. It must be secured of that the system provides for strict punishment of computer-crime and computer criminals so that the same acts as a method to prevent crime for others. Now, most of the offences committed under the Information Technology Act are Bailable with punishment 'up to 3 years' imprisonment. This punishment should be increased to a term which would change the set of opinions of a computer-criminal of committing almost the same and like offences again. Separate bench is needed to be made up equal to for fast following and recording of Computer cases in an effective manner. With the constitution of cyber judges, the police Internet security to be tightened. Some other suggestions are:

- Encryption technology to be used
- Intrusion detection systems to be used
- Cyber forensic lab should be get established in all the police stations
- Establishment of cyber courts for handling cyber-crime cases.
- Educating the public on cyber-crimes cases
- Motivating cyber-crime victims for registering complaint against the criminals.

REFERENCES

[1]. V. Nandan Kamath, Law relating to Computers, Internet and E- commerce: A Guide to Cyber Laws and the Information Technology Act, 2000
[2]. Dr. Pawan Duggal, Text Book on Cyber Law
[3]. Dr. Karnika Seth, Cyber Crime Against Women: An Indian Law Perspective, 2018 Edition.
[4]. Debarati Halder, K. Jaishankar, Cyber Crime Against Women in India, 1st Ed., 2017.

[35] (2016) 15 SCC 485.

[5]. Debarati Halder and K. Jaishankar, Cyber Crime and Victimization of Women Laws, Rights And Regulations, 2012.
[6]. The Information Technology Act, 2000 (Act 21 of 2000)
[7]. The Bharatiya Nayaya Suraksha Sanhita, 2023 (Act 46 of 2023),
[8]. https://en.wikipedia.org/wiki/Cybercrime
[9]. https://www.splunk.com/en_us/blog/learn/cyber-forensics.html
[10]. https://www.ebsco.com/research-starters/science/cyber-crimes-and-forensics
[11]. https://www.ecsbiztech.com/what-is-the-importance-of-cyber-forensics/
[12]. https://www.cadosecurity.com/wiki/history-of-digital-forensics-how-it-evolved-over-time