INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

THE ROLE OF CYBER FORENSICS IN CYBER CRIME INVESTIGATION

AUTHORED BY - MANSI PRAGYA
Lecturer,
Silver Oak Law College,
Silver Oak University.

ABSTRACT

As technology advances, the increased use of the internet and technological advances leads to cyberthreats. Cyber forensics is used to collect electronic information and investigate suspicious evidence collected in a system or on a network in a way that is legally admissible in court. The number of internet-related crimes and malware attacks on digital devices has increased. Technological advancements have resulted in the advancement and utilization of the Internet. The rise in the number of internet users have led to an increase in cybercrime. To tackle this issue, the field of cyber forensics concentrates on real-time, online proof such as monitoring emails and online chats, in addition to all other aspects of computer-related connectivity. This research paper will discuss cyber forensics, also known as computer forensics, which is a branch of digital forensic science concerned with the detection of evidence in computers and digital storage media. The goal of cyber forensics is to conduct forensically sound investigations of digital media in order to determine, retain, retrieve, evaluate, and report facts and opinions about digital data. Despite its association with the investigation of cybercrime, computer forensics can also be used in civil proceedings. Cyber forensic evidence is typically subjected to similar procedures and serves as ancillary forensic data. With these advances, it was hoped that cyber forensics would protect users while remaining citizen-centric. It also demonstrates that more research is required to comprehend the potential ramifications of cyber forensic research in order to improve discovery of cybercrime.

Keywords- Cyber forensics, cybercrime, digital evidences, forensic investigation

ISSN: 2582-6433

INTRODUCTION

"Forensics is the application of science to the legal process."

We are getting closer to utilising both new and old online opportunities as Internet technologies spread throughout daily life. One such chance is in the field of cyber forensics, a special technique for finding, conserving, analysing, and delivering forensic evidence in a way that is acceptable by the law. Forensics is described as "related to the use of technology or knowledge in the inquiry and identification of evidence or facts in a court of law" by the American Heritage Dictionary[1].

Identification, documentation, and interpretation of computer media are all part of cyber forensics, which can be used to reconstruct crime scenes or use the media as evidence. The process of locating, gathering, conserving, evaluating, and presenting computer-related evidence in a way that is legally admissible by a court is referred to as computer forensics. Computer evidence, computer forensics, system forensics, network forensics, email forensics, cyber forensics, forensic investigation analysis, enterprise forensics, proactive forensics, and other terminology have emerged as a result of the recent branching out of computer forensics into multiple overlapping fields.

Cyber forensics is the study of how and why things transpired online. On standalone machines, system forensic analysis is carried out. In order to identify the sources of security assaults, network forensics entails gathering and analysing network events. Web forensics is another name for the same procedure used on the internet. Analysis of both volatile and non-volatile data is the main emphasis of the data forensics major. A proactive forensic investigation is one that is ongoing, and there is a chance to gather prospective evidence actively and consistently over time. One or more emails are used as evidence in forensic investigations in email forensics.

RESEARCH METHODOLOGY

a. Methods of research

We will use a purely doctrinal and analytical approach to our inquiry. To research and prepare for the present task, numerous reports, articles, legal provisions, and case laws will be employed. This article will use data from both primary and secondary sources.

[1] Kruse W.G, and Heiser J.G, Computer Forensics Incident Response Essentials, 2002, Addison Wesley Pearson Education, Boston

ISSN: 2582-6433

Primary data sources include distinct constitutions, laws, court rulings from various countries, and international treaties.

The researchers will consult secondary data sources such books, numerous national and international journals, papers, and online resources.

b. Research Questions

- Whether the investigating officer's acquisition of cyber forensics is a violation of the right to privacy.
- Do different countries have established legal frameworks for cyber forensics?
- Is there a better cyber forensics department in India? If yes, what are some potential fixes and ideas?

c. Hypothesis

- The laws and regulations created for cyber forensics and cybersecurity by India's parliament, police force, and court system will aid in identifying any gaps in them.
- The manner in which cyber forensics and cybersecurity are currently practised in India, so that Cybercrimes are avoidable.

d. Aims and objectives

- To learn more about cyber forensics
- To be aware of the regulations and laws created for cyber forensics and cyber security in India by the judicial, police, and legislative systems, and to identify any gaps in them.
- To understand the pattern and trend of computer forensics and cyber warfare in India currently.

HISTORY OF CYBER FORENSIC

What is currently known as cyber forensics was previously known as "computer forensics" until the late 1990s. Law enforcement officials who like computers served as the first cyber forensic specialists. In the USA, the FBI Computer Analysis and Response Team started operations in 1984 (CART). The UK's Metropolitan Police established a computer crime squad under John Austen under the Fraud Squad a year later.

ISSN: 2582-6433

At the start of the 1990s, a significant change occurred. The UK law enforcement agencies' investigators and technical support staff, as well as outside experts, realised that cyber forensics needed established techniques, protocols, and procedures just like other fields did. These frameworks did not already exist, but they needed to be created immediately. The present British cyber forensic approach was developed during a series of conferences that were initially organised by the Serious Fraud Office and the Inland Revenue at the Police Staff College in Bramshill in 1994 and 1995.

OVERVIEW OF CYBER FORENSIC

Cyber forensics is employed to find concrete proof of a computer-assisted crime or to assist in the investigation of cybercrime. Cyber forensics as a field of study first emerged in the late 1990s and early 2000s. Everyone with a stake in the legal system, law enforcement, decision-makers, corporate leaders, educators, and the government is interested in Cyber Forensic. Both the practise of criminal law and private inquiry frequently use cyber forensics. It has typically been connected to criminal law. For something to withstand cross-examination in court, it needs to meet strict standards. It is turning into a source of research since courts will not accept software tools like Encase, Pasco, and Ethereal as expert witnesses, making human expert witnesses crucial[2]. Numerous professions, including the military, commercial enterprise, academia, and law, can benefit from understanding cyber forensics. Data protection, data collecting, imaging, extraction, interrogation, normalisation, analysis, and reporting are just a few of the many requirements in these fields. A working and functional lexicon of terminology, such as bookmarks, cookies, web hits, etc., that are consistently used throughout the profession and industry is crucial for all experts working in the developing field of cyber forensics. The cyber forensics field manual focuses on worldwide standards, related core concepts, and technologies. Cyber forensics' goal is to locate digital evidence so that an investigation can be conducted using the scientific approach to reach findings. Investigations involving child pornography, illegal computer use, and cyber terrorism are just a few examples where cyber forensics is used.

Forensics systems enable the administrator to identify problems, hence the discipline of cyber forensics has become a popular research area for these reasons:

1. In order to prevent cybercrimes, intrusion detection systems are essential.

[2] Benjamin Turnbull, Jill Slay, Wireless Forensic Analysis Tools for use in the Electronic Evidence Collection, IEEE Proceedings of the 40th Annual Hawaii International Conference on System Sciences-2007 (HICSS'07)

ISSN: 2582-6433

2. Proactive forensics can be used to detect changes.

CYBER CRIME

Any criminal conduct or other offence involving electronic communications, information systems, including any device, the Internet, both, or more of them can be referred to as "cybercrime."

In 1995, *Sussman* and *Heuston* initially suggested the phrase "*cybercrime*." Cybercrime is best defined as any criminal activity which takes place on or over the medium of computers or internet or other technology[3]. These are illicit activities, when a digital device or information system is either a tool, a target, or both. *Other names for cybercrime include e-crime, high technology crime, information age crime, and electronic crimes*. Cybercrime, to put it simply, is any offence or crime committed through electronic communications or information networks[4]. These types of crimes are essentially any unlawful actions that involve a computer or network. The volume of cybercrime activities is growing as a result of internet development because it is no longer necessary for the criminal to be physically present to conduct a crime. The peculiar aspect of cybercrime is that it is possible for the victim and the perpetrator to never have a face-to-face encounter. In order to decrease the likelihood of being discovered and prosecuted, cybercriminals frequently choose to operate from nations with non-existent or lax cybercrime legislation. People have a misconception that cybercrimes may only be done online or in cyberspace. The 21st century saw the continuing discovery of new trends in cybercrime[5]. New, highly sophisticated methods of committing crimes, such as "phishing"[6] and "botnet attacks"[7] as well as the emergence of technology that is more challenging for criminal justice system to handle and investigate, such as "voiceover-IP (VoIP)[8] communication and "cloud computing"[9] dominated the first ten years of the new millennium. The impact has

[3] https://www.ijarcsse.com/docs/papers/Volume_3/5_ May2013/V3I5-0374.pdf
[4] http://www.academia.edu/7781826/IMPACT_OF_SOCIAL_MEDIA_ON_SOCIETY_and_CYBER_LAW
[5] Gupta AK, Gupta MK. E-governance initiative in cyber law making. International Archive of Applied Sciences and Technology
[6] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph." linked to popular hacker naming conventions.
[7] Botnets is a short term for a group of compromised computers running a software that are under external control. For more details, see Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress
[8] Simon/Slay, Voice over IP: Forensic Computing Implications, 2006
[9] Velasco San Martin, Jurisdictional Aspects of Cloud Computing, 2009; Gercke, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499

ISSN: 2582-6433

altered in addition to the ways. Offenses rose as criminals developed the ability to automate attacks. The mounting issues have prompted nations and regional and international organisations to prioritise combating cybercrime.

KINDS OF CYBER CRIME

The following are some prevalent types of cybercrime:

1. **Illegal Access (Hacking, Cracking)**

   One of the earliest computer-related crimes, "hacking" is the term used to describe the act of gaining unauthorised access to a computer system[10]. This crime has spread widely since the emergence of computer networks, particularly the Internet. Password-protected website password cracking and computer password circumvention are both considered hacking offences. However, actions associated with the term "hacking" also cover preparatory actions like setting up "spoof" websites to force users to reveal their passwords and installing hardware- and software-based keylogging techniques (like "key loggers") that record every keystroke and, consequently, any passwords used on the computer and/or device.

2. **Erotic or Pornographic Material (Excluding Child Pornography)**

   One of the first types of content to be commercially distributed over the Internet was sexually explicit content, which has benefits for sellers of erotica and pornography including:

   - Media exchange without the need for expensive delivery.
   - The Internet is frequently seen as an anonymous medium, which pornographic users value in light of prevailing societal perceptions;
   - Worldwide access, reaching a substantially higher number of clients than retail establishments; To varying degrees, erotic and pornographic content is illegal in several nations.

   In order to safeguard children, some nations allow the sharing of pornographic material among adults while restricting criminal prosecution to situations in which children access the material. According to studies, giving children access to porn may be harmful

[10] In the early years of IT development, the term "hacking" was used to describe the attempt to get more out of a system (software or hardware) than it was designed for. Within this context, the term "hacking" was often used to describe a constructive activity.

ISSN: 2582-6433

to their development. "Adult verification systems"[11] have been created to abide with these rules. Without focusing on particular populations, several countries outlaw the exchange of pornographic material, even among adults (such as minors).

3. Child Pornography

Nowadays, it is very common for children to be sexually abused online. Children are easy targets for cybercrime because they are so vulnerable. Children now have easy access to the internet since computers and the internet are become necessities in every home. On the internet, there is also simple access to pornographic material.

By disseminating pornographic material, paedophiles entice minors to meet them for sex or to snap their naked photos, especially those in which they engage in sexual postures. In chat rooms, paedophiles have been known to approach kids while pretending to be teenagers or kids their own age. Once they gain the kids' trust, they start getting friendly with them. Then, to help kids lose their sex-related inhibitions, paedophiles progressively introduce sexual conversation before calling them out for intimate behaviour. After that, the youngsters are actually exploited by being given money or being given false hope for the future. The youngsters are then sexually exploited, either by being used as sexual objects or by having their pornographic images taken and sold online.

4. Cyber Stalking

Stalking, in broad terms, is the practise of repeatedly disturbing a victim, such as by following them, making threatening phone calls, damaging their property, or leaving notes or other materials behind. Serious violent behaviours, such as harming the victim physically, may accompany stalking. Cyberstalking is the practise of a cybercriminal repeatedly intimidating or threatening a victim via the internet. All the victim's personal information, including name, family history, phone numbers, etc., is gathered by stalkers. The stalker may be a friend of the victim or a stranger.

He can readily obtain this information if he knows the victim. If the perpetrator is unknown to the victim, he gathers data from online sources, such as various profiles the

[11] 2006 Draft Law, Regulating the protection of Electronic Data and Information and Combating Crimes of Information (Egypt): Sec. 37: Whoever makes, imitates, obtains, or possesses, for the purpose of distribution, publishing, or trade, electronically processed pictures or drawings that are publicly immoral, shall be punished with detention for a period not less than six months, and a fine not less than five hundred thousand Egyptian pounds, and not exceeding seven hundred thousand Egyptian pounds, or either penalty

ISSN: 2582-6433

victim may have completed when opening a chat or email account or when creating an account with some website, and then harasses the victim via calls, emails, and other methods.

STEPS INVOLVED IN CYBERCRIME INVESTIGATION

In the age of digital India, there have been several technological advancements, as well as numerous breakthroughs, and numerous new inventions are currently in the works. Technology-related crimes are growing along with technology's advancement. The IT Act of 2008, which was updated in 2010, is used to register many cases. Data theft, hacking, illegal access, pornography, intellectual property theft, cyber terrorism, viruses, and many other examples have been reported. The threat posed by cybercrime to industry, national security, and the general public is growing.

The mechanism for investigating cybercrime is as follows[12]:

1. **Questioning**

   Attempting to gather information regarding the crime, who committed it, why, and how to start the inquiry.

2. **Gathering Information**

   In addition to analysing webcams, wiretaps, and other sources, occasionally the evidence is also gathered from the hacker's machines.

3. **Computer Forensics**

   Using forensic techniques, the evidence is gathered after the questioning and information gathering process. Given that they must be presented in court, the gathered evidence should be carefully preserved. Investigation methods for cybercrime: Identifying the person.

A computer forensic Investigator should follow some of the investigation procedures in order to discover the truth, including: tracking IP address, analysing webserver logs, tracking email account, trying to recover deleted evidence, trying to crack the password, and looking for concealed data. To discover the truth, they must adhere to certain processes. Without disrupting the chain of custody, one should obtain the evidence. Once the evidence has been acquired, one should work on the duplicate data while keeping the original data safe. The forensic investigator should ensure data integrity. The actions listed below should be taken by forensic

[12] Gupta AK, Gupta MK. E-governance initiative in cyber law making. International Archive of Applied Sciences and Technology.

ISSN: 2582-6433

investigators when looking at cyber forensic cases. The investigation process should not harm the credibility of the investigator and the company as a whole.

ROLE OF CYBER FORENSICS IN CYBER-CRIME INVESTIGATION

As cybercrime rises, there is a strong demand for cyber forensic specialists across all business sectors, but especially among law enforcement agencies, which rely on cyber forensics to track down cybercriminals. Cyber forensics is more recent than forensic science, which is a relatively new profession. Each of the many subfields of cyber forensics is extremely challenging to practise. The importance of cyber forensics, however, cannot be overstated, particularly in the modern era of space laws, artificial intelligence, and the Internet of Things (IoT).

India has started several technology-driven programmes, including the National E-Governance Plan (NeGP) and Digital India. Cyber forensics will be crucial in cases ranging from straightforward internet theft to complex satellite hacking. India is undoubtedly a novice in this area, so we must begin with the fundamentals of cyber forensics.

Cyber forensic investigators are professionals at decrypting encrypted data using a variety of programmes and equipment. Depending on the kind of cybercrime they are investigating, investigators employ a variety of emerging tactics. Cyber investigators' tasks may include recovering erased material, deciphering passwords, identifying the source of a security incident, etc. After being gathered, the evidence is then archived and translated so that it can be used in court or for future investigation by the police. Cyber forensics' goal is to preserve data in its most authentic state so that historical events can be accurately reconstructed through a structured examination[13].

Law enforcement organisations, public prosecutors, and judges all struggle with even the most fundamental applications of cyber forensics principles. The moment a flawed police investigation is launched, the case against a cybercriminal is put in jeopardy. **In India, we have police and intelligence personnel with excellent investigative skills. Unfortunately, not all of organizations are able to use these online investigation tools.**

[13] Diva Rai, Cyber Crimes: Classification and Cyber Forensics, IPLEADERS https://blog.ipleaders.in/cyber-crimes-classification-and-cyber-forensics.html

ISSN: 2582-6433

It is crucial to understand that, for an act to be investigated as a cyber-crime **under Section 66 of the Information Technology (Amendment) Act, 2008**[14], it must be an act as defined **under Section 43 of the Act**[15] combined with dishonest and fraudulent intentions according to **Sections 24**[16] **and 25**[17] **of the Indian Penal Code**. In other words, it must be an act as defined under Section 43 of the Act. The act will not be investigated as a cybercrime if it does not meet the aforementioned requirements and instead comes under the purview of the adjudicating authority as an offence.

RIGHT TO PRIVACY IN CYBER FORENSICS AND CYBER SECURITY

In **Gobind v. State of Madhya Pradesh**[18], privacy is defined as the ability for each natural being to be left alone in an untouchable core, although the individual's autonomy is constrained by her connections with other members of society.

There isn't even a single defined rule in India that addresses the development of cyber-forensics as a field of forensics. This might be because technology law in India is still in its infancy. **Since there are no laws controlling cyber forensics, anyone who wishes to specialise in this**

[14] Computer Related Offences
If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both. Explanation: For the purpose of this section, - a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code; b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code.

[15] Penalty and Compensation for damage to computer, computer system, etc
If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network - (**a**) accesses or secures access to such computer, computer system or computer network or computer resource (ITAA2008) (**b**) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium; (**c**) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network; (**d)** damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network; (**e**) disrupts or causes disruption of any computer, computer system or computer network; (**f**) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (**g**) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder, (**h**) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, (**i**) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means (Inserted vide ITAA-2008) (**j**) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, (Inserted vide ITAA 2008) 17 he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. (Change vide ITAA 2008)

[16] "Dishonestly". —**Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly"**.

[17] "Fraudulently". —**A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise**.

[18] AIR 1975 SC 1378

ISSN: 2582-6433

field only needs to complete a certified course in it after receiving their degree. In India, there is no agency that oversees the cyber forensics industry. **The main purposes of cyber forensics in India are to uphold the law and resolve complex situations, so it is crucial to establish a regulatory organisation that can verify whether those working in this field are truly qualified to do so**. The majority of the time, the examination of digital media yields data and evidence that must be used in court. This is a result of the widespread availability of the internet, which is also leading to an increase in the number of crimes involving digital media. For instance, the only and best way to prove that a female is being blackmailed on a message app in court is to present proof, which in these situations is typically in digital form.

A fundamental right that is protected **by Article 19 of the Indian Constitution**[19] is the right to privacy. When electronic data is provided to forensic science analysts, there is a chance that privacy will be violated. It makes sense to assume that forensic investigators should have access to anything that might be useful in finding the accused so that the victim might receive justice. **However, the majority of the time, the investigator takes not only the necessary information but also all of the confidential information that is irrelevant to the case or is not valuable for it.** They apply it to different ends.

Therefore, there is always a chance that privacy will be violated during a cyber forensics' inquiry. This may be comparable to the contentious Aadhar Card case[20], when the UDIAI used to gather all the data from Indian individuals on behalf of the government. As a result, in such circumstances, it would be simple for any unauthorised person to manipulate the account and use it for illicit reasons if they had access to the PIN, password, Username, or other necessary information due to the forensic science analyst. So, in a manner, we can say that it should be considered a breach of the right to privacy if forensic investigators have access to that private information that is not necessary for the case at hand[21]. In India, there is a need for some sort of regulatory body that will create a code of conduct and accredit forensic investigators. This

[19] All citizens shall have the right—
(a) to freedom of speech and expression;
(b) to assemble peaceably and without arms;
(c) to form associations or unions;
(d) to move freely throughout the territory of India;
(e) to reside and settle in any part of the territory of India;
(g) to practise any profession, or to carry on any occupation, trade or business.

[20] Justice K.S. Puttaswamy and Anr. vs. Union of India (UOI) and Ors. (2019) 1 SCC 1

[21] Sangh Priy Gautam, "THE RIGHT TO PRIVACY IN EMERGING DIGITAL ERA: INDIAN LEGAL SCENARIO" 2014-2015, (Unpublished work, DR. B.R. AMBEDKAR UNIVERSITY,AGRA)

ISSN: 2582-6433

code of conduct may also include rules for the violation of a person's right to privacy if a disclosure of personal information puts that person's life in danger. Cyber forensics are governed by well-established international organisations.

The forensic science department of the Indian government may adopt those organisations' codes of conduct. It will facilitate a swifter investigative procedure. The International Society of Forensic Computer Examiners is one such group that the Indian forensic department ought to join (ISFCE). In the subject of cyber forensics, it is one of the most well-known organisations.

One must pass the test and receive a certificate from the organisation in order to be a competent forensic investigator. Most of the globe accepts their accreditation.

The National Treaty of the Convention on Crime of the Council of Europe also systematically addresses cybercrime. It is a multilateral agreement that provides provisions for both cybercrime and invasions of privacy. Additionally, it has tried to balance and harmonise the process of gathering cyber forensic evidence in cybercrime while also providing a robust code and rules for safeguarding individual privacy rights. The member countries guarantee a shared set of rules, guidelines, and practises while also promoting international collaboration in the investigation of global cybercrimes.

The major goals of the treaty are to preserve information technology and to provide criminal consequences for the following situations:

- Using a computer in excess of what is permitted or gaining access to one without authorisation.
- Unauthorized data blocking,
- Unauthorised data manipulation,
- Unauthorised system interference, and unauthorised device use are all examples of data crimes.

In addition to the treaty, there are other bilateral agreements that safeguard people's rights in cases of cyber forensics. The framework of the US-India Cyber Relationships provides in-depth security, cooperation, and investigation standards that are also consistent with other national and international obligations.

ISSN: 2582-6433

CHALLENGES FACED BY CYBER FORENSICS

Regardless of how efficient a technology or system may be. The same has always had a disadvantage. Like this, keeping data or information for use as evidence is advantageous to the court, but on the other hand, there can be some technical or human impediments to acquiring the information. Here are a few of the restrictions:

- Some built-in browser features for saving WWW pages to disc are insufficient because they only store the texts and not the associated graphics. Between what is visible on the screen and what is saved on the disc, there might be differences.
- A specific file may not have distinct labelling indicating when and where it was obtained depending on the method used to store it.
- Most of the time, it becomes challenging for the system to retrieve the page that was last acquired. Such files are easily falsified or updated. It is considerably more challenging to distinguish which episode was earlier and which was later when the full series is looked at.
- Proxy servers are frequently used by ISPs to hasten the transmission of popular online pages. As a result, the consumer may not be certain of what his ISP has sent him from that specific page.

CONCLUSION

Computers will become increasingly important in the next years. Without a computer, we would be unable to complete any tasks in our daily lives. Therefore, when technology is used more frequently, crime rates will rise as well. To get to the facts, the cybercrime case needs to be treated very cautiously. It is crucial to provide training for law enforcement and judicial officials. India still has a lot to learn about managing cybercrime cases.

An illustration of a legal use case for cyber forensics is as follows:

- The use of cyber forensic techniques to gather electronic/digital evidence is significant in criminal trials and is permitted as evidence under current legislation.
- Cyber forensic tools have a wide range of uses in criminal investigations and improve conviction rates.
- Law is slow to adapt to technological advancements, thus in order to ensure that offenders are prosecuted, the current legal framework in the area of cyber forensics needs to be synchronised and updated.

ISSN: 2582-6433

- Law enforcement personnel lack adequate training in gathering and applying cyber forensics.

SUGGESTIONS

In order to prosecute computer-based crime cases on a war footing, it is necessary to secure processes and staff. It must be ensured that the system imposes severe penalties on computer crimes and their perpetrators for it to serve as a means of crime prevention for others. Most offences under the Information Technology Act are now punishable by up to three years in jail and are bailable. This sentence needs to be lengthened to a level that discourages computer criminals from committing similar offences in the future. For quick following and efficient recording of computer cases, a separate bench must be constructed. The police department can demonstrate their skill in situations involving cybercrimes thanks to the establishment of cyber judges.

Criminals frequently use technology to commit both conventional and cybercrimes. An international threat has emerged from cyberterrorism. The use of computers, the internet, mobile devices, and other computing tools in economic crimes is also on the rise. As a result, both traditional and cybercrime are on the rise. However, the conviction rate in both instances is lower, and it is clear why this is the case: neither the investigation nor the prosecuting authorities were able to provide sufficient evidence in court. It shows that law enforcement organisations are ignorant about the application of cyber forensic methods in criminal investigations.

Additionally, there is a lack of communication among the organisations that conduct research on cyber forensic tools, forensic labs, investigation agencies, and prosecuting agencies. Since failure to achieve a sufficient conviction rate may have a cascading effect, resulting in societal disorder and a threat to our lives, liberty, and property, interdisciplinary study is necessary to close the gap. The possibility of increased criminal activity is multiplied in equal or higher quantities by the growing usage of technology in our lives.

The following recommendations are made:

1. Increased internet security,
2. The adoption of encryption technology,
3. Intrusion detection systems,

ISSN: 2582-6433

4. The establishment of a cyber forensic lab in each police station are all necessary.
5. The creation of cyber courts to hear matters involving cybercrime.
6. Informing the public about cybercrime cases;
7. Encouraging victims of cybercrime to file complaints against the offenders.

BIBLIOGRAPHY

1. Books Referred

- Sharma Nitesh, Cyber Forensic in India: Legal Perspective, Universal Law Publication, Edition 2017
- Sharma B.R., Forensic Science in Criminal Investigation and Trials, Lexis Nexis Publication, 6th Edition, 2020

2. Articles Referred

- 'Crime in India 2014 Compendium', National Crime Records Bureau, Ministry of Home Affairs • Ahmad, Farooq, Cyber Law in India (Law on Internet), Pioneer Books.
- Ashok KM, 'What NCRB statistics says about Criminal Justice system in India?' JANUARY 10th 2023, http://www.livelaw.in/what-ncrb-statistics-says-aboutcriminal-justice-system-in-india.
- Cyber Forensic and Admissibility of Evidence, JANUARY 10th 2023 https://shodhganga.inflibnet.ac.in/jspui/bitstream/10603/268180/13/13_chapter%207.pdf
- Building Foundations for Digital Records Forensics: A Comparative Study of the Concept of Reproduction in Digital Records Management and Cyber Forensics", JANUARY 9th 2023, https://www.researchgate.net/publication/284207349_Building_Foundations_for_Digital_Records_Forensics_A_Comparative_Study_of_the_Concept_of_Reproduction_in_Digital_Records_Management_and_Digital_Forensics
- Kiran Kumar Akate Patil, 'Hurdles in Cyber Forensic Investigation in India', IOSR Journal of Computer Engineering, JANUARY 12th 2023, https://www.iosrjournals.org/iosr-jce/papers/Conf.17003/Volume-2/4.%2018-21.pdf

ISSN: 2582-6433

3. **Websites**

- https://digitalguardian.com/blog/what-cyber-security.
- https://iaeme.com/MasterAdmin/Journal_uploads/IJRMS/VOLUME_10_ISSUE_1/IJRMS_10_01_002.pdf
- https://www.ecsbiztech.com/what-is-the-importance-of-cyber-forensics/
- https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/cyber-forensics-criminal-cases/