THE ROLE OF A.I AND CYBER FORENSICS IN ACHIEVING SDG 5 AND 16 DEALING IN SPECIFIC REFERENCE TO CYBER OFFENCES AGAINST WOMEN

Ujjwal Kumar Singh[*] *Assistant Professor, Law College Dehradun, Uttaranchal University, Dehradun

Prof (Dr). Rajesh Bahuguna[**] **Dean, Law College Dehradun, Uttaranchal University, Dehradun.

1. Introduction

The internet has global face today, India being a formidable part of this system is not exception to it. India also took seismic shift in this new era of Information and Technology. India got its first cyber law legislation namely Information and Technology Act -2000 (I.T Act -2000) . With an objective to grant legal recognition to all transactions done via electronic exchange of information and as well as digital signatures.

In this information era, Cybercrimes are growing impetuously and changing global scenario. Modern era is more challenging and alarming. By the growth of Artificial intelligence, IOT, Deep Learning, Machine learning .These challenges are behaving like *hydra headed*. Internet is being strong in the era of Internet of Things (IOT), deep learning machine learning, big data etc. Presently we are facing new challenges in dealing with cyber offences against women due to rise of Meta-Verse and robo-relationship. Privacy in virtual world is really shrinking. Women is worst affected in Cyber world. It is not affecting only netizens but also affecting students, working women, writers, celebrities, transgender, women, and even tribes who never come across this virtual world.

1.1. Artificial intelligence- There is no generally accepted definition of Artificial Intelligence till date. In 2016 Report issued by *Barack Obama* administration in America "Some define Artificial Intelligence loosely as a computerized system that exhibit behavior that commonly thought of as intelligence. Other defines it as a system capable to solve complex problems

relating to cyber world. In 2018 Microsoft attempted to define it as "a set of technologies which helps us in enabling computers to perceive, learn, reason and assist in decision making to solve problems in ways that are similar to what people do.

1.2. Cyber forensics- This term was first time coined in 1991 by International Association of Computer Specialists in *Oregon*. It developed as a branch of forensic science where we can apply techniques of investigation in dealing with cyber offences.

Basically cyber forensics dealt with scientific examination and data analysis of data held in computer for the purpose of presentation before the court.

Internet related forensics may be classified in three heads.

A. Computer Forensics - It generally deals with extracting hidden or deleted data from computers

B. Cyber Forensics- It may also be called as *Network forensics* and is capable to deal basically with analysis of digital or electronic evidence that is across the large network. The main object of Cyber forensics is to identify potential perpetrator and to assess the impact of crime.

C. Software Forensics- It is generally used in analyzing software source code or binary code (O-1) to determine intellectual property infringement. It helps in suits relating to IPR related disputes in cyber world.

1.3. Cyber offences-Due to changing and dynamic nature of subject the term cyber offences may not be defined particularly. The misuse of computer or in the era of IOT , AI, or Cyborg the nature of these offences is changing very fast so it is not possible to define or cribbed , cabined and confined this word in some established set of rules.

Cyber Offences may be defined as" Crimes directed to a computer or whole computer system" But the complex nature of cyber offences may not be defined in such simple term.[3]

Some other organizations also defined this concept.[4]

Some kinds of cyber offences are discussed below:[5]

---

[3]Talat Fatima, Cyber Crime 89 (Eastern Book Company) (2011)

[4]The Organization for Economic Co-Operation and Development (OECD) , *Computer related crime means any illegal, unethical,or unauthorized behavior relating to the automatic processing and the transmission of Dat*a

[5]Rita Esen, *Cyber Crime: A Growing Problem*, 66 J. CRIM. L. 269 (2002).

a. **Hacking**- Hacking is generally an act of unauthorized use of digital devices and electronic networks. Generally, it is not always malicious act, it may be with alter motives. In hacking hacker misuse the devices like computer, smart phones, tablets or other similar devices and networks, and by it he may gather data of user or he may disrupt data in device.

   Hackers are especially skilled coders and they may classified in three broad heads. This classification is basically based on function and motive of the hacker. They may classify in Black, White and Yellow Hackers. In which Black hat hackers are serious threat to data and they work generally in profitable syndicate.

b. **Child Pornography**- Pornography is depiction of a content it may be printed or visual. It contains narration, display or demonstration of sexual activities or any other obscene material with an inherent intention to trigger sexual excitement to the particular viewer.

   The term Child pornography has been defined under Sec 2 (da) POCSO ACT 2012. It may explain *as "Child pornography is any kind of visual display of overt sexual activity that engages a child. It includes all those image which shows involvement of child in any sexual act".*

c. **Password Sniffers**- Password sniffer scans all data by installing a host device/ machine. It may apply to various network protocols like HTTP, FTP, Telnet, etc.

   Password sniffers purpose is generally bona-fide and it may use as a security tool, but Hackers use it for illegal purposes.

d. **Denial of service attacks-** Denial of service i.e. DoS is an attack on device and as a resultant it becomes impossible to gain access by its legitimate intended user. It may done by flooding the target with traffic and also by sending a message that is capable to trigger crash.

   The most common dos attack may be illustrated as Buffer overflow attack, ICMP flood, SYN flood etc.

e. **Computer Fraud**- We know that a deceit who does not deceive is not a deceit. Fraud may be committed also in virtual world. It may done by using computer data with malafide ulterior motives or by unlawful gaining by that data.

It may be classified in various heads like accessing computers without authority by engagement in data.

f. **Cyber Pornography**- In simple words we may say Cyber Pornography is use of cyberspace with an objective to create, display, distribute, publish obscene materials. Traditional pornographic content has been widely replaced by virtual contents.

g. **Sale of illegal articles**- In contemporary world we see that internet is being widely used in selling and purchasing illegal goods like Weapons, Wild life , Drugs, etc. Generally by exchange of e mail I.Ds customer and seller may contact with each other and after verification and chance of secrecy they may complete this sale transaction.

h. **On-line gambling**- Gambling in India is illegal and generally it governs by the Public Gaming Act 1867. When this act was passed at that time we are not having any idea relating to virtual world. This act does not provide any effective remedy relating to virtual gambling. It may include virtual poker, Sports betting, virtual Casinos etc.

On line gambling is not restricted globally. There are some nations like Gibraltar, Malta etc. allowed gambling with certain regulations and licensing.

i. **Copy right Infringement**- Copy right is a protection to the author of any book, owner of any published. Literary, artistic, dramatic or scientific work. It excludes other from getting any unlawful gain by this work. When anyone breaches the condition and takes unlawful gains of it without the permission of owner it amounts to infringement of such copyright.

j. **E-mail Spoofing**-It is also a form of Cyber attack. In cyber spoofing hacker sends a manipulated mail, which appears as originated from original and trusted source. By taking advantage of known credentials hacker may take sensitive data of user.

k. **Forgery**- In forgery the person creates a data which he knows that it is not genuine but still he uses and projects it as genuine. It may done by various modes like affixing others signature on a document. Digital forgery implies forgery in virtual world.

l. **Cyber defamation**- Offensive Speech targeting women on internet- Such speech has a tendency to create hatred based on sex against women. There are some particular groups of women like young

women, women in media, women having political participation and also individually every women on internet and social platforms have potential threat to be victim of it. It is a global challenge no matter that Malala Yusufjai in Pakistan or a women in eight high income nations.

Cyber offences against women-

1. **Offensive Speech targeting women on internet**-Cyberbullying is an aggressive and intentional, act that was committed by an individual person or by a group with the aid of electronic tools and internet. It is repeatedly attack on victim.

   Cyberbullying is very much alike to traditional bullying but having very wide negative impact on the victim

2. **On-line grooming**- Online grooming is a tactics which may be used by attacker on child victim with an intention to sexually exploit her. The essence and object of this crime is exploit the children and his trust by leveraging shame oif reputation and dignity or by fear of any consequential evil.

   In cyber world or in meta verse it is biggest challenge which society will face

3. **Cyber Stalking-** It is an activity in which attacker, abuser or stalker stalks or harass another person by misusing of internet.

   In cyber-stalking stalker may use e-mail, social media platforms or any such platform with an intent to contact the victim.

   According to Sec. 2(n) of the Sexual Harassment of Women at Work Place (Prevention, Prohibition and Redressal) Act 2013 it includes-

   - Unwelcome physical contact and advances,
   - Demand sexual favors
   - Making sexually colored remarks
   - Showing Pornography
   - Any other verbal /non-verbal conduct of sexual nature[6]

4. **Privacy infringement/ Voyeurism**- As per sec. 66 E of Information and Technology act 2000, Whoever, intentionally or knowingly captures,

[6]Sexual Harassment of Women at Work Place (Prevention, Prohibition, and Redressal) Act 2013, §.2(n)

publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding Rupees two lakh or with both.[7]

The different terminologies associated with the section are explained by the explanation clause following the section 66E of the said Act which are discussed below:

Explanation: For the purposes of this section—

1. "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons:
2. "capture" with respect to an image, means to videotape, photograph, film or record by any means
3. "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast
4. publishes" means reproduction in the printed or electronic form and making it available to public
5. "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that-
   - He or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or
   - Any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.[8]

5. **Revenge Pornography**-Revenge pornography means non-consensual distribution of sexually explicit graphics contents like images, videos and like materials in cyberspace. It is an illegal act to share or publish images and videos of anyone with an ill motive. It may called by other names like non-consensual pornography or sextortion.
6. **Sexting-** the term sexting can be understood by the combination of two words sex+textingwhich can be explained as an act to send sexual text messages. The ambit of sexting may also include sending of nudes or seminude photos and explicit videos of oneself. It may happen through any electronic device.

[7]Information and Technology Act, 2000, § 66 E
[8]*ibid*

Sexting risks for teens; Cyber Bullying- some time leak contents becomes the cause of cyber bullying. A cyberbully may use this leaked media to bullying by Impersonation, Text message harassment, uploading on porn websites.

7. **Defamation** - Some time cyberspace may be used for defamation of any person or community by wrongly portray him. Similar event we have witnessed by Bullibai app. By making this app they were wrongly portraying women. It resulted in causing defamation by hurting the feelings of women.
8. **Meta verse and safety challenges**- Meta verse is also having potential threat to women in cyber world. Recently we have already witnessed many events in which women has been subjected to brutal cruelty in meta verse. Meta verse is generallya new concept having less or no regulation.

Role of cyber forensics in dealing with cyber offences against women-

Forensic evidence is needed for finding out precisely and exactly what data was stored in a computer at the time of occurrence of a particular event. There are many important documents within the computer, the main among them includes files whether normal or deleted, hidden files, passwords, free space, file slack etc.

The digital forensics examination method basically ensures that data should not be tampered.

In U.S, it was held in a case that deleted files on a computer hard disk drive are discoverable. The other party must allowed to retrieve recoverable files. On the same path in other case[9] it was held that onsite inspection of computer hardware to discover relevant records.

On the same path Indian courts also recognized the importance and followed it as a normal procedure in deciding cyber offences.[10]

Cyber forensics may help in dealing with cyber forensics in these heads-

- In maintaining integrity and continuity of data
- Secure collection of computer data
- Examination of data

[9]Eugene J.Strasser v. Bose Yalumachi, 669 So. 2d 1142
[10]Shafhi Mohammad v. State of Himachal Pradesh-2012 SLP(Crl)9631-9634

- Collection and presentation of relevant information.
- Protection of relevant data

2.1 Challenges before Cyber Forensics in dealing with Cyber Offences against Women –The aim of digital forensics investigation is to extract evidences from data and detailed facts and use these evidences in the court of law. It plays an important role in any investigation where data is evolved after a security breach. This data contents may be related to business or strictly confidential. Digital forensics investigation may use to investigate cyber and computer related crime. This investigation may be classified-

a. Collection of evidences without altering the crime scene;
b. Examination of evidences
c. Analysis of these evidences
d. Reporting his analysis before the court/jury

Challenges before digital forensics may be explained in these heads-

- Scientific developments growing popularity of heterogeneous hardware and software.
- Increasing variety of file formats and operating software
- Modern smartphones and utilization of end to end encryption.

Other challenges—

a. High speed and Volume of data—It is not confined to a single host, it is scattered among different physical and virtual locations. Due to this reason more expertise tools and time are needed.

b. Privacy preserving investigations—At this time cyberspace is being used by persons to bring many aspects of life which is personal in nature. It may cause serious privacy infringement where cloud computing is involved.

c. Development of standards—Due to technological development we need cutting edge technology in investigation in dealing with cutting edge cybercrimes. We need processing of these information in a collaborative way. So digital forensics community needs Proper development in dealing with these challenges.

d. Legitimacy—Legitimacy is a big challenge before modern forensic

community in the age of fog computing. It's really a challenge to investigate in this border less scenario.

e. **Rise of anti-forensic Techniques**—Now modern defensive measures encompass encryption, cloaking techniques, obfuscation including information hiding. New tools for cyber forensics should competent to deal with different investigations and privacy protection.

Eric holder, *Deputy Attorney General, the United States Subcommittee on Criminal Oversight for the Senate* has classified these challenges in three categories-

a. **Technical challenges—**Technical challenges includes- Encryption, Anti Forensics, Different media formats and there dynamic nature, Steganography, Live acquisition and analysis.

b. **Legal challenges—**Legal Challenges includes- Relevancy of Scientific evidence[11], Lack of standard legislation capable to deal with this matter, not clear calculation about potential rate of error of used methods in examination and analysis of these documents, General acceptance of theory/method by scientific community.

c. **Resource challenges—**Resource challenge includes – Heterogeneous hardware and software platforms, Volume of data, to satisfy prosecutorial needs of government at all levels.

Other possible challenges—

- Scalability
- Pervasive Encryption
- Automation and intelligence
- Internet of things (IOT)
- Cloud Computing
- Visualization and collaborations

Limitations of Cyber Forensic Tools- These are the limitations of cyber forensic tools—

- Poor and Limited in their functionality
- Incapable to hold terabytes of data into a succinct report.
- Incapable to re-create a unified time line of past events before the court of law

[11]Selvi v. State of Karnatka-2010,(7) SCC 263

- Slow in speed during data analysis
- Digital forensic may be conducted till data is present in the computer
- Needs much integrity and faith before the court

Challenge against fundamental rights like Right to privacy

3.1. Role of AI in helping Cyber Forensics-By using AI technology increases the chances of investigating and identifying cybercrimes. It help us investigating agencies solving the problems effectively and it saves a lot of time and money of the agency. Artificial Intelligence helps in solving these problems and may also play precautionary role in Cybercrimes. Ai can detect suspects by sifting through unstructured data. It can also help investigators to easily look through criminal records and identify potential suspects. The most important role of ai is capability to swiftly analyzing the data. The major contemporary issue before digital forensics is exponential data storage. This issue has only one solution and that is Artificial intelligence.

The prime role of digital forensics is to focus on solving some real time challenges which may arise like reducing the work load of inputs and provide maximum valid output. Artificial Intelligence deals with the proper handling of data and managing the resources.

Advantages of AI In dealing with cybercrimes—

- Detecting new threats
- Thorough understanding of good bots and bad bots, during website traffics.
- Helps in asset inventory and threat exposure
- Strengthening cyber security

Specific AI methods that impact digital forensics—

1. Knowledge re-presentation- One of the pivotal function of Artificial Intelligence is the representation of knowledge. Semantic web can be attributed as the major growth in this area. It is the future of WWW(World Wide Web). It, i.e. the sematic web, generally allows user computer to draw the required connections between web pages and information store. Artificial intelligence can ease the understanding and interpretion of natural language texts witch are required computational task. The two known methods to standardized data is XML (Extensive markup language) RDf (Resource Data Framework). However RDF is generally concerned about semantics which is not very useful in a computer system without syntax[12].

[12]Fadi Al-Kalani, Mamoun G.Awad, Nabeel Bani Hani Semantic Web: Improving Web Search Using RDF Instead of XML, 10 ORIENT. J. COMP. SCI. AND TECHNOL, December 2010.

2. Pattern recognition- Identification of data cluster is done by pattern recognition. Pattern recognition is process to recognize pattern by using a machine learning algorithm. It can be defined as a classification of data based on already gained knowledge. Examples Speaker identification, speech recognition etc.

3. Expert systems- It explain s the4e reason behind particular process and conclusion obtained during the process of this digital forensics. It allows a person to analyze and critique the process. It can expose flaws in getting conclusions.

AI techniques which may help in data forensics—

- **Live forensics**- Live forensics is a growing branch of digital forensics that helps in performing forensic activities in live system. Active system normally means running system. It helps in providing accurate and consistent data for investigation.
- **Data recovery**- Ai also plays major role in data recovery and data protection. It is already providing some real good solutions to complex data recovery problems. Although Ai is at very infant stage but when it will be able to restore data within a few minutes.
- **Password recovery**- The basic thinking behind the password recovery is it that average user often choose similar words, passing phrases, or pattern. With that fixed rules hacker hacks the password. This system works in these stage.
    1. Initiating Private Information look up.
    2. Data Collection and indexation module.
    3. Semantic analysis module of database of found password or potential passwords.
    4. Mutation of data and attempt to guess probable password.
- **Known file filtering**—It is a common forensic technique used to relocate relevant files out heap of irrelevant ones. The major demerit of it that it can work only when hash match perfectly. It can't apply on a damaged file.
- Timeline analysis- In performing investigation of an event it becomes crucial for us to know the existing relationship and communication between parties. Timeline analysis gives us clear data through specific day, month, year, views. It helps examiner in taking decision on particular time line basis.

4.1. Conclusion- In this modern era of cyborg it's really a mammoth challenge before justice system to deal with cyber offences against women. This new branch of science and law cyber forensics though it is in its developing stage is playing a vital role in dealing with these offences. In this fast developing cyber world its really great challenge before the law to maintaining the pace with criminals. They are adopting technology very early. Artificial Intelligence is playing vital role in solving recent challenges before the cyber forensics. Now after adopting new technologies like artificial intelligence, IOT, big data, machine learning application of law is being more effective. But these new challenges like anti-forensics, new hardware and software applications are imposing new limitations before the law and adjudicating agencies.