CYBERCRIME VICTIMS: A COMPREHENSIVE STUDY

Vishi Aggarwal, Ms. Shruti

Student, B.A.LL.B.(H), 10th Semester, Assistant Professor,

Law College Dehradun, Uttaranchal University, Dehradun , India

Abstract:-

With the advancement of technology, the way of conducting crime is becoming more sophisticated, complex and there had been a significant change in the outlook of world in human perspective. Cybercrime is real threat to the fast technology development. This technologies advent not only redefined the human life but also redefined cyber crimes. The rapid growth of internet users and dependence drastically increased the risks of commission of crime. Cybercrime is also categorized into violent and non violent cybercrime like cyber squatting, stalking, morphing, plagiarism, email spoofing, cyber bulling, piracy, vandalism, cyber fraud, etc. Though crime against women is on a rise in all fields being a victim of cybercrime could be most traumatic experience for a women. To protect women from this Information Technology Act, 2000 is made and cyber cells are also formed. In the above backdrop, this paper deliberately attempts to define cyber crime which is a real threat to women and some suggestions and measures required to fight against cyber crime and it also covers the first reported case relating to cybercrime against women i.e. Ritu Kohli's case[i].

Index Terms:- Cybercrime, Women, Information Technology, victim, sextortion

Introduction:-

TECHNOLOGY AN OVERPOWRING POWER,
HAS TAKEN AWAY THE GREEN BROWERS,
IT WAS INTRODUCED FOR A GOOD USE,
BUT NOW HAS BECOME ONLY A MISUSE.

The above saying is true as the technology which was introduced for well being of humans, but now has became only a bane for humans. As many crimes are committed with the help of these technologies. The greatest achievement in the field of technology is that of computers and with the emergence of time new crime also evolved with it i.e. cybercrime. Cybercrime, which is a universal problem, is also known a computer oriented crime, is crime that involves a computer and a network. These include a plethora of illegal activities. The term cybercrime is an umbrella under which many illegal activities may be grouped together. The computer may have been used in the commission of a crime, or it may be the target. Cyber crimes can be defined as: "Offences that are committed against individuals or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)".[ii]

Cybercrime may threaten a person or a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, sextortion, child pornography, and child grooming.

Some of the newly emerged cybercrimes are cyber-stalking, email bombing, cyber defamation, worms, polymorphic virus etc. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication

networks such as internet and mobile phones".[iii] Today, the crime against women is increasing at a very high rate. Women are made targets through internet and then their personal information is being asked and then they are blackmailed by those people. Sometimes people are also given job offers and when people opt for those offers they are trapped and it leads to crime against them. It has been seen that woman go missing after going to visit her facebook friend. Recently a game "blue whale" was launched in which children were made easy target and then they were told how to become unsocial and then they were blackmailed and finally they were asked to commit suicide. These all are victim of it, and this crime is also a crime against body as the individual is harassed mentally, exploited sexually and everything which is required to degrade a person's body and reputation is done by the offender.

What is cyber crime?

Cybercrime is a broad term encompassing acts committed or facilitated by the use of computer technology.

As regards exact definition of cybercrime, it has not been statutorily defined in any statute or law as yet. Even the IT Act, 2000 does not contain the definition of cybercrime. However, it may precisely said to be those species of crime in which computer is either an object or a subject of conducting constituting the crime or it may be even both.[iv]

Sometimes viruses are hidden in seemingly legitimate emails and advertisement on web, which if once clicked infect the computer and due to this the person is not able to use their computers.

The expanding reach of computers and the internet has made it easier for people to keep in touch across long distances. However, the means that enable the free flow of information and ideas over long distances also give rise to a worryingly high incidence of irresponsible behavior. The vulnerability and safety of women is one of the biggest concerns of any criminal and penal law, but unfortunately women are still defenseless in cyber space. Cybercrime against women is on at alarming stage and it may pose as a major threat to the security of a person as a whole. The World Wide Web allows users to circulate content in the form of text, images, videos and sound. In recent years, there have been numerous reports of women receiving unsolicited emails which often contain obscene and obnoxious language. And the main concern is that these matters are generally not reported by women[v].

Categories of Cybercrime:-

It is very important to note the various categories of cybercrime and to place specific offenses into those categories. Cybercrimes can be easily placed into two categories; Violent and Non-violent cyber crimes[vi]. Most of the cybercrimes are non-violent offenses, because of the fact that interaction is without any physical contact. Some of the non-violent cybercrimes are cyber trespass, cyber theft and cyber fraud.

Categories of cyber crime with various types placed in it:

1. Violent Cyber crimes
 (i) Cyber Terrorism
 (ii) Cyber Stalking
 (iii) Pornography
 (iv) Cyber bullying
2. Non violent cyber crimes
(i) Cyber Theft
 • Embezzlement
 • Unlawful appropriation
 • Corporate Espionage
 • Plagiarism
 • Piracy
 • Identity Theft
(ii) Cyber Fraud

(iii) Cyber Trespass
(iv) Destructive Cyber crimes
• Cyber Vandalism
• Viruses
(v) Other Non violent Cyber crimes
• Cyber Prostitution
• Online Gambling
• Cyber laundering
• Internet Drug Sales

1. Violent Cyber Crimes:
Violent Cyber Crimes are those crimes that pose a physical danger to some person or persons. They are further classified as follows:

i). Cyber Terrorism: "Cyber Terrorism" is basically a convergence between cyberspace and terrorism. But there is a growing concern among government agencies such as the Federal Bureau of Investigations (FBI) and the Central Intelligence Agency (CIA) that such intrusions are part of an organized effort by cyber terrorists, foreign intelligence services, or other groups to map potential security holes in critical systems. A cyber terrorist is someone who intimidates or coerces a government or an organization to advance his or her political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them.
Cyber terrorism in general can be defined as an act of terrorism committed through the use of cyberspace or computer resources. As such, a simple propaganda piece in the Internet that there will be bomb attacks during the holidays can be considered cyber terrorism. Anyone can be victim of cyber terrorism i.e. the man, women or a child.

ii). Cyber Stalking: It is a type of cyber crime in which an attacker harasses a victim by using electronic communication. In some cases, cyber stalking originates from a real world stalking and is carried over to the internet. Stalking is a problem that many people especially women, are familiar with in real life. When this problem occurs through the medium of internet, is known as 'Cyber Stalking' or 'On-line Harassment'. Cyber stalking includes harassment, embarrassment and humiliation of the victim. Cyber stalking can also result in personal hurt offline. Cyber stalkers are motivated by hate, anger, revenge, jealousy, obsession and mental illness. Delhi Police registered India's First Case of Cyber stalking in the year 2003. A lady complained against an individual who was using her identity to chat over the Internet in the Delhi region for some days. He was chatting on the Net, using her name and giving her address and phone number and even used obscene language. Consequently, she received almost 40 calls in three days mostly at odd hours from far off places. The said calls created havoc in her personal life and hence she reported the matter. Finally, the IP addresses were traced and police arrested the culprit on the said complaint. A case was registered under section 509, of the Indian Penal Code (IPC)[vii].

iii). Pornography: Pornography Internet is easily accessed on computer, pocket PC, wireless, mobile phone, etc. To a much surprise pornography is the first successful e-commerce product. An important mention here is about a case which was filed in the Juvenile Court, Delhi on the charge of cyber pornography. A student of a reputed school, New Delhi was arrested by Delhi police in year 2001, April because he created a porn website as revenge of having being teased by classmates and teachers. He listed the names of his 12 schoolmate girls and teachers in sexually explicit manner. He was charged under section 67 of the Information Technology Act 2000 and section 292,293, 294 of the Indian penal code and the Indecent Representation of Women (prohibition) Act, 1986.[viii]
Another case is of internet chat room in which a 30 year old man represented himself as a girl before a boy from year 2002 to 2004. The boy ran away from his home to meet this so called girl at Mumbai and discovered the truth. The accused men sexually abused the victim, stole money from him and beat him up. This was the result

of chat room friendship which caused homosexuality which is prohibited under section 377 of the Indian Penal Code, 1860[ix].

iv). Cyber Bullying: Cyber bullying is the use of cell phones, instant messaging, e-mail, chat rooms or social networking sites such as Facebook and Twitter to harass, threaten or intimidate someone.

Cyber bullying is often done by children, who have increasingly early access to these technologies. The problem is compounded by the fact that a bully can hide behind a pseudonymous user name, disguising his or her true identity. This secrecy makes it difficult to trace the source and encourages bullies to behave more aggressively than they might in a situation where they were identified.

2. Non Violent Cyber Crimes:

Non violent cyber crimes do not cause any physical damage to persons; instead they cause financial loss, psychological disorders and social harm. They are further classified as follows:

i) Cyber Theft:- Cyber Theft is a way of using a computer and Internet to steal money or information. This is also the most popular cyber crime because the ability to steal from a distance reduces the risk of detection. Cyber Theft includes:

• Cyber Embezzlement- Online embezzlement means misuse or alteration of data by an employee of a company who has legitimate access to the company's computerized system and network. Example- an employee misusing the company's computerized payroll system in such a way that he is paid extra.

• Unlawful Appropriation- Wherein an individual gains access from outside the organization to transfer funds and modify documents in such a manner that it gives him legitimate right to property he doesn't own. Unlawful appropriation, differs from embezzlement as the offender is not interested with the valuables but gains access and transfers funds or modifies some information.

• Corporate Espionage- In this crime, an individual from inside/outside the company uses the network and steals marketing strategies, trade secrets, financial data, client lists etc in order to gain a competitive advantage. In corporate or industrial espionage, the person uses the company's network to steal trade secrets, financial data, confidential client lists, marketing strategies or any other information to gain a competitive edge.

• Plagiarism is to steal someone else's original writing and call it as its own. This form of crime is increasing everywhere as more and more people have access to computers and internet.

• Piracy is an unauthorized copying of copyrighted software, video, music, books, etc which causes loss of revenue to the owner.

• Identity Theft- In this victim's personal information is stolen by the criminal to commit financial frauds.

ii). Cyber Fraud: Another form of cybercrime which has a firm grip on society is cyber fraud and scams online. But, the problem with this is the lack of systematic and official data. Internet Crime Complain Centre (ICCC) is the only source available whose primary role is to receive public reports of cybercrime and refer them to the relevant criminal justice agencies for action. The Central Crime Station (CCS) investigators reported that six more cases have been registered under cyber fraud and police have identified at least 20 fake data conversion companies after this incident. This depicts the fact that technical experts are faced by culprits who use optimal technical assistance for committing crimes

iii). Cyber Trespass (Hacking): In the case of cyber trespass a computer or network is accessed by the offender without authorization, but may not misuse it. For example, a teenage hacker hacks a network just to prove him to peers or takes it as a challenge. These trespassers enjoy reading emails of others but they don't use any information they find. However, cyber trespass is a crime in majority of countries. Cyber crime causes more harm to society than traditional crimes. Hacking attack on AIMS, World Trade Centre, Bhabha Atomic Research Centre, RBI etc are examples of cyber hacking, they caused more harm than traditional crimes.

iv). Destructive Cyber crimes: In destructive cybercrimes, network services are disrupted or data is damaged or destroyed, rather than stolen or misused. They are classified as:

• Cyber vandalism is a form of vandalism that includes defacement of a website and denial of service attacks.

• Spread of New viruses has seen an upsurge in recent years. Many viruses are linked to notable dates, such as Christmas, Valentine Day or April Fool day, as by doing so, virus writers and distributors feel that they have better chance of success

v). Other non violent Cyber Crimes: Many non violent cyber crimes include Online Prostitution, Gambling, illegal drug sales on Internet and Cyber laundering.
• Cyber Prostitution: It involves carrying out prostitution online through various advertisements on sites.
• Internet Gambling: It denotes customers who use credit cards online to place bets in virtual casinos.
• Internet drug sales: Online pharmacies sale drugs to customers who are unable to purchase it from public or private dealers.
• Cyber laundering: It means using net to hide illegal money. Online banking offers opportunity to criminals who open accounts in an offshore bank and transfers funds electronically.

Types Of Cybercrime That Are Committed Against Women:
 Amongst the various cyber-crimes committed against individuals and society at large, crimes that are specifically targeting women are as follows: –
1. Cyber-stalking- In Cyber Stalking, stalker access the victim's personal information like name, family background, telephone numbers and daily routine of the victim and post them on the websites related to dating services with the name of victim.
2. Harassment via e-mails- One form may include Harassment through e-mails includes blackmailing, threatening, bullying, constant sending of love letters in anonymous names or regular sending of embarrassing mails to one's mail box. Indian Penal Code, Criminal Procedure Code and select sections of IT Act deal with the protection from cyber-crime.
3. Cyber Bullying- Cyber bullying is willful and repeated harm inflicted through the use of computers, cell phones or other electronic devices, by sending messages of an intimidating or threatening nature. India is third behind China and Singapore in online bullying.
4. Morphing- Morphing is editing the original picture by an unauthorized user. When unauthorized user with fake identity downloads victim's pictures and then uploads or reloads them after editing is known as morphing. It was observed that female's pictures are downloaded from websites by fake users and again reposted/uploaded on different websites by creating fake profiles after editing them.
This amounts to violation of I.T. Act, 2000. The violator can also be booked under IPC also for criminal trespass under Section 441, Section 290 for committing public nuisance, Section 292A for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail and under Section 501 for defamation.
5. Email spoofing- A spoofed e-mail may be said to be one, which misrepresents its origin [Legal India]. It shows its origin to be different from its actual source. E-mail spoofing is a popular way of scamming online.
6. Cyber Defamation- Cyber tort including libel and defamation is another common crime against women in the net. Although this can happen to both genders, but women are more vulnerable. This occurs when defamation takes place with the help of computers and/or the Internet when someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

Motive behind cyber crime:
A motivation involved in cyber crime depends on criminal's intent and need. Following are the common motives behind cyber crimes:
1) Monetary Profit – Like many offline crimes, cyber crimes are also motivated by the desire for financial gain.
2) Political Motive – Internet is used by extremist and radical groups for propaganda, to attack the websites and network of their opposite groups.
3) Sexual Impulses – Sexually deviant behaviour is illegal and is considered harmful. People view porn sites to fulfill their immoral desires and needs.

4) Entertainment – Many cyber crimes are done for fun and enjoyment unlike other cyber crimes, in which internet is means to an end. For cyber criminals such as hackers, fun is both a means and an end.

5) Emotional Motivators – Cyber criminals who use anger as motivation are spurned lovers, fired employees, business associates or someone who feels cheated. Revenge is much better planned than anger and it could be more dangerous because cyber criminal has more time to think and plan his tracks which often reduces the possibility of being caught.

Reasons for the Growth of Cyber Crime against Women in India:

The transcendental jurisdiction of Internet causes the major threat to the society in the form of cybercrime. The main victim of this transgression can be considered women and children. The study shows that we have 52 million active internet users in India which reached at 71 million in the year 2009. Among them working women net users are 8 percent and 7 percent nonworking women in the year 2009 and 37 percent usage of all users accessing internet through cyber cafe. It is very common phenomenon that the important information of the net surfer is being disclosed easily by the owners of cyber café and then it is used for illegal purposes.[x] Although acquaintance with technology is positive aspect that can be considered important for the development of any country but at the same time it is becoming the source to increase the crime rate with technology against the weaker section of the society. The reason for the increasing cyber crime rate against women can be categorized into two folds; legal and sociological reasons.

- **Legal Reasons**: The object of the IT Act is crystal clear from its preamble which shows that it was created mainly for enhancing ecommerce hence it covers commercial or financial crimes i.e. hacking, fraud, and breach of confidentiality etc. but the drafters were unaware about the safety of net users. Cyber defamation, email spoofing, cyber sex, hacking and trespassing into one's privacy is domain is very common now days but IT Act is not expressly mentioning them under specific Sections or provisions13. Whereas IPC, Criminal Procedure Code and Indian Constitution give special protection to women and children for instance modesty of women is protected under Section 506 and rape, forceful marriage, kidnapping and abortion against the will of the woman are offences and prosecuted under IPC. Indian constitution guarantees equal right to live, education, health, food and work to women. But the same modesty of women seems not to be protected in general except for Section 67 which covers cyber sex in Toto.

- **Sociological Reasons:** Most of the cyber crimes remain unreported due to the hesitation and shyness of the victim and her fear of defamation of family's name. Many times she believes that she herself is responsible for the crime done to her. The women are more susceptible to the danger of cyber crime as the perpetrator's identity remains anonymous and he may constantly threaten and blackmail the victim with different names and identities. Women still do not go to the police to complain against sexual harassment, whether it is in the real world or the virtual world they prefer to shun off the matter as they feel that it may disturb their family life.

Suggestions for (women not becoming victim) of cyber crime:

Prevention is always better than cure. A citizen should take certain precautions while operating the internet and should follow certain preventive measures for cyber crimes which can be defined as:

- Identification of exposures through education will assist women to meet these challenges.
- One should avoid disclosing any personal information to strangers via e-mail or while chatting.
- By empowering women and making them hesitation free and bold in complaining about the crime.
- By tightening security of internet.

- One must avoid sending any photograph to strangers by online as misusing of photograph incidents increasing day by day.
- Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt policies in regard of this. Encryption technology should be used.
- Web servers running public sites must be physically separately protected from internal corporate network. Intrusion management should be made.
- False email identity registration should be treated as an offence.
- Use of voice-recognizer, filter software and collar-ID for protection against unauthorized access.
- Formation of special cybercrime investigation cell for Hi-tech crimes.
- E-judiciary and video-conferencing for speedy justice.
- Appointment of cybercrime reporters or cyber law journal.
- Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of citizens.
- IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.
- As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime.
- A complete justice must be provided to the victims of cyber crimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminal of cyber crime.

Case Laws:-

1. **Ritu Kohli Case:** First cyber sex crime which was reported in India. In this case one Manish Kathuria was arrested by officials of crime branch of Delhi Police for stalking an Indian lady Ms. Ritu Kohli by illegally chatting on website 'MIRC' using her name. He used obscene and obnoxious language and distributed her residence telephone numbers, inviting people to chat with her on phone. As a result of this, Ritu kept getting obscene calls from everywhere and people talked dirty with her. In a state of shock, she called Delhi police and reported the matter. The police promptly swung into action, traced the culprit and started criminal proceedings against him under sec 67 of IT Act read with sec 509 of IPC for outraging Ritu Kohli's modesty.[xi]

2. One case was reported from Kottayam in Kerala where a girl went to meet with a person she had become friend on Facebook. However when she met him, she was abducted. The girl was however traced and later she told the police that when she met with the boy he had forcibly taken her to a hotel and assaulted her.

3. **State of Tamil Nadu vs. Suhas Katti,**[xii] in the present case emails were forwarded to the victim (a divorcee woman) for information by accused through false email account opened by him in her name. The posting of messages resulted in mental harassment to the victim as annoying phone calls were coming to her in the brief that was soliciting. She therefore, filed a complaint in the Egmore Court in Feb 2004 and the Chennai police cyber cell arrested the accused. He was filled under sec 469/509 IPC and sec 67 of IT Act,2000. Charges were proved against him and he was booked under the above mentioned sections.

Key Findings:

1. Online abuse is a serious issue in India, affecting more than half of survey respondents, yet women and other targets lack support and understanding to respond effectively.

2. Though avid users of social media, respondents lose trust in popular platforms because of harassment against them or someone they know. Over half want stricter community standards for content, and the ability to escalate reports of abuse.

3. Mechanism to report abuse on social media platforms fall short. Victims are more likely to block abuse than to report it, yet blocking is ineffective against organized, sustained campaigns using multiple accounts.

4. Thirty % of survey respondents said that they were not aware of laws to protect them from online harassment.

5. Uttar Pradesh accounted for the highest number of cybercrime cases at 21.4%, followed by Maharashtra (19.3% of the cases) and Karnataka (8.9%).

6. During 2013, 21.8% of cyber crimes was reported for fraud/ illegal gain (1,240 out of 5,693 cases) followed by eve-teasing/ sexual-harassment with 19.6% (1,116 cases) and greed/ money with 14.4% (821 cases).

7. Similarly in 13.2% cases of cyber crime, suspects were 'neighbors / friends & relatives' (749 out of 5,693).

Conclusion:

Over the last three decades, computer technology has become an entirely ubiquitous component of modern life. The increasing dependence on technology to support and manage our lives has created unparalleled opportunities for crime and misuse. In fact, most forms of crime now involves technology in some way, whether through the use of cell phones and text messages or more novel applications of technology to commit crimes that are not otherwise possible outside of digital devices.

Cyber space offers a plethora of opportunities for cyber criminals to cause harm to innocent people. Indian women netizens are still not open to immediately report the cyber abuse or cyber crime. The biggest problem of cyber crime lies in the modus operandi and the motive of the cyber criminal. Cyber space is a transit space for many people, including offenders. While people do not live in cyber space, they come and go like any other place. This nature provides the offenders the chance to escape after the commission of cyber crime. Many websites and blogs provide security tips for the safety of women and children in the net. But still then cyber crime against women is on rise. As they are the easy target and they can be victimized easily i.e. why women are made the main target.

In reality it is seen many chat friends enjoy teasing their women friends by words such as "sexy", "attractive" which are the virtual beginning of cyber obscenity. They slowly take their female friends into confidence and start discussing about their own problems like a true friend. Hence in many occasions they are successful in turning the net friendship into a strong bond and gradually proceed to send obscene or derogatory remarks. If the recipient shies away, the sender of such messages would become more encouraged to continue. The problem would be solved only when the victimized woman then and there report back or even warn the abuser about taking strong actions.

In order to avoid the cyber-crime we should not engage in conversation with people we don't know. People on the other end of the computer may not be who they claim to be. We must keep our passwords protected and do not keep sensitive material on the computer as that can be accessed by the hacker. If anything seems wrong, contact law enforcement immediately.

Women should always be alert while using internet and should not open any site which can lead them into trouble. They should not engage in chit chat with strangers in order to protect themselves from being victimized. Even our government is also taking action like it is planning for setting up the NIC-CERT (National Informatics Centre-Computer Emergency Response Team) to combat cybercrime in India and the home ministry proposing to set up the Indian Cyber Crime Coordination Centre (I4C), the government is hoping to beef up India's cyber security network.

At last I would like to say that 'to remove cybercrime is my plan, I know my friends if we join hands together surely we can'.

REFERENCES:

[i] The Hindustan Times, New Delhi dated 23 dec 2003

[ii] http://www.cyberlawtimes.com/articles/103.html

[iii] https://en.wikipedia.org/wiki/Cybercrime

[iv] Vishwanath Paranjape, Legal dimensions of cybercrimes and preventive laws, Pg no.7, Central law Agency, Allahabad, edn,.1st ,2010

[v] http://www.elixirpublishers.com/articles/1351168842_47%20(2012)%208891-8895.pdf

[vi] https://www.legalindia.com/cyber-crimes-and-the-law/

[vii] https://www.oneindia.com/india/new-wave-cyber-crime-against-women-1894591.html

[viii] Vishwanath Paranjape, Legal dimensions of cybercrimes and preventive laws, Pg no.33, Central law Agency, Allahabad, edn,.1st ,2010

[ix] *ibid*

[x] http://www.thehindu.com/news/national/many-cybercrime-cases-not-investigated/article21235628.ece

[xi] The Hindustan Times, New Delhi dated 23 dec 2003

[xii] Decided by Add. CMM, Egmore, Chennai on 5/11/2004