CRIMES AGAINST WOMEN IN THE CYBER WORLD

Sankalp Sharma[*]
Gaurav Singh[**]
Sumit Singh Shekhawat[***]

Abstract

The first part of the paper deals with basic definition, meaning, nature and scope of cyber crimes. Cybercrime is defined as any illegal activity in which a computer is the main object of the crime or is used as a tool in order to commit an offence. It is an offence that is committed against individuals or groups of individuals with malice to harm the reputation of the victim or cause physical, emotional or mental harm to the victim directly or indirectly, through modern technology and communication networks such as Internet. Some examples of Cybercrimes are identity theft, phishing, distribution of child pornography etc. The second part of the paper is about the types of cyber crimes and the laws related to it. It includes the different types of cyber crimes like Cyber stalking, Cyber bullying, Cyber harassment, Morphing and the various laws related to them under The Indian Penal Code, 1860 and the Information Technology Act, 2000.

The third part of the paper elucidates methods to be safe from any type of cyber crime and the reasons for the growth of cyber crimes in the recent times and the current lockdown. It enlists various methods like keeping a check on children, reporting of matters without hesitance and keeping updated anti-virus softwares. It mentions both legal and social reasons for the growth of cyber crimes

Keywords: Cyber crimes, Identity theft, Phishing, Cyber bullying, Cyber harassment, Child pornography, Indian Penal Code, Information Technology Act.

* Student. Army Institute of Law, Mohali.
** Student, Army Institute of Law, Mohali.
*** Student, Army Institute of Law, Mohali.

INTRODUCTION

There has been a significant increase in cyber crimes against women during this recent lockdown with cybercriminals who have been caged during the lockdown. The lock down was imposed from March 25th to April 14th and was further extended till 3rd May and then again extended till May 15. The main aim of this was to stop the spread of corona virus that has claimed many lives worldwide. According to the National Commission for Women data, 54 cyber crime complaints have been received online in April and 37 complaints have been received by post in March and 21 complaints in the month of February. Experts believe this is just the “tip of the Iceberg". In a span of one month from March 25th to April 25th there were a total of 412 genuine complaints relating to Cyber abuse. Of these 396 complaints were serious issues from women and these reports range from abuse, ransom demands, blackmail and more, said the founder of Akanksha Foundation. This organization works for empowerment and education of people by imparting knowledge on cyber security.

Experts believe that this is a result of the frustration and anger of people which is coming out to the forefront as there is no other release right now as they have been 'caged' due to the lockdown. The founder and President of Cyber peace Foundation believes that the cases of extorting money and sexual favours from someone by threatening to reveal evidence of their sexual activity through means like morphed images have increased during the lockdown. Immediately after lockdown it has been seen that there was a rise in cases of misinformation fake news and women getting duped online when they try to click on Malware links which captures information which is on their phone and turns on the microphone and camera and captures intimate moments which is further used for blackmailing. It is very common for women to not make official complaints in these cases as such matters tend to question their respect in the society. Many women want these matters to be handled unofficially. It has been noticed that when the whole country is on a lockdown and people are at home they depend a lot, on spending time on the internet due to which even cybercriminals have become innovative and craftier in their methods and techniques. For example sending information of the current corona virus situation to people as a method to try and gain their confidential details like their address phone numbers etc. They make these emails appear like they have come from legitimate sources such as the government in form of advisories when actually they are not at all related to the government. Another challenge is the creation of fake profiles cyber bullying and online stalking.

Prevention of Cyber crimes is a difficult task but we can all try to prevent it as much as possible. Cyber crimes can be prevented through education on technology. Teaching people how to securely use digital media, spreading

awareness on phishing emails, fake videos and securely sharing information on the internet can also be of a lot of help for safeguarding women. It is often noticed that there is a lack of awareness among women on where to reach and report whenever something wrong happens. Although there are various ways like there is a cyber police in every district and also many NGOs and other organisations which women can contact once they become the victim but due to the lack of knowledge that is sometimes not possible.

UNERSTANDING CYBERCRIME

Cybercrime is defined as any illegal activity in which a computer is the main object of the crime or is used as a tool to commit an offence. It is an offence that is committed against individuals or groups of individuals with malice to harm the reputation of the victim or cause physical, emotional or mental harm to the victim directly or indirectly, with the help of modern technology and communication networks such as Internet.[1] Some examples of Cybercrimes are identity theft, phishing, distribution of child pornography etc. Women, especially young girls, not completely understanding the world of Internet and new to many technological aspects like internet safety, tend to fall prey to cyber criminals. They are not aware of the problems and evils the Internet brings with its use. In fact, cyber bullies and criminals target women for crimes like virtual stalking and distribution of child pornography.

Cyber Laws

Cyber Law in our country is not a separate legal framework. Whereas it is a combination of contract law, intellectual property law, data protection and privacy law. While in the recent times computer and internet are taking over almost each and every aspect of our life, there is a need for a strong cyber law. The cyber laws should supervise the circulation of Digital information software, E-Commerce and monetary transactions. The information technology act 2000 addresses the new age price. Software Computer technology and mobile devices and internet are mediums and targets of the new age crime.

Evolution of Cyber Law in India

The recent increase and dependency on the use of internet and Technology there was a need for strict cyber laws in the country. Just like every coin has two sides, the dependency on technology also has its pros and cons. As the recent generation is more tech savvy cyber criminals have become more advanced and sophisticated. The internet and Technology was invented for research purposes and for making the lives of human beings easier but there has been a lot of misuse of the modern technology and internet.

Objective of Information Technology Act

[1] https://theresearchpaperlegal.wordpress.com/2018/06/03/cyber-crime-against-women-and-legal-measures-in-india/

The objective of the Information Technology Act, 2000 is as following:

- To provide legal recognition for e-transactions.
- Give legal recognition to digital signatures as a form of valid signatures to accept it payment online
- Give legal recognition to keep accounting books in electronic form by bankers and various other organizations.
- For the protection from Cyber crimes and online privacy.

VARIOUS TYPES OF CYBERCRIME AGAINST WOMEN ARE:

1) Cyber Stalking

Cyber Stalking is where a person again and again engages in a behavior of harassment aimed at another individual which could reasonably and seriously alarm, or terrorizes that person. This is one of the most common cyber crimes that occur in the modern world. The internet exists in parallel to the real world. That means it also reflects the real people with real life problems. Cyber stalking commonly occurs with women, who are stalked by men or children who are stalked by adult predators or pedophiles. Different investigating agencies and experts both agree that stalking has become more rampant with the presence of unregulated internet.

Generally a cyber stalker‟s victim is someone who‟s new to using internet and is not well aware of the functioning of the internet. It can be safely assumed that over 75% are women. The figures are more based on a general idea and assumptions because usually most of the cases go unreported and the accurate figures are unpredictable.

There are various psychological reasons behind stalking like

- Jealousy: Jealousy is a strong and common reason behind stalking especially when it is towards someone they know or have been with.
- Obsession and attraction: Another motive behind stalking could often be obsession and attraction. The stalker could be attracted to victim sexually or mentally. It is important to understand that there‟s a fine line between admiration and stalking.[2]
- Erotomania: It is a mental condition in which the stalker assumes that the victim, usually a stranger or a celebrity, is in love with him/her. It mostly always involves sexual inclination towards someone.
- Sexual harassment: It is considered to be one of the most common motive behind cyber stalking as the internet reflects the real life.

[2] http://docs.manupatra.in/newsline/articles/Upload/455C1055-C2B6-4839-82AC-5AB08CBA7489.pdf

- Revenge and hate: There are instances when the victim is not even a reason for the feeling of hatred and revenge in the mind of the stalker yet he/she becomes the target of the stalker. Internet provides a platform for the stalker to vent out his feeling of hatred and revenge.

Ritu Kohli's Case: Eye Opener for India (Manish Kathuria v. Ritu Kohli, C.C.No. 14616/2014)

This was the first case of cyber stalking to be reported in our country. The victim in this case filed a complaint to the police, her identity was being used by a stalker and was he was sending obscene and offensive messages using her identity. She further mentioned in her complaint that the culprit was also giving her home address and her personal mobile number to various people, due to which frequent calls were made to her at indecent timings. Ultimately the „IP" address of the culprit was traced and police investigated the matter swiftly and arrested the culprit, Manish Kathuria. A case under Section 509 of the Indian Penal Code was registered for outraging the modesty of the victim. But Section 509 of the Indian Penal Code only refers to word, gesture or act intended to insult modesty of a woman but when similar things are done to someone via the internet, then there is no specific law about it that in the said section of the Indian penal code. The conditions mentioned under Section 509 do not cover cyber stalking thus, Ritu Kohli"s case was an eye opener to the Indian Government, to make laws related to cyber stalking for the protection of victims.

The aftermath of this case was that Section 66A was added in Information Technology Act, 2008. Which prescribes imprisonment for a term which may extend to three years and/or with fine for sending offensive/indecent messages over the internet etc. Various amendments were made to the Indian Penal Code, 1860 introducing cyber stalking as a criminal offence, by the Indian Parliament. The Criminal Law (Amendment) Act 2013 added Section 354 D in IPC, 1860. It defines Stalking as a man who follows or contacts a woman, despite clear indication of disinterest to such contact by that woman, or monitoring of use of internet or electronic communication of a woman. A man or a woman committing the offence of stalking is liable for an imprisonment of up to 3 years for the first offence, and shall also be liable to fine and for any subsequent conviction would be liable for imprisonment up to 5 years and/or with fine.[3]

2. Cyber Harassment or Bullying:

Cyber Harassment is intentional continuous behavior aiming to disturb or upset a person through use of internet. The type of harassment which is sexual in approach is known as sexual harassment, consisting of persistent and unwanted sexual advancements.

[3] http://www.legalserviceindia.com/legal/article-639-cyber-crime-in-india-are-women-a-soft-target.html

Indian law has defined sexual harassment under the Criminal Law Amendment (Bill) 2013 as

(i) A demand or request for sexual favours; or

(ii) Making sexually coloured remarks; or

(iii) Forcibly showing pornography; or

(iv) Any other unwelcome physical, verbal or non-verbal conduct of sexual nature.

Women are most commonly harassed by emails. Women have been subjected to harassment since the age of letters, which were sent to them anonymously and they were threatening in nature. Email harassment is the modern technological advancement of the same.

The purpose of harassing women through emails ranges from bullying, threatening and blackmailing to cheating and financial frauds. Usually, miscreants send numerous emails, sometimes offensive and aggressive, to threaten or blackmail the victim.[4]

Section 67 A and 67 B of the IT act explains sexual harassment related to offences of publishing or transmitting of material which contain sexually explicit acts and child pornography in an electronic form. It is extremely difficult to find the culprits in cases cyber harassment as often, people create fake identities on internet for such purposes.

The Information Technology Act does not explicitly cover email harassment. However, Section 292A of the Indian Penal Code (IPC) is applicable for those printing or publishing obscene or offensive matter, or any matter intended to blackmail. Furthermore, one can even invoke Section 509 of the IPC in cases involving any gesture or statement insulting the dignity of a woman.[5]

3. Cyber pornography:

It is described as depiction of sexual material on the Internet. It is the procedure of creating, sharing, downloading or importing sexual content on the internet. It is one of the most dangerous threats to women on the internet as one can never know which action of theirs is being recorded without their consent and would later on end up on web. This includes porn websites and adult magazines created and published using digital methods and the internet.

Now a day, there is rampant increase of females using social media platforms to upload and share their personal images and videos. These pictures and videos are then used by criminal minded crooks to create and publish adult and sexual content on the web.

Cyber pornography can deal some serious damage to a female‟s reputation and image in the society forever. It can have devastating effects on women either mentally or emotionally.

[4] https://www.ardcindia.org/online-harassment-and-cyber-crimes-against-women/

[5] https://www.ardcindia.org/online-harassment-and-cyber-crimes-against-women/

Unlike other cyber crimes like Cyber stalking, Morphing, Email Spoofing, Cyber defamation, Cyber Pornography is an exception which has been covered by Section 67 of the IT Act 2000.

Along with IT Act the accused can be charged under various Sections of Indian Penal Code,

- Section 290 for committing public nuisance
- Section 292 for sale of obscene books etc.
- Section 292A for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail
- Section 293 for sale etc. of obscene objects to young persons
- Section 294 for doing or composing, writing etc. of obscene songs and,
- Section 509 for outraging the modesty of women

Air Force Balbharati School case[6]: The very first case relating to cyber defamation was filed in New Delhi, when the Delhi police Cyber Crime cell registered a case under section 67 of the Information Technology Act, 2000. In which, a teenager of the Air Force Balbharati School, New Delhi, was bullied by all other students in his class.

He decided to get back at his classmates. He created a website, www.amazing-gents.8m.net. The site was hosted by him on free web space. It was exclusive to Air Force Bal Bharti School. On this site, indecent and sexual details were given about different girls and teachers of that particular school. The website also became an adult joke amongst male students.

One day, one of the boys told a girl, "portrayed" on the site, about it. The father of the girl, being an Air Force officer, filed a case under section 67 of the IT Act, 2000 with the Delhi Police Cyber Crime Cell. The accused was put into a Juvenile home.[7]

4. Cyber defamation: Defamation is another common crime against females on the web. Cyber defamation is done with the help of social networking services on the internet.

Cyber defamation consists of sending, posting or sharing derogatory and defaming content about someone on the social media platforms. Crooks post defamatory material about the victim by hacking into one‟s social media account or by creating a fake profile. The fake profile consists of all personal and applicable information about the victim which makes it look like a real one.

Cyber Defamation creates a nuisance in the victim‟s life and can cause several other problems like emotional trauma etc.

A person aggrieved of the offence of Cyber defamation can make a complaint to the cyber crime investigation cell, which is a part of the Criminal investigation department. As per the section 65a and 65b of the Indian Evidence Act:

[6] https://indiaforensic.com/certifications/cyber-crimes-india/

[7] https://indiaforensic.com/compcrime.htm

- Any electronic record printed on paper are copied in optical or magnetic media shall be considered as a document and shall be divisible by Court.
- E-mails are admissible.
- Online chats are admissible

There is no specific law regarding Cyber defamation but Section 66A of the Information Act, 2000 makes punishable the act of sending grossly offensive material for inflicting injury, insult or criminal intimidation.

In the recent case of ***Kalandi Charan Lenka v. State of Odisha,***[8] the Petitioner was stalked online and a fake account was created using her name. Many obscene messages were sent to the victim‟s friends by the offender with an intention to defame the Petitioner.[9]

5. Morphing:

Morphing is the act of downloading an image from the web and editing it completely or almost in a different manner. With the help of this technology perpetrators download pictures of women from different social media sites life Instagram, Facebook and Twitter. After morphing these pictures, the perpetrators create new ones in which the victims are portrayed in compromising situations indulging in sexual acts. Ultimately, these criminals blackmail the women with these morphed pictures for different favors like money etc. There are many cases in which women fall right into their traps to safeguard their image and status in society.

- Indian Penal code

Section 292 speaks about sale etc. of obscene materials shall be deemed to be obscene if it tries to deprive and corrupt the person's personality. The circulation of obscene material would be through any means in order to earn profit and enhance lifestyle etc. In the first conviction the person who was committed such offence shall be liable for imprisonment which may extend up to 2 years and fine up to 2000 rupees and in the second conviction he shall be liable to imprisonment up to 5 years and fine to 5000 rupees.

- Information Technology Act, 2000

Section 67 relates to the punishment for publishing and transmitting obscene material in electronic form say is that in any event of first conviction the person shall be liable for imprisonment resulting up to 3 years with a fine which may extend to 5, 00,000 rupees and in case of second conviction up to 5 years and a fine up to 10 lakh rupees. Photo morphing has become a threat for individuals and there is a need for stringent laws related to Cyber crimes in India.

In the case of **State v. Madachirayil Gopinathan Suni on 31 August, 2018**[10]**,** which

[8] 2017, SCC OnLine, Ori 52
[9] https://www.lexology.com/library/

[10] https://indiankanoon.org/doc/89437851/

was tried in the court of Chief Metropolitan Magistrate (Central) TIS Hazari Courts, Delhi, the complainant had sent 2 pictures which were of her marriage through email to a few of her friends/colleagues, including the accused MG Suni. Her face from one of these pictures, was morphed and made into a derogatory pornographic image by the accused and was shared on the internet. He also sent the same as attachment through emails to the victim.

In the case of **Subhash Kumar Sharma vs State on 20 June, 2018,**[11] the complainant alleged that the present applicants, amongst some others, had been again and again extorting money from him, over a period of 12 to 13 years, threatening to make public his morphed pictures, showing the complainant in a questionable position with a woman named Pooja with whom, the complainant contended, he has no relation with whatsoever. In the case, the complainant stated that Harish Tiwari introduced himself as an advocate, and put forward that a certain woman had some documents, which could harm the reputation of the complainant and to be safe, the complainant had to give "a small amount" to Harish Tiwari. After 2-3 years, it was alleged that Harish Tiwari met the complainant again and mentioned that Subhash Sharma had told him something against the complainant, which was again objectionable, which subsequently forced the complainant to, pay him a small amount “to avoid any nonsense". The complainant further claimed that Harish Tiwari also took some money for filing a case, which was never filed, and that he had never met Subhash Sharma. This series of blackmail and extortion continued periodically at 6 to 8 monthly intervals and the culprits in this case took a huge amount of 12-14 lakh rupees from the complainant over the years. The culprits were held liable for blackmail and for morphing of pictures of the victim.

Reasons for the growth of cyber laws in India

CSC e-governance services India Limited which is licensed for providing internet services, state that there has been a major increase in data consumption. Research shows that there are 4, 621, 24,989 internet users in India. Although the knowledge of technology is a very constructive facet that it has been considered as an important aspect for the development of any country but still this has also been a reason for the increasing rate of Cyber crimes. The objective of the IT Act can really understood from experience which confirms that it was formed for improving the e-commerce therefore it covers more of the economic and commercial crimes recharge hacking fraud breach of confidentiality etc. But the drafters were not focusing on the protection of other internet uses.

Few of the other reasons due to which cybercrime go unreported are due to the shyness and hesitancy of the victim and fear of defamation on their family's name. Many a times they think that they are responsible for the crime

[11] 2019, SCC OnLine, Del 6953

which happened with them. The victims are more endangered to the damage of a cybercrime as the person who has committed the crime, their identity remains anonymous and they can constantly blackmail the victim without showing their identity or by changing their names. A question remains unanswered in the minds of the victims that whether any support would be provided to them by their family, friends or the society at large. These are a few reasons which stop women from reporting cyber crimes and this also causes the spirits of the criminals to get a high.

How can we protect ourselves against cybe-rcrime?

All the users on the internet should be careful as these days cybercrimes are on a rise. Here are some precautions that we can take to help protect ourselves against different kinds of cybercrimes out there.

1. Use a full-service internet security

For instance, Norton Security provides prote-ction against many existing and emerging malware including viruses, and helps us protect our private and financial information when we are online.

2. Using of strong passwords

Passwords should not be repeated on different sites, and we should change our passwords regularly. The main objective is to make them more and more complicated. It is advised to use a blend of at least 10 letters, numbers, and symbols etc. Using of a password managing application can also be a great idea.

3. Keeping our system up to date

It is specifically important for our computer systems and cyber security softwares. Cybercriminals are known to frequently exploit the faults in our outdated software to acquire access to our system. Patching these outdated softwares and defects decreases the possibility to be a cybercrime victim.

4. Manage your social media settings

Keep your personal and private data hidden and secure. For example, if you share a post about your pet‟s name or give away your high school best friend you might just reveal the answers to two very general security questions.

5. Children should be educated about internet

We should teach our children regarding the usage of internet and teach them how to use it safely in a secure manner. As parents we should be accessible to them if they are caught in any problem so that they can tell us freely.

6. Keep a check and knowledge of common security infringements

You should be vigilant enough to have knowledge of all the recent security breaches that keep happening around you and you should to be equipped to defend yourself from those.

7. Precautions should be taken to defend against identity thefts

Identity thefts happen when someone tries to act as you in order to gain money or get entry to any place. Identity thefts can be quite harmful and could lead to huge losses and even wrongful cases. Identity thefts can happen if someone‟s gains access to your network or if you for example, connect to a free public Wi-Fi or use a hacked vpn etc.

8. Parents should keep a check on children

There is also a need to defend children against identity theft. Children have tender minds and a very les experience thus they are quite vulnerable to various cybercrimes. Therefore, you need to keep a track on their browsing history and also have the knowledge about what should be done if there is a security infringement.

9. Should have the knowledge how to react if we become a victim

If we fall prey to any kind of cybercrime, we should straight away report it to the cyber cell. Even if the crime looks small or there is some suspicious activity you should not ignore it. The cyber cell is associated with the central investigation department and it will tell you of any possible data leakage of crime. One should not be afraid of reporting a crime as it gives the culprits a boost to do such activities.[12]

CONCLUSION:

Through this paper, we have discussed that there are lots of ways and means through which perpetrators commit cyber crimes in the web space. Though women are considered to be an easy prey by cyber criminals, we cannot assume that other people are safe from cyber crimes. Anyone with less knowledge of the web space and safety can fall in the trap of cyber criminals.

The government has formulated many laws covering cyber crimes and provided for special investigative agencies and cyber cells present in almost all of the metro cities. Regardless of this development, cyber crimes are on a rise because of the unregulated access of internet and unawareness of people regarding cyber laws. Hence it is vital for everyone, especially women to be up to date with these crimes and take precautions to avoid any loss. It is sensible for all to know a little about cyber laws.

Besides, the cybercrimes may not be put as some technological problem. Instead, this is an approach based problem as it is not the computer systems that are damaging and threatening other people instead it is the people themselves who are exploiting technology to commit illegal activities and create an unsafe environment. Hence, it is us who are required to be cautious

[12] https://www.just40days.com/detail_11-ways-to-help-protect-yourself-against-cybercrime_37529

enough to know about the diverse methods that cyber criminals can adopt. It is advised to have an aware and involved mindset to detect any such scenario which could lead to a cybercrime. The answer to such crimes cannot come from technological advancements. The technologies can only help to track the misuse of the internet and put a break on cybercrimes to some extent.