LAW MANTRA THINK BEYOND OTHERS
(I.S.S.N 2321- 6417 (Online)
Ph: +919310053923 Website: journal.lawmantra.co.in
E-mail: info@lawmantra.co.in contact@lawmantra.co.in

CYBER SPACE AND WOMEN*

Abstract

Technological development in recent years has surely helped people in staying in touch with each other. Internet is considered as one of the pre – eminent creation of technology. With the emergence of the internet the whole world has been integrated into beads of a single necklace. It has eliminated traditional boundaries by creating a virtual world which gives us ample opportunities to create personal as well as professional relations across the globe. But as the trend of technology has drastically increased it has also led to emergence of new crimes, and one such is the 'Cybercrime'. Cybercrime is considered a modern – day crime which is severely on the rise and the majority of the victims of this crime are women and children. Criminals try to harass them; through cyber stalking, child pornography, sending obscene emails, identity theft, cyber bullying, etc. They try to extort money by hacking into their social media accounts and thereon blackmailing them. Various instances can be found where women in western countries have become the victim of cybercrime, however it is significantly less in comparison to Asian countries like India, where majority of women are unaware about this modern – day crime. Even the children have been roped into these crimes by throwing them into sex slavery. Through the medium of this research paper we would elucidate upon the problem of cybercrime against the women and children and how we can prevent and clampdown on it.

* **Mr. Arnav Avasthy & Mr. Aditya Rastogi, Student, Amity Law School, Amity University, Noida (U.P.).**

Introduction

Technology is something that works as a fuel in our life. Without it we cannot call ourselves evolved. Without technology our life could not have been so much easy. In recent years there has been a tremendous development in technology. One of the most important result of this development is the 'Internet'. The emergence of Internet has led to the creation of a new world i.e. the cyber world/space. The term cyberspace is not a very old term. It was termed by William Gibson in his book Neuromancer which was written in 1984.

The term 'Cyber Space' is made up of two words 'Cyber' which is related to the internet and 'Space' which means area available for expanse. Cyberspace, unlike the real world where everything can be either felt through any of our senses, is a virtual world, a world made by the internet. In the real world where there are various objects whom we have named, in the virtual world all the objects are called 'Blocks', blocks of data moving from one place to another. The virtual world cannot be felt by our senses. It's a world we do not live in but subconsciously have made it a part of our life. In today's date even if a person is not aware of cyber space, he is still actively using it or say in it. As the technology is changing, we are quickly moving towards the virtual world. Today everything from ordering food at home to commanding a nuclear attack on a country, everything comes within the cyberspace and is controlled in it. Now a day's various things have come under the scanner of the term cyber like cybercrime, cyber litigation, cyberwar, etc.

Due to the emergence of the cyber space it has created a world which is beyond all the boundaries. It gives people an opportunity to expand relations both personally and professionally across the globe. Cyber space helps in superintending equal opportunity for the people around the globe. Now gaining any kind of knowledge is not restricted to books only and almost everything is available online, starting from sharing any kind of blogs on social media platform to educational videos on YouTube. Anything can be shared with people just on a click of a button. The cyber space also promotes the concept of entrepreneurship as many start – ups like Flipkart, Zomato, Uber technically functions in the cyber space. With many telecom companies providing Mobile Data at a very reasonable rates nations like India who had a very negligible data consumption contribution

is now in the 'top 10 mobile data users around the globe'. But as they say "Everything comes with some attachment of pros and cons", well internet is not an exception

Changing time and technology

The world is rapidly moving and the future is such where we will be completely dependent on the internet. Being connected with the internet is more or less being in the cyberspace and being in the cyberspace has its good and bad things. Though it helps us a lot in communicating with each other, browse and order various things, etc but it also means increasingly getting prone to hacking. Hacking has become infamous mafia of the cyberworld. Earlier since people did not had much knowledge and access to internet, most of the work was saved on the papers. But with so much development taking place, everything is being converted into softcopies and is stored online presuming it to be safe. But privacy in cyberspace is just a myth. Now as people are getting more and more educated about the internet, they are finding new ways to steal money, virtually. Earlier, even if a person used to keep a simple password it was not so easy to hack but now a days the toughest of toughest passwords are being easily cracked.

Cybercrime and its victims

Technology plays a very important role in our lives, be it the men, women or the children. It has helped all of us in some way or the other. It has transformed the way of our lifestyle and has changed the way of our communication. Today communicating with people, making friends, playing games, shopping has totally changed. Gone are the days when we necessarily had to go out of the house to do all these things. Now most of the things are possible at some clicks. The cyberspace has connected us to various users, some we know and some we don't. With increase in number of users of cyberspace, the things that is also increasing at the same pace are the cybercrimes. Cybercrimes are nothing but the crimes that take place in the virtual world i.e. cyberspace. These offences can take place against individuals as well as institutions using computer and internet. Cyber Criminals use various mediums like social media platforms and emails to attack their victim.

Cybercrimes though can take place against anybody irrespective of the gender and age but the statistics have shown that the majority of these crimes take place against women and children.

They also take place against the institutions but the types of crimes that are committed are usually limited to financial frauds.

Women

The crimes against women is something prevalent from a very long time. This is due to our patriarchal culture which tells us that women can never at the same level as men. Women have always been told to stay at home, don't do jobs, take care of the house, etc. What we don't understand is that due to this they have almost no exposure to the new technologies, and have become technologically illiterate. Due to this, when they try to get into the modern – day technological world, they become easy prey of cybercrimes.

Some of the main reasons why women fall easy prey of these crimes are:

Change in lifestyle (from joint to nuclear family):

Earlier, the concept of joint family was prevalent, especially in a country like India where many generations of the same family use to reside together under one roof. However, as people started migrating from villages to the cities in search for better job prospects, many women still stay at home but are now home alone, since nuclear family concept is something which in the modern – day society everyone follows. Many women serve as home – maker and stay at home the entire day. Staying the entire day at home make them feel aloof. The result is that they start visiting various social media platforms to seek friendship.

Since women are comparatively more emotional than men, they tend to reveal their personal details easily, like their e-mail ids, phone numbers, pictures, address, etc with strangers who they find as friend on these social media platforms and hence fell in their trap.

Lack of Technical knowledge:

Statistics have shown that not only the women are less employed in cyber workforce but are also technically very less educated. Young girls and women though know how to browse on internet, how to use social media sites (Facebook, Instagram, YouTube), how to use computer tools but they are not aware of the precautions that should be taken while performing any activity on the internet. They are not aware of cyber related problems and thus have no idea of how to tackle it.

Everyday thousands of users are being added on the internet but sadly most of them have no idea about safe and secured usage of the computer.

The primary causes of having less technical knowledge than men can be broken down as:

Culture – Since the time computers were invented, they have always been promoted as a toy for boys/men. Technology related things have always been shown as things which are meant for boys.

Gender Stereotype – Till the 12th class all boys and girls have the same education, it is after this what changes the course. But after 12th very few girls opt for computer science as a subject. This is due to both parental and social pressure.

In Group Favouritism – According to a study in the American Sociological Review, hiring managers tend to recruit those who are culturally similar to themselves (i.e. with the same tastes, hobbies, experiences)[1]

Social Stigma:

Society plays a very important role in our life. We all want to see ourselves being respected by the society. So, when a crime against women takes place, parents and even the victims are hesitant to file a complaint. They fear that their family name and the girl's future might get damaged, if the society gets to know about it. Due to this reason criminals easily escape from being convicted and again go on hunting to harass other women. They are motivated by the fact that there are very less chances of them being reported to the police.

Laws and Government role:

Cyber crimes against women also take place due to ineffective actions of the Government. There are very less laws to tackle these problems and the laws which exist are not stringent enough. Legislations in countries like USA, UK, Canada, Australia and even in India are mainly associated with e – commerce and for this reason the laws mainly cover commercial and financial crimes.

[1] https://www.nextgeneration.ie/blog/2018/08/why-arent-there-more-women-in-tech (Last Modified on 27/09/2016)

According to a report 70% women are not aware of the fact that they are being bullied on the cyber space or they are being stalked, 25% women are not willing to file any complaint in this regard and only 5% women actually report and are aware that they are being abused sexually.

Children

Children are highly vulnerable to these crimes because they are not aware of these crimes and neither do, they know how to protect themselves.

Various types of cybercrimes taking place against women and children:

Cyberstalking:

Cyberstalking means when the stalking takes place in the cyber world. It is not necessarily restricted to only virtual world and also includes stalking in the offline world. But to constitute cyberstalking some part of the crime should have been committed online. Stalkers keep track of their victim virtually like, location track, keeping tracks of their photos and constantly keeping record of their social media websites. After getting their details they harass them virtually, by blackmailing them or threating them and at times by doing these same things in the real world. Though there are no specific laws relating to it but the existing criminal laws and some provisions of IT Act do deal with it.

Photo Morphing:

Photo morphing means giving various effects to the pictures. According to a survey approximately 3.5 billion images are uploaded each day on the social media platforms. Thus, uploading pictures on various social media platforms give hackers an opportunity to access the pictures from there, morph it to make it sexually explicit and then upload it on porn sites. It is also observed that people who upload these photos often blackmail the victims for money or sexual favour.

Cyber bullying[2]*:*

[2] https://cybercrime.gov.in/cybercitizen/home.htm (Pdf. Format) Paragraph 2, Page 11(Last Modified on : 03/07/2015)

Cyber bullying is one of the types of cybercrime which mostly takes place against children and young people. Though it can take place against anyone but due to lack of knowledge about cybercrime, the children become easy prey to this crime.

Cyber bullying means using internet or mobile technology to intentionally harass or bully someone by sending rude, mean or hurtful messages, comments and images/videos. A cyber bully can use text messages, emails, social media platforms, web pages, chat rooms, etc. to bully others.

Cyber bullying can have a very bad impact on children's mental and physical health, thus affecting their academic performance and also their day to day life.

Currently there are no specific laws to deal with cyberbullying, and existing criminal laws are applied to it.

Child Pornography:

Child pornography is publishing and transmitting obscene material of children in electronic form. In recent years child pornography has increased due to the easy access of the internet, & easily available videos on the internet. It is a huge black – market business and many children are trafficked into such acts.

Information Theft:

Information theft usually happens when an imposter identifies key pieces of personal information like Pan Card, Aadhar Card and then tries to impersonate that person virtually. Private conversation on social media platforms like Facebook or Instagram are also hacked into by the hackers and is used by them against the victims.

Cyber Grooming:

Cyber Grooming is another type of cybercrime. In this the criminals try to build emotional bonds with children in order to gain their trust with the objective of sexually abusing or exploiting them. These criminals are called cyber groomers and they use social media as their platforms, creating fake IDs and try to win their trust. They try to lure kids with various attractive offers and then later on ask them to share their sexually explicit images with them.

Online Gaming:

Online Gaming is a big platform which is accessible to all. It is a place where children can easily get bullied. Many gamers try to harass either by using inappropriate language or by cheating. They may also try to befriend you to win your trust and later on may try to get your personal information.

Some other cybercrimes:

E-mail Spoofing:

It can be defined as a term which is used to describe fraudulent e – mail activity where the sender address and other parts of the email header are altered from the original in such a way as to make it look real/original. The criminal tries to make the mail look as it has come from the actual source. When the user opens the mail and logs into his credentials all the data gets transferred to the hacker. This method is often used by cyber criminals to extract personal information and private images of unsuspecting women, etc. Even children are spared, the attacker send spoof mails which looks to have come from the gaming company, they demand money and to provide secret hacks of the game and thus children easily fell in this trap.

Profile Hacking:

Profile hacking is a concept where a person is not able to log into his account as his account is completely under the control of the other person. The primary reason why profile hacking takes place is because first, people often forget to log out from their social media accounts. Second, sharing passwords with other people. Third, using various apps to log into Facebook. However, this problem can be resolved by not using anonymous application for logging into Facebook and using different combinations of password to prevent hackers to hack into the account.

Offer and Shopping Scams:

In the present – day scenario many shopping scams are revolving in the cyber space. Example spin a wheel and get couple tickets to Singapore or buy an iPhone for ₹ 25,000. Often such shopping scams demand prior details of card and net banking and once such details are given amount is deducted from the account and by the time victim realises that such fraud has been committed, perpetrators are long gone.

Legislations

In today's tech savvy world, the environment has become technologically sophisticated and so have the crimes. Internet was initially developed as tool of connecting with people and to gather information conveniently but now it has developed in a medium of doing business, both legal and illegal. The question arises, how safe are we in the cyber space or what are the steps that have been initiated by our government to resolve the cases of cybercrimes.

According to a survey conducted by National Crime Record Bureau, 1791 cases of cybercrime were recorded in the year 2018 in comparison 976 cases recorded in 2017.

The Information Technology Act, 2000[3]

This is the main tool to tackle cybercrimes. It has laws specifically to deal with such crime. It came in the year 2000 and was later amended in the year 2008. After the amendment the following provisions were added. These provisions are as follows

Section 66C of the IT Act makes identity theft a punishable offence. Instances of cyber hacking would be covered by this provision. Under this provision, whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66E of the IT Act deals with the violation of the privacy of a person. Capturing, publishing or transmitting the image of a private area of any person without her consent, under circumstances violating her privacy, is punishable with imprisonment, which may extend to three years, and/or fine.

Section 67 prohibits, and punishes with imprisonment extending up to three years and fine for first conviction and to five years and fine upon second conviction, the publication, transmission and causing of transmission of obscene content. Obscene content has been defined in the same manner as in Section 292 of IPC, and therefore the test of obscenity is to be the same as under that provision.

[3] https://feminisminindia.com/2016/11/24/cyber-laws-india/ (Last Modified on : 15/10/2017)

Section 67A makes the publication, transmission or causing of transmission of sexually explicit material punishable.

Section 67B makes publication/transmission of sexually explicit content depicting children punishable.

The Indian Penal Code, 1860[4]

Prior to 2013, no law directly dealt with online harassment or crimes pertaining to women in the cyber space. The 2013 Criminal Amendment Act was inserted to the Indian Penal Code, 1860 by way of Section 354A to Section 354D

Section 354A: A man committing any of the following acts – a demand or request for sexual favours; or showing pornography against the will of a woman; or making sexually coloured remarks, shall be guilty of the offence of sexual harassment, may be punished with rigorous imprisonment for a term which may extend to three years, or with fine, or with both. In case of the first two and with imprisonment of either description for a term which may extend to one year, or with fine, or with both.

Section 354C defines 'Voyeurism' as including the act of capturing the image of a woman engaging in a private act, and/or disseminating said image, without her consent. For the act to qualify as 'Voyeurism', the circumstances must be such where the woman would "*usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator*". A person convicted under this section is liable to be punished with fine as well as imprisonment up to three years on first conviction and seven years on subsequent convictions.

Section 354D introduced a provision for stalking which also covers cyber stalking. Stalking has been defined to mean an act where a man follows or contacts a woman, despite clear indication of disinterest to such contact by the woman, or monitors the cyber activity or use of the Internet or electronic communication of a woman. A man committing the offence of stalking would be liable for imprisonment up to three years for the first offence, and shall also be liable to fine and for any subsequent conviction would be liable for imprisonment up to five years and with fine.

[4] https://feminisminindia.com/2016/11/24/cyber-laws-india/ (Last Updated : 09/05/2015)

Other than the specific amendments that have been made to the Code, there exist certain other sections under which cybercrimes may be reported or the accused may be charged. These are Section 499, 503, 507, 509.

Indecent Representation of Women (Prohibition) Bill, 2012[5]

The Indecent Representation of Women (Prohibition) Act regulates and prohibits the indecent representation of women through the media of advertisements, publications etc. The Indecent Representation of Women (Prohibition) Amendment Bill, 2012 seeks to broaden the scope of the law to cover the audio-visual media and content in electronic form, and distribution of material will also include distribution on the Internet and the portrayal of women over the web.

Judgements

Some of the few landmark cases relating cybercrime are as follows:

Ritu Kohli Case[6]:

Ritu Kohli Case is considered as first case ever registered related to cyber stalking.

Facts: In the following case Mrs. Ritu Kohli complained to the police against a person, who was using her identity to chat over the Internet at various websites. Mrs. Kohli further complained that the person was chatting on the Net, using her name and giving her address. The same person was also deliberately giving her phone number to other users on the websites encouraging them to call Ritu Kohli at odd hours. Consequently, Mrs. Kohli received almost 40 calls in three days mostly on odd hours. The said call created a havoc in personal life of the complainant. Later on IP addresses was traced and police investigated the entire matter and ultimately arrested the offender.

Judgement: A case was registered under the section 509, of IPC and thereafter he was released on bail. This is first time when a case of cyber stalking was reported. Similar to the case of email

[5] https://feminisminindia.com/2016/11/24/cyber-laws-india/ (Last Updated: 07/07/2016)

[6] https://poseidon01.ssrn.com/delivery.php?ID=991004073021020076083004075096081091096025095076029067119003126024068092005003012072121042119015047112061083124079118007064008119066064011050071076016105115030009099046054032120015085121094028092097031075119096080030088088084103006094010015085071096127&EXT=pdf (Last Updated on: 14/05/2016)

harassment, Cyber stalking is not covered by the existing cyber laws in India. It is covered only under the ambit of Section 72 of the Information and Technology Act, 2000 that perpetrator can be booked remotely for breach of confidentiality and privacy. The accused may also be booked under Section 441 of the IPC for criminal trespass and Section 509 of the IPC again for outraging the modesty of women.

Another Land mark Judgement relating cybercrime is **Delhi Metro CCTV**[7] Footage Leak case.

Facts: In the following case a CCTV recording was released on a porn website where a couple was seen getting intimate in metro stations which had been duly recorded by security cameras and was leaked.

Judgement: At first the CISF was declared liable for releasing the video online but in its defence CISF stated that the access to the control room where the footage is recorded is under the control of DMRC Officials hence DMRC was held liable for releasing the video.

The consecutive case is related to Morphing of images. The following case is also known as **Airforce Bal Bharti Case**[8]

Facts: In this case a student was teased by all his classmates for having a pockmarked face. The child tired with the cruel jokes, decided to seek revenge from his classmates and teacher. He scanned photograph of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. The father of one of the classmates saw it on the website and lodged a complaint with the police.

[7] https://poseidon01.ssrn.com/delivery.php?ID=991004073021020076083004075096081091096025095076029067119003126024068092005003012072121042119015047112061083124079118007064008119066064011050071076016105115030009099046054032120015085121094028092097031075119096080030088088084103006094010015085071096127&EXT=pdf (Last Updated on: 14/05/2016)

[8] https://poseidon01.ssrn.com/delivery.php?ID=991004073021020076083004075096081091096025095076029067119003126024068092005003012072121042119015047112061083124079118007064008119066064011050071076016105115030009099046054032120015085121094028092097031075119096080030088088084103006094010015085071096127&EXT=pdf (Last Updated on: 14/05/2016)

Judgement: It was held that such acts can be penalised under Information and Technology Act, 2000 and attracts punishment under Section 43 & Section 66 of the Information and Technology Act, 2000. The violator can also be booked under IPC Section 509 also.

The following case is related to Child Pornography and is cited as **Avnish Bajaj vs. State**, famously known as **Delhi Public School MMS Scandal case.**

Facts: In the following case a girl from the DPS School was seen in a compromised position with her boyfriend. A video of them in such position was shot and uploaded on one of the porn websites.

Judgement[9]: The court observed that a prima facie case for the offence under Section 292 (2) (a) and 292 (2) (d) IPC is made out against the website both in respect of the listing and the video clip respectively. The court observed that "*[b]y not having appropriate filters that could have detected the words in the listing or the pornographic content of what was being offered for sale, the website ran a risk of having imputed to it the knowledge that such an object was in fact obscene*", and thus it held that as per the strict liability imposed by Section 292, knowledge of the listing can be imputed to the company. However, as far as Avnish Bajaj is concerned, the court held that since the Indian Penal Code does not recognize the concept of an automatic criminal liability attaching to the director where the company is an accused, the petitioner can be discharged under Sections 292 and 294 of IPC, but not the other accused. As regards S. 67, read with Section 85 of the IT Act, the Court however, observed that a prima facie case was made out against the petitioner Avnish Bajaj, since the law recognizes the deemed criminal liability of the directors even where the company is not arraigned as an accused. The judgement however did not declare Avnish Bajaj guilty.

Conclusion

[9] https://indiancaselaws.wordpress.com/2013/10/20/avnish-bajaj-vs-state-dps-mms-scandal-case/ (08/11/2016)

After doing a detailed research on the contemporary issues related to what is cybercrime, various modes by which cybercrime is committed, why is it that major victims of cybercrime are women and how the problem of cybercrime can be curbed, we have reached a conclusion. To begin with cybercrime being a modern-day crime, it can be escaladed in the multiple ways like cyber bullying, cyber stalking, child pornography, imaging morphing etc. It is a matter of sincere concern that the major victims of these crimes are women and children. The agony of the situation is that it becomes very difficult to trace and punish the wrong doer because just like the ocean cyber space is very vast and by the time the accused is identified he is gone. And if the accused is from the other country then it becomes even more challenging to find the accused.

Now a days everyone has a social media account where they upload their likes, dislikes, date of birth, marital status, etc which can easily be accessed by others. Even marriage and job portal also act as a good source of seeking information about women. The problem of cybercrime is contemporary one and it needs to be cured fast as technology is considered as the future of new era and people will we dependent on it completely. To curb the problem of cybercrime various initiatives have been taken by the government like the implementation of Information and Technology Act, 2000 which was later amended specifically focusing on various issues relating to cybercrime.

The government ministries are issuing various guidelines to curb various problems that are the result of the cyberspace. The government has started setting up cyber cells and cyber police stations throughout the country to crack down on these problems. Though the initiatives are great but they are very slow paced. In today's time where technology is changing in seconds, laws are also needed to be amended. Current laws are either too weak or are not at all effective. Since legislations are not stringent, it gives the culprits opportunities to keep on doing these crimes. The government needs to come up with amendments fast and should continuously amend them with time. There is also a need of spreading awareness among the netizens. They should know about the cybercrimes and how they can keep them safe. Secondly, we as netizens also have some responsibility. We should try to keep ourselves self – aware of these things, though the government is present but we also have a moral obligation. At last, making laws and being self – aware does not suffices the problem hence we also need to educate our children regarding the use of internet, also we should

educate them about harassment and what to do if they are being harassed. It should be joint effort by the government and we as individual.