This chapter deals with the legal regulations that protect Indian women in cyber space. Various issues that are discussed in this paper are: Cyber harassments including hacking and hacking related offences against women and regulatory provisions, Stalking women and the concerned laws, Harassments, threatening, blackmailing, defamation and related laws. Legal approach to problems of ‘forced pornography’, obscenity and the Liability of the ISPs as per the Indian laws are also discussed. The paper ends with a discussion. In this paper as strong emphasis is made on the need for new laws that will protect Indian women in cyber space as a serious lacuna is found in this issue.

**Key Words: -**

`Cyber Harassment, Stalking Women, defamation, Cyber Space`

**INTRODUCTION**

Cyber crime is a global phenomenon. With the advent of technology, cyber crime and victimization of women are on the high and it poses as a major threat to the security of a person as a whole. Even though India is one of the very few countries to enact IT Act 2000 to combat cyber crimes, issues regarding women still remain untouched in this Act. The said Act has termed certain offences as hacking, publishing of obscene materials in the net, tampering the data as punishable offences. But the grave threat to the security of women in general is not covered fully by this Act.

Cyber bullying can affect everyone, including children. Safety Web provides support for parents to improve internet safety for kids.

**Types of cyber crime that are committed against women:**

Amongst the various cyber crimes committed against individuals and society at large the crimes which can be mentioned as specially targeting women are as follows: –

1. Harassment via e-mails.
2. Cyber-stalking.
3. Cyber pornography.
4. Defamation.
5. Morphing.
6. Email spoofing.

**Brief discussions of these offences are as follows:**

**I. Harassment through e-mails** is not a new concept. It is very similar to harassing through letters. Harassment includes blackmailing, threatening, bullying, and even cheating via email. E-harassments are similar to the letter harassment but creates problem quite often when posted from fake ids.

**II. Cyber Stalking** is one of the most talked about net crimes in the modern world. The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering
the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc. Cyber Stalking usually occurs with women, who are stalked by men, or children who are stalked by adult predators or paedophiles. Typically, the cyber stalker's victim is new on the web, and inexperienced with the rules of netiquette & Internet safety. Their main targets are the mostly females, children, emotionally weak or unstable, etc. It is believed that Over 75% of the victims are female. The motives behind cyber stalking have been divided in to four reasons, namely, for sexual harassment, for obsession for love, for revenge and hate and for ego and power trips. Cyber stalkers target and harass their victims via websites, chat rooms, discussion forums, open publishing websites (e.g. blogs and Indy media) and email. The availability of free email and website space, as well as the anonymity provided by these chat rooms and forums, has contributed to the increase of cyber stalking as a form of harassment.

There are a couple of reported cases, which speak of the position of the cyber stalking in India. The recent being the case of Manish Kathuria who was recently arrested by the New Delhi Police. He was stalking an Indian lady, Ms Ritu Kohli by illegally chatting on the Web site MIRC using her name. He used obscene and obnoxious language, and distributed her residence telephone number, inviting people to chat with her on the phone. As a result of which, Ritu kept getting obscene calls from everywhere, and people promptly talked dirty with her. In a state of shock, she called the Delhi police and reported the matter. For once, the police department did not waste time swinging into action, traced the culprit and slammed a case under Section 509 of the Indian Penal Code for outraging the modesty of Ritu Kohli (Indian child, 2005). In another case, an engineering and management graduate, facing prosecution in a dowry harassment case, was arrested by Delhi police for sending obscene e-mails in his wife’s name to several persons. In June 2000, a man was arrested by the Delhi police for assuming the identity of his ex-employer’s wife in a chat channel an encouraging others to telephone net. The victim who was getting obscene telephone calls at night from stranger made a complaint to the police. The accused was then located “on line” in the chat room under the identity of the, victim and later traced through the telephone number used by him to access the internet (Mishra, 2001).

III. Cyber Pornography is the other threat to the female netizens. This would include pornographic websites; pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc).

Internet has provided a medium for the facilitation of crimes like pornography. Cyber porn as it is popularly called is widespread. Almost 50% of the web sites exhibit pornographic material on the Internet today. Pornographic materials can be reproduced more quickly and cheaply on new media like hard disks, floppy discs and CD-ROMs. The new technology is not merely an extension of the existing forms like text, photographs and images. Apart from still pictures and images, full motion video clips and complete movies are also available. Another great disadvantage with a media like this is its easy availability and accessibility to children who can now log on to pornographic web-sites from their own houses in relative anonymity and the social and legal deterrents associated with physically purchasing an adult magazine from the stand are no longer present. Furthermore, there are more serious offences which have universal disapproval like child pornography and far easier for offenders to hide and propagate through the medium of the internet. Recent Indian incidents revolving around cyber pornography include the Air Force Balbharati School case. A student of the Air Force Balbharati School, Delhi, was teased by all his classmates for having a pockmarked face. Tired of the cruel jokes, he decided to get back at his tormentors. He scanned photographs 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. It was only after the father of one of the class girls featured on the website objected and lodged a complaint with the police that any action was taken.

In another incident, in Mumbai a Swiss couple would gather slum children and then would force them to appear for obscene photographs. They would then upload these photographs to websites specially designed for paedophiles. The Mumbai police arrested the couple for pornography.
IV. Cyber Defamation: Cyber tort including libel and defamation is another common crime against women in the net. This occurs when defamation takes place with the help of computers and/or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

V. Morphing: Morphing is editing the original picture by unauthorised user or fake identity. It was identified that female’s pictures are downloaded by fake users and again re-posted/uploaded on different websites by creating fake profiles after editing it. This amounts to violation of I.T. Act, 2000 and attracts sec. 43 & 66 of the said Act. The violator can also be booked under IPC also. The Times of India reported that in October, a Delhi-based beautician told the police that her photograph was flashed on a porno portal along with her mobile number.

VI. Email Spoofing: A spoofed e-mail may be said to be one, which misrepresents its origin. It shows its origin to be different from which actually it originates. A review in the CyberlawTimes.com shows that India has crossed the danger mark in cyber crime targeting women and children. Statistics show, and law enforcers confirm, that the maximum number of cyber crimes related to obscenity occurred in Mumbai last year. There were at least 40 cases in 2006 (of which only ten were registered), a steep rise from only five cases in 2005. Delhi was close behind, with 30 obscenity-related cases (nine registered), but topped in cases of hacking. Bangalore, Chennai, Hyderabad and Pune reported only a handful of obscene crimes but saw a greater incidence of hacking.

The more common method used by men is to email vulgar photographs of themselves to women, praising their beauty, and asking them for a date or inquiring how much they charge for 'services'. Besides sending explicit messages via e-mail, SMS and chat, many also morph photographs - placing the victim’s face on another, usually nude, body. In another instance, a couple entered an internet chat room agreeing to strip for each other using a web camera.” The guy stripped, but the person at the other end was actually another man and his friends, who obviously didn’t. They recorded it and uploaded the clip on a porno website,” said Duggal. “These things happen in every city but only one in every 500 cases is reported,” added Duggal. According to Borwankar, most cases go unreported because people are “petrified of adverse publicity”. While Mumbai is battling obscenity, other cities are concerned about hacking. While Delhi reported 67 cases last year, there were 30 in Bangalore.

Provisions of the IT Act 2000 relating to cyber crime and offences against women in India and the loopholes of the said Act:

Unfortunately even though Chapter XI of the IT Act deals with the offences such as Tampering with computer source documents (s.65), Hacking with computer system (s66), publishing of information which is obscene in electronic form (s.67) Access to protected system (s70), Breach of confidentiality and privacy (s.72), Publication for fraudulent purpose (s.74) IT Act 2000 still needs to be modified. It does not mention any crime specifically as against women and children.

The elementary problems, which are associated with Cyber-Crimes, are Jurisdiction, Loss of evidence, Lack of cyber army and Cyber savvy judges who are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such stage, which needs appreciation, is the P.I.L., which the Kerela high Court has accepted through an email. Today with the growing arms of cyberspace the growing arms of cyberspace the territorial boundaries seems to vanish thus the concept of territorial jurisdiction as envisaged under S.16 of C.P.C. and S.2.of the I.P.C. will have to give way to alternative method of dispute resolution.

Again, under no section in IT ACT 2000, Obscenity – personal viewing – Is an offence, infact like in IPC 292 again if it is proved that you have published or transmitted or caused to be published in the electronic form only
then under Section 67 it can be an offence. Last but not the least, the IT Act 2000 does not mention the typical cyber crimes like cyber stalking, morphing and email spoofing as offences.

CONCLUSION

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 crimes against women are on rise.

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 victimised woman then and there report back or even warn the abuser about taking strong actions.

REFERENCES

1. Cyber Crimes And Fraud Management, Indian Institute of Banking & Finance
2. Bare Act of Information Technology Act, 2000, Universal Publication
3. Mishra S.N., Indian Penal Code

Author: Rohit Agarwal
Designation: Student

Student B.Com.LL.B.(Hons.) 6th Sem. / 3rd Year, College of Law & Legal Studies, Teerthankaer Mahaveer University, Moradabad – 244 001, Uttar Pradesh