

# Regulation of Cyber Crimes Against Women – A Critique

G.Tanuja Reddy

*Research Scholar, Andhra University*

**Abstract - A rapid increase in the use of computer and internet has given rise to new forms of crimes like publishing sexually explicit materials in electronic form, video voyeurism and cyber crimes namely, cyber defamation, cyber bullying, cyber stalking etc. There are no specific provision in the IT Act, 2000 that specifically deal with the cyber crimes against women as does the provisions of the Indian Penal Code, the Constitution of India or the Code of Criminal Procedure for that matter. There is a need for bringing an exclusive legislation for the protection women from cyber crimes.**

**Index Terms - Bullying -Blackmailing –Cyber-crimes-Cyber-Harassment-defamation-Information Technology Act-Morphing-Pornography-Punishment under IPC Revenge porn- Stalking.**

## INTRODUCTION

The rapid growth of Internet and computer technology globally leads to the growth of new forms of transnational crimes. The internet has thrown wide open the doors for computer-based commerce, telephone, mail services and a lot of other areas. Cyber-crimes against women in India is became an issue of concern by which women are subjected to suffer by crimes like pornography, morphing and blackmailing through mails or cyber stalking.

National crime Records Bureau (NCRB) reveals that the statistics show highest crime rate of women in India. The number of social network users in India has increased drastically from 181.7 million in 2015 to 216.5 million in 2016 to a projected 250.8 million in 2017. It was expected that the same would increase to at least 336.7 million by 2020. Though, it is a boon, on the other side, it has created insecurity in the lives of women due to the increasing criminal activities in the virtual world. Security of females of all ages and backgrounds are in a vulnerable position.

The social media (which includes Facebook, chat rooms, Instagram, Skype, WhatsApp, Dating sites etc.) can be seen as a double-edged tool. If it gives you a space to express yourself, it also creates space for

people to respond violently to your thoughts and views. If it gives you anonymity, it also gives abusers or assaulters the anonymity. Women in India have seen both edges of this tool of which only very few have come forward to persecute the culprit through legal formalities. A huge section of the population going through this chooses to remain silent, majority of which is because they are not aware about their rights and the rest out of fear of damage to reputation and prestige.

## REGULATION OF CYBER CRIMES AGAINST WOMEN

The Indian Law has not given any definition to the term ‘cybercrime’ It is pertinent to note that the Indian Penal Code does not use the term ‘cybercrime’ at any point even after its amendment by the Information Technology (amendment) Act 2008, the Indian Cyber law.

Cyber Crime may be generally defined as “unlawful acts wherein the computer is either a tool or target or both” The computer may be used as a tool in the following kinds of activity financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking.

Cyber harassment: Interfering with the personal space of another by modern telecommunication networks without consent by hacking into the account of the victim, getting personal data, photos or videos, distributing rumours to damage one’s social standing. Cyber Stalking Cyber Stalking means when an individual or organization uses cyber space to bother or harass someone, the motive behind it being obsession, vengeance, ego, sexual harassment, etc. It is seen as an encroachment of an individual’s privacy and is one of the highest reported cyber offences against girls and women. Cyber Stalking is punishable under S.354D of IPC, which defines and prescribes punishment of imprisonment for up to 3 years and fine.

Cyber stalking has been considered as one of the worst types of harassment that can be meted out to women on the internet and through digital communication technology. In India, cyber stalking had not been recognized as an offence earlier. Hence, there was no clear perception of online stalking either with the police and lawyers, or with the general public.

Cyber pornography is when the cyberspace is used to create, publish, transfer or circulate pornographic material. IPC S.292 deals with pornography and defines the term 'obscene' and makes any kind of distribution, sale, transfer, publishing, printing of any obscene material punishable with imprisonment for up to 2 years or fine of Rs.2000 or both. S.67 of the IT Act, 2000 makes circulation, selling, distribution of obscene material a punishable offence with a term up to 3 years of imprisonment and fine of Rs.500. S.67A of the IT Act states that whoever publishes/transmits in electrical form any material which contains sexually explicit act or conduct shall be punished with imprisonment of 5 years and fine which may extend to Rs. 10 Lakhs.

Revenge Porn is when a person willingly publishes, circulates, distributes or prints any obscene or sexually explicit material without the consent of the person either to shame the victim or to lower her reputation. The motive behind is vengeance. The offender shall be booked under S.66E of the IT Act which states "whoever intentionally captures, publishes, distributes or transmits the image of a private area of a person without his/her consent under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to 3 years or fine not exceeding Rs. 5 lakhs or both."

Meanwhile S.509 of IPC books the offender for "outraging the modesty of woman". S.72 of the IT act says that for those who publish any obscene material of their partner without their consent or have accessed any electronic data or evidence of that person without their assent, discloses it shall be punished with imprisonment for 2 years or fine of up to Rs. 1 lakh or both. However, what seems to be a major hindrance to the efficiency of the above mentioned provisions of law is that S.77 of the IT act makes all pornography related offences bail-able.

Cyber bullying is when a person uses electronic means or the internet for transmitting, distributing, posting and any sensitive material concerning someone with an intention to harass/humiliate/shame that individual.

There are no specific legal provisions for it except IPC S.509 prescribes punishment for outraging the modesty of a woman with imprisonment of a term up to 1 year or fine or both.

S.66A of IT act, which used to deal with any material that would cause annoyance to any person, was struck down by the Supreme Court in the Shreya Singhal Vs. Union of India as it was said to curb the fundamental rights of speech and expression and was however loosely worded.

Cyber Blackmailing means stealthily gaining or tracking someone's information without their knowledge and then circulating, distributing or publishing sensitive content, private images or videos, or obscene morphed photographs or threatening to do so with a motive behind it being either vengeance or illegal monetary demands. It is punishable under S.384 and S.385 of IPC which deal with extortion prescribing a punishment of imprisonment up to 3 years or fine or both.

Both cyber bullying and cyber blackmailing are dealt under S.506 of IPC- criminal intimidation with punishment of imprisonment of a term up to 7 years or fine or both and S.507- criminal intimidation by anonymous communication with punishment for imprisonment in addition to the punishment prescribed under S.506.

Morphing is when an illegitimate user accesses a person's photo, edits it and then re-uploads it in a different website under a fake profile mostly with a malicious intention to either deprave the reputation of the woman or humiliate and embarrass her. It is punishable under S.66 of IT act and S.43 of IT act which attracts damages or compensation for the victim. The offender can also be booked under S.292 of IPC for obscenity. The offender usually edits the photo of the victim by attaching a photo of a naked woman so as to defame her and deprave her character. For this, the offender can be punished under S.501 for defamation for a term up to 2 years or fine or both.

Cyber defamation is when someone circulates/publishes some defamatory statement or material about someone via internet or electronic means. The offender can be booked under S.499 and S.500 of IPC for up to 2 years of imprisonment and fine in case of defamation. Women are usually faced with sexual remarks or statements which are defamatory and hampers their reputation in both online and offline space. Certain provisions of the "Indecent

Representation of Women Act” also deal with such matters.

The cyber violence committed against women are gender specific and affect only the females. These crimes are governed and sentenced by the Indian Penal Code (IPC) and the Special and Local Laws (SLLs). The SLLs are the two statutes namely, the Indecent Representation of Women Prohibition) Act, 1986 and the Information Technology Act, 2000. Of these two acts, the IT Act is not gender specific but it has few provisions which deal with gender specific problems and prescribe punishment for the acts. The Indecent Representation of Women (Prohibition) Act, enacted in 1986 was brought into action to mainly deal with obscene representation of women and to combat it through advertisements or in publications, writings, paintings or figures.

The IT Act, 2000 is not a SLL which deals with only cybercrimes against women but it does have some provisions which take into account these offences and determine the punishment for their commission. Cybercrimes like defamation, email spoofing, cybersex, hacking and trespassing into one’s private domain is very common nowadays but they have not been expressly mentioned in the IT Act specifically. Majorly, Section 66A, 66E, 67 and 67A deal with the crimes which are primarily against women. Section 66A gives the punishment to be awarded for sending offensive messages via communication services. This provision takes into account any e-mail or message which has been sent for the purpose of annoying or causing inconvenience or deceiving or misleading the addressee or the recipient about the original source of the messages.

Online threatening of rape, abusing, sending disparaging messages, hacking someone’s e-mail id or social media account to defame the victim are booked under this provision. Section 66E provides for punishment for violation of privacy, i.e., the publication of any picture of any private area of the victim without the consent of the victim is a punishable offence. Talking in context of females, it has been specifically mentioned “buttock of female breast”. Further, Section 67 prescribes for punishment for the publication or transmission of any type of indecent material in electronic form. Section 67A provides for punishment for publication or transmission of any substance which consists of sexually explicit activity in an electronic form. Mostly,

the complaints of cyber violence are registered under the Section 67 and 67A of the IT Act.

#### LACK OF SPECIFIC LEGISLATION RELATING TO CYBERCRIMES AGAINST WOMEN

Even though there are plenty of legal provisions against cybercrime, India is not entirely successful in protecting women in cyberspace. Information technology Act, though deals with the major provisions relating to the cyber-crimes against women, it primarily deals with the economic and commercial issues as said in its preamble. Cyber stalking is one of the serious crimes committed online. There was no law against cybercrime till 2013. It was introduced only in 2013 after the recommendation of Justice J.S Verma committee. Stalking was made punishable under section 354(D) of IPC. But section 354(D) defined stalking as an act committed only by men. India needs to have separate and elaborate law against cyber-crime like that of America.

Morphing is a cybercrime which is rapidly rising in modern days. Morphing photos of celebrities with nudes or trolling political leaders via morphing has caused a lot of hue and cry. Cases have been filed against perpetrators and have also been charged. But the close observation of IPC and IT Act shows us the word morphing has never been defined nor the act has been considered punishable under either of the statutes. The charges are filed under section 66, 66(E), 67, 67(A) of IT ACT and section 354 or 509 of IPC. None of these provisions deals with morphed contents and these sections can be invoked only for defamation of person. With such weak protective laws, it would be difficult to charge the perpetrators in future, when increased number of cybercrimes highlights the loopholes in the justice system.

The legal provisions enacted to tackle cases of cybercrimes are not adequate enough to fully counter them. . The initial step in the direction of providing legal remedy to victims is to make sure that online experience of threat or harassment or violence or intimidation caused to women is precisely translated into written regulation via amendments in the two main statutes.

The IPC and the IT Act do not cover all the cyber offences against women. Many a times, women are not even aware of the laws that could protect their rights.. There is even lack of separate provisions for various cybercrimes. The women themselves need to come out

and report the crimes for the laws to get executed. With the steep increase in the number of cyber-crimes against women, there is a need of stringent laws against such crimes and proper implementation of the laws should be looked into.

Indian laws are outdated and needs to be updated at the earliest. Amendment from time to time is necessary to keep up with the changing world of technology. India needs to ramp up its cyber laws in order to fight against hackers and stalkers. Protection of women in cyber space. Proper laws to protect women from various Cyber Crimes should be introduced.

Cybercrime reporting portal -As per the Constitution of India 'Police' and 'Public' are the subjects of state and states have the prime responsibility of detention, prevention and investigation of crimes through the law enforcement machineries. The Cybercrime reporting portal is an initiative of the Ministry of Home Affairs, Government of India under National Mission for the safety of women to facilitate victims/complainants to report cybercrime complaints online. The portal was launched on a pilot basis on August 30, 2019. It enables filing of cybercrimes especially against women, children. Key cyber security policies launched by the Government of India

1. The Government of India introduced the National Cyber security Policy in the year 2013 to deals with the planned course to defend the country's cyber ecosystem.
2. National Critical Information Infrastructure Protection Centre (NCIIPC): was established in 2014 to protect the India's critical information infrastructure against cyber-crime and terrorism.
3. National Cyber security Coordination Centre (NCCC): In 2017, the NCCC was created in order to spread awareness of Cyber Crimes in the country. 1.

In the year 2017, Cyber Swachhta Kendra was brought into light for internet users to clean their computers and devices by throwing out viruses and malware.

4.government of India created a fund of Rs.5 crores Promoting research and development to support the cyber security in the country.

4.Sectorial and state CERTs: Computer Emergency Response Team (CERT) is a team of experts was computer which looks after managing the security incidents. The government of India has introduced CERTs in Power and Finance sectors.

The National Commission for Women on 23rd of September 2014 has submitted a report on "ways and means to safeguard women from cybercrimes" which inter-alia recommended for stringent law, Policy to discourage and combat cybercrimes.

Ministry of Home Affairs has developed a portal [www.cybercrime.gov.in](http://www.cybercrime.gov.in) to enable people to report cybercrime complaints. Ministry of Electronics & Information Technology has issued an advisory on functioning of Matrimonial website on 6th June, 2016 under IT Act, 2000 and Rules made there under directing the matrimonial websites to adopt safeguards to ensure that people using these websites are not deceived through the means of fake profiles or misuse/wrong information posted on the website.

The Ministry of Electronics & Information Technology (MEIY) has set up Cyber Forensics Training Labs in north-eastern States and cities such as Mumbai, Pune, Kolkata and Bangalore to train State police officials and judiciary in cybercrime detection and collection, preservation and seizing of electronic evidence and dealing with cybercrime.

The number of complaints received in National Commission for Women and closed under category of Cybercrime against women during last four years is as under:

Year	Received	closed
2014	209	53
2015	223	86
2016	311	119
2017	370	250

As per laid down procedure these complaints are taken up with concerned authorities including police authorities.

National Commission for Women had provided comments on project "Cyber Crime Prevention against Women and Children (CCPWC)" under NIRBHAYA Fund. The Empowered Committee constituted under the Chairmanship of Secretary, Ministry of Women and Child Development has already approved the project "Cyber Crime Prevention against Women and Children (CCPWC)" of Ministry of Home Affairs.

#### CONCLUDING REMARKS

Cybercrimes against women is increasing on a rapid rate on the global level and it is very difficult to track

down the offenders committing cyber violence as it is very easy for a person to fake his identity and be hidden from the authorities. Hence, there is much need to create awareness and enactment of necessary legislation throughout the globe for prevention of computer related crimes.

The enacted laws to tackle offences against women in cyber world are not adequate enough to fully counter them. The mental and physical agony that women and children in cyberspace are experiencing is not completely reflected by these laws. The IT Act, 2000 has an overriding effect over the IPC provisions while governing the cybercrimes, there are numerous cybercrimes that are not extensively dealt by the IT Act, 2000. Still there is dire need to bring out special legislative provisions to change and evolve as quickly as hackers do if it has any hopes of controlling cybercrime.

#### REFERENCE

- [1] Mayura U. Pawar, Archana Sakure .Cyberspace and Women International Journal of Engineering and Advanced Technology (IJEAT)ISSN: 2249 – 8958, Volume-8, Issue-6S3, September 2019
- [2] Halder D. & Jai Shankar, K. Cyber victimization in India: A baseline survey report. Center for Cyber Victim Counselling Tirunelveli, India. 2010 Available at [http://www.cybervictims.org/CCVCresearcher report 2010.pdf](http://www.cybervictims.org/CCVCresearcher%20report%202010.pdf) (Accessed on 2020.01.11)
- [3] The Information and Technology Act 2000
- [4] Press Information Bureau Government of India Ministry of Women and Child Development on 28 DEC 2018 4:33PM by PIB Delhi