Cyberspace and Women: A Research

Mayura U. Pawar, Archana Sakure

Abstract:-With the fast-growing reach of the internet, speedy spread of mobile information and the escalated use of social media, our lives being inextricably mixed with online media has purported the emergence of crimes committed in cyberspace. This advent of technology has led to the emergence of cyber violence against females of all age groups which is posing a problem at the global level as it causes danger to the security, dignity and privacy of a human being as a whole. The cyber space has a virtual reality in which the criminals commit crimes by faking their identities and then hide in the same space provided by the internet. The legal structure of India is not yet well-equipped to deal with cybercrimes and also the lack of awareness leads to the unstoppable commission of these offences.

The paper discusses the major reasons for the growth of cyber violence against women in the arena of cyber socialisation. This paper also recognizes the common types of cybercrimes against women, which are namely cyber stalking, cyber pornography, circulating images or video recordings of females becoming involved in intimate acts, morphing, sending obscene or defamatory messages or e-mails, blackmailing or threatening, trolling or bullying and impersonation. The paper discusses the substances of every type of offence, analyse the relevant laws and highlight the cases and their judgements on this matter.This paper seeks to introspect the gaps between cybercrimes against women and the laws made to protect them. This paper will also recommend the steps that are required to be taken up in order to mark cyber crimes against women and girls in a holistic and efficient way.

I. INTRODUCTION

The internet is one of the most significant invention in the communication sector with the help of which, people living across the globe can communicate with each other without realising the distances between them. It has diminished the boundaries among people and provides them with opportunities to make better relations at both the personal as well as the professional fronts.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 is expected that the same would increase to at least 336.7 million by 2020

Though, it is a boon on one side, but 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 with the emergence of internet. The advent of technology has led to cybercrimes and victimization of females and it is a great threat to the security of a person as a whole.

The question that arises here is that what exactly the term cybercrime means? It is a term of any illicit activity that involves the use of a computer as its elementary means of the commission. It is a wrongdoing which is committed against a single individual or a group of them with a criminal mind to intentionally cause harm to the dignity of the sufferer or to cause physical or mental trauma to the victim in any manner, direct or indirect, by way of modern telecommunication networks like the internet.

Although, the number of people using the internet in India is increasing day by day but there is some gender disparity which is clearly visible among the social network users. This can be seen in various fields such as the number of people using the internet as well asthe number of people using Facebook or Twitter or Instagram and so on. The imbalanced number of users on the internet is the major contributor of this phenomenon. It is very closely related to the escalating incidents of cybercrimes against females.

Coming to the legal framework in India to combat cybercrimes, essentially, there are majorly two statues that address cybercrimes against females. Namely, they are the Indian Penal Code, 1860 and The IT Act, 2000. The IPC does not specifically talk about cybercrimes, rather it is general criminal law, which defines the different offences and specifies punishments to be awarded for the commission of those offences. It should be taken into notice that the offences listed in the code are addressed for their commission in physical or tangible or the real world. The provisions of the IPC are relevant to cyber violence against females via legislative amendments and judicial interpretations. The IT Act covers majorly commercial and economic crimes but there are no specific provisions to cover cybercrimes against women.

Access to the internet is the need of every person and therefore, it is rapidly turning into a necessity for financial prosperity and is being viewed as a basic human right. Thus, it is important to make sure that this digital public space is a guarded and enabling place for all, including females of all ages.

II. MAJOR REASONS FOR THE GROWTH OF CYBER VIOLENCE AGAINST WOMEN

The usage of the internet for criminal activities causes big threat to the society in the form of cyber violence and the major victims of this crime are females of all age groups. According to studies, it has been shown that the number of users which was 52 million went up to 71 million in 2009. In these users, 8% of the users were working women and 7% of the users were non-working women in 2009 and 37% of all the users used the internet by way of cyber cafés. What commonly happens is that the cyber café owners leak the personal and essential data of the internet surfer which is

Revised Manuscript Received on 14 August, 2019.

Ms.Mayura U. Pawar, Assistant Professor of Law, New Law College, BharatiVidyapeeth Deemed to be University, Pune, India.(Email: mayura.pawar@nlc.bvdu.in)

Ms.ArchanaSakure, Assistant Professor of Law, New Law College, BharatiVidyapeeth Deemed to be University, Pune, India.(Email: archana.sakure@nlc.bvdu.in)

then used for illicit activities. Although, the advancement of technology is a productive facet that can be taken into account to be vital for the development of the nation but at the same time, it is also resulting to be the foundation towards increasing of the offense rate with technology being against the fragile sector of the community.

The constant increment in cyber violence against females against women is due to the following reasons:

(1) Easily available information of the victims:

Social networking websites are made for people to connect to each other even at long distances and also to let people know each other. To show the presence of a profile, the users have to put their personal data like age, phone number, residential address, marital status, and so on. Though some of these websites give users the publication of their information as an option and even making profiles with fake names is totally allowed but the first-time registrants, including females give away their private info on the internet through these websites without even knowing the menacing effect of publishing such information. This information is visible to the public and is then used by the perpetrator to victimize women.

(2) Ignorance and carelessness of the users:

The social networking websites provide for several options to keep the profiles secure and keep oneself protected from being harassed in numerous ways such as putting up security measures and giving options to lock the personal photos, albums as well as messages. A user can also block a harasser which permanently hides the profile and cannot be found on the website by the harasser. Further, there are options like with whom to share information, a user can select to share it with only the members or with the public or with just oneself. Even after all these security measures provided by the social networking websites, women are prone to all types of cyber violence such as stalking, morphing, hacking, cheating, defamation and sexual abuse on the online platform. Some females had oral arguments with their group mates and they suspected that their user profiles on the website were hacked by some people. Very less number of women are aware of their legal right to protect their privacy from any outside intervention on the social networking website although many women experience cybercrime more or less and in some or the other way.

(3) *Hiding one's real identity under fake profiles:*

The fundamental right of freedom to speech and expression has encouraged the right to be unidentified on the social media. These websites provide space for changing names, addresses and other personal details regularly. This was done by social networking websites to allow a user to change their physical condition and geographical location from time to time so as to get in contact and interact with the other member on that website but, this has resulted in the other way around where the perpetrators commit crimes and get a blanket to hide under different identities which are fake. These fake account users have put females in more danger and risk on the social media.

(4) Torpid reaction of social networking websites:

Cyber socializing is dangerous because of the lackadaisical response of the social networking websites. Almost all of these websites have the option of reporting the abuse of any of the services provided by them, i.e., harassment, bullying, threatening, pornography on these websites can be reported by the users.But in maximum of the cases, social networking website have their own policies to declare that a post is defamatory or harassing. It is not virtuous on their part that most of these websites put up in their privacy policies that any type of harassment caused by one user to the other user is not their responsibility and they won't be responsible in any way for the same. However, these websites do provide important safety tips for the users in their settings menu bar which give a warning to the users that their profile might be removed if it is found harassing other users or creating hate campaigns which request pornographic material and so on, but unfortunately, these guidelines are not adhered to properly.

(5) Lack of adequate laws, statutes and legal provisions:

The most usual types of abuses on the social networking websites are not identified by any uniform statute, convention or rules. Furthermore, most of these socializing websites are registered in the United States and so they are governed by their laws. The U.S. laws provide immunity to these from being sued as defamatory media according to Section 230 of the Communication Decency Act, 1996. In India, the Information Technology Act which was enacted in 2000 and later amended in 2008 and the Indian Penal Code take into consideration these offences but they are not adequate enough as they do not recognize all the offences. The offences of bullying, harassment, profile cloning, etc. have not been recognized by these statutes. Therefore, the lack of adequate laws to govern the social networking websites, lack of identification of offenses against females and award sentences for the offences committed in cyberspace is a vital reason for the increment of victimization and cyber violence against women.

III. TYPES OF CYBERCRIMES COMMITTED AGAINST WOMEN

(1) Cyber Harassment:

This is a form of harassment, including blackmailing, threatening and continuous sending of love letters by fake names or constant sending of embarrassing e-mails to the mail box of some other user. This of behaviour is intended to disturb a person through the usage of internet. Sexual harassment is a specific type of harassment which is particularly sexual in nature, among several other types of them, it vitally takes into consideration constant and undesirable sexual activities.

(2) Cyber Stalking:

Cyber stalking is one of the most talked about cybercrimes in the modern day. It takes into account following the movements of a person all over the internet by

sending messages which are sometimes threatening on the bulletin boards and going into chat-rooms frequently visited by the victim, consistently bombarding the mail box of the victim, etc. The offence of cyber stalking is generally committed by men who stalk women or by adults who stalk the children or by paedophiles.

(3) Cyber Pornography:

It is defined as the posting of sexual substance on the internet. This is again a threat to female internet users as they don't even know that which of their activity is being recorded and might then go viral all over the web. It is a non-consensual activity wherein pictures and videos of the victim are obtained by certain ways such as hacking into the computer or phone of the victim, via social media accounts, etc. and these harm the life of the victim in the real world. This offence has been covered under the IT Act, 2000 to some extent under Section 67.

(4) Cyber Defamation:

Defamation is a tort and cyber defamation is when the defamation is committed by the use of computers and on the internet. It happens when people start publishing defaming statements or obscene material on various social networking websites on the online platform. The bulletin board of a user is open to be accessed by all other users which means that anyone can post defamatory statement on their board and then it is visible to everyone. Cyber defamation is also called as cyber smearing.

(5) Morphing:

It is to make a picture look different completely or partially form what it originally looks like by a fake identity. The offenders download photos of women from their social media accounts and edit (morph) them and then again upload the new picture in the name of a fake account. Morphing is generally done with two pictures wherein one picture is mixed with another picture and shown in a compromising situation or position which make it look like the women is indulging in the act portrayed in the picture. After this comes blackmail, where the woman is threatened to do something and if not, the pictures would go viral all over the web which will lead to embarrassment of the woman in the community and her status will be diminished too. The offenders committing this crime are booked under Section 43 and Section 66 of the IT Act, 2000.

(6) Email Spoofing:

Email spoofing is to change the real origin of an email in a fraudulent and illegitimate manner. The header part of the address and the sender's address is changed in such a way that it is not possible to recognize that the email has been spoofed and looks like that it as been sent from a different source. Men generally send their obscene and vulgar photographs to women via such emails, glorifying their beauty, demanding favours for them and asking for a date or for the price the woman would take for a night with them.

IV. LAWS, STATUTES AND LEGAL PROVISIONS IN INDIA AND THE GAPS

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 in 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. Halder in 2013 had put forth that, "It is definitely a welcome move as India may get a law focused solely on the victimization of women through indecent portrayal, but at the same time, the concept of indecent representation of women must be freed from patriarchal meanings of social value and morality". Her words indicated that, to bring such reforms and change the position of women in the country as well as to provide justice to the victims of cyber violence,the initial need is to change the mentality that people have.

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 likedefamation, 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 areprimarily 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. The IPC which also governs cybercrimes to some extent has Section 354 which gives punishment for the offences of voyeurism, stalking and sexual harassment.

The police are not equipped enough to deal with the electronic records due to lack of knowledge. It is easy for the police to arrest a person for cybercrime but it is difficult for the police to charge sheet them as the police is not well-

equipped for the same. Due to the lack of knowledge it becomes difficult for the police to track the authentic origin of the message used for cyber violence. Data about a person being arrested for cyber violence can be found from the news media but no updated data is easily available regarding the charge sheeting or the conviction of the accused and it's often a case that the people arrested are not charge sheeted and thereby acquitted by the court. Registration of a crime is not of major importance until and unless charge sheeting, conviction and acquittal are considered as it is not practicable to understand the complete situation. Many a times, the case is that the cybercrime against women occurs within marital relations wherein the husband who is alienated from the relationship posts obscene pictures of his wife, in such cases it becomes difficult and complex to prove the consent of the victim. Further, one more reason for the smaller number of complaint reports is that women are not aware that such laws exist which protect their privacy of body as well as of all physical activities. This scenario is going to be the same if the work of the law enforcing is going to be limited to the registration of cases and then their investigation. Significant measures must be taken up by the police, authorities and local administration to make people aware and sensitize them about the purview of laws and that the involvement of the civil society needs to be done. It seems through the laws that the state is in a paternalistic role controlling the sexual conduct of the people. The motive of law in these times is to control the generation of virtual material that might lead to uncontrolled sexual life of people; rather it should be to protect the dignity, security and privacy of females. The negative approach of the state can be clearly seen by the use of the words 'lascivious' and 'prurient' interest towards sexuality. The body of a female is depicted as a medium which has the power to make people dishonest and unprincipled. Further, there is large gap between arresting and charge sheeting of accused and suspects. This lower rate of charge sheeting indicates the deficient investigation procedure.

According to the IT Act, the investigation must be done by a police officer not lower than the rank of an inspector which in many cases, results into inadequate enquiry because of the shortage in manpower. Also, there is major requirement of proper training of the officers who enquire the matters of cyber crime is also a vital part as such investigation involves technology or it becomes difficult to track down the offenders and impart justice to the victim. Moreover, the police stations which are in charge of looking into matters of cybercrimes need to work in close coordination with the CID (Criminal Investigation Department), DD (Detective Department) and women's police stations. This coordination is important as these departments are trained enough to look into these cases but this this coordination is missing till date.

There are various NGOs like All India Women's Conference SakshilNavjyoti etc. which provide help in these matters. The judiciary needs to be made aware about keeping electronic records and also hoe to deal with them. Other than the judiciary, even the police needs to be made more well-acquainted in tackling electronic records. The lack of compatible evidence makes it difficult to reach justice for the victims and convict the perpetrator.

V. IMPORTANT CASES AND THEIR JUDGEMENT

1. *YogeshPrabhu v. State of Maharashtra*

This case was decided by M. R. Natu in July, 2015 who was the then Additional Chief Metropolitan Magistrate. This judgement was the first conviction awarded in any case of cyber stalking against a woman. Initially, in 2009, the woman started chatting with the accused YogeshPrabhu on a social networking website. Yogesh proposed her for marriage and she turned the proposal down. After this also, she received messages continuously but she stopped responding towards them and ignored them as she suspected his strange behaviour. She blocked him on the website so that he couldn't find her. However, he kept stalking her and after few months, he started sending her emails consisting of obscene images and video clips from an unknown account. Seeing this, she lodged a police complaint which was later taken up by the Cyber Crime Investigation Cell for investigation. The IP (Internet Protocol) address of the device was tracked down and it was found to be of a firm named 'Vashi' of which, YogeshPrabhu was an employee. The investigation was done and the accused was convicted under Section 509 of IPC and Section 66E of the IT Act which was the then followed provisions.

2. *SuhasKatti v. State of Tamil Nadu*

This case was decided by a court of Chennai in November, 2004. It was the first conviction awarded in any case of cyber pornography of a woman. The victim was a divorcee and she started receiving messages by the accused after she had turned down the proposal of marriage given by him. The accused man was sending her obscene, annoying and defaming pictures in a chat group of Yahoo by a fake e-mail ID in the name of a female. The victim was also being called by people on phone who believed that she was soliciting for sexual activities. The victim lodged a police complaint stating the above problems being caused to her which were further investigated by the Chennai Cyber Crime Cell. On the completion of the investigation, the accused was convicted for a period of 2 years of rigorous imprisonment and a fine amounting to Rs. 500, further, one-year simple imprisonment and Rs. 500 fine, this sentence was awarded under Section 469 and Section 509 of IPC respectively. Moreover, he was awarded conviction of rigorous imprisonment for 2 years and fine of Rs. 4000 under section 67 of the IT Act.

3. *Avnish Bajaj v. State*

This case was decided by Justice S. Muralidhar of Delhi High Court in May, 2008. It is a very well-known case of voyeurism which is also known as the Delhi Public School MMS incident of 2004. It took into account the making of a pornographic video recording of two school students engaged in sexual activity and it's illegal circulation among students in the form of a MMS. Also, the video was bid to auction on the website named eBay India. Legal enquiry was then initiated against Chief Executive Officer of eBay

India and sentenced under the IT Act.

4. Saddam Hussain v. State of Madhya Pradesh

This case is important as it shows that cases of cybercrimes are taken very seriously by the courts. The modesty of the victim was caused indignation by the accused. The accused video clipped the same in his mobile and then blackmailed her to do favours for him. A criminal complaint was filed by the victim under Section 507 OF IPC, Section 354D of IPC and Section 66A of the IT Act. The petition was filed in the MP High Court pleading for overturning on the premise of a settlement reached at between the victim and the accused. The HC denied to do this and affirmed that these offences affect the society at large and any kind of private settlement between the parties won't stop the proceedings of the case.

VI. RECOMMENDATIONS AND REMEDIES& RESULTS

1. Cybercrime against women is increasing on a rapid rate on the global level and this is of great worry all over the world. 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. Stricter rules and laws are needed to be formulated and applied on the Internet Service Providers (ISP) as it is them who have the full record of the data and history accessed or being accessed by any user who is surfing the internet. A rule must be made wherein, the ISPs must be bound to report any kind of suspicious activity taking place on the online platform by any user, this will help in combatting cybercrime on a very early stage.
2. Law makers should make severe regulations for cyber cafés, wherein the café owners should keep a record of the customers visiting the café and using their systems. Also, the browsing history of a user should be tracked to check for any suspicious activity and such activity should be reported. Offenders generally use systems from the cyber cafés to indulge into illegal activities so that they can not be tracked by the IP address and they go untracked by the authorities and therefore result into unsuccessful investigation.
3. People need to be aware of such crimes and the laws provided for them by the state. People should know their rights and the provisions under which they can seek justice. People need to be attentive that which of their activities are likely to be recorded and should be cautious about them. Awareness among people should be spread by the state by campaigns, posters, drama, etc.
4. The police should be made more well-equipped and trained in technology so that they are able enough to track the perpetrators. Shortage of manpower should not become a reason of insufficient investigation; more cyber cells should be created for successful investigation of cybercrimes.
5. Victims of cybercrimes should contact their nearest women assistance cell or NGO as son as possible. These platforms assist women and guide them about the laws present and the procedure of investigation so as to seek justice. Also, the involvement of these institutions and organisations makes sure that the police and other authorities are not taking any case lightly.
6. Copies of any suspicious chats should be saved by women which will further act as evidence in investigation. This will be helpful for the victim if the harassment continues and the victim wishes to file a complaint with the authorities.

VII. CONCLUSION

Several forms of cybercrimes against women are in action in India during the present times. The need of the internet and its importance has made it a vital part of everybody's life. People of all ages use internet and it brings with itself both pros and cons. Cybercrimes against women is not limited to India, rather it is a global phenomenon. Also, it is a huge matter of concern among countries because of its continuous growth.

The legal provisions enacted to tackle cases of cybercrimes are not adequate enough to fully counter them. The ground realities of what women facing cybercrimes experience are not completely reflected by these laws. 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.

Thus, to combat cyber violence against women in India, not only severe legislative changes are required but also awareness is needed on the large scale. These reforms can not be brought by just a group of people, rather several institutions like NGOs, women assistance cells as well as the government need to join hands to bring them in action.

REFERENCES:

1. Sarda, M., Deshpande, B., Shringarpure, S.: "Smart city – Use of technology and the needed labor reforms", International Journal of Innovative Technology and Exploring Engineering 2018.
2. Sarda, M., Deshpande, B., Deo, S., Karanjkar, R.: "A comparative study on Maslow's theory and Indian Ashrama system", International Journal of Innovative Technology and Exploring Engineering, 2018.
3. Sarda, M., Deshpande, B., Dharm, J., Dhere, V.: "Different aspects of environmental laws", International Journal of Recent Technology and Engineering, 2019.
4. Deshpande, B., Girme, A. : "Research methods made simple", International Journal of Innovative Technology and Exploring Engineering, 2019.
5. Girme, A., Deshpande, B.: "The life line of human beings–"Right to potable water", International Journal of Recent Technology and Engineering, 2019.
6. Sinha, S., Deshpande, B., Deo, S., Vedpathak, S.: "Potential appeal mechanism by consent: Arbitration", International Journal of Recent Technology and Engineering, 2019.
7. AsthaSrivastava, Cyber Delinquency: Issues and Challenges under Indian Legal System, nternational Journal of Engineering and Advanced Technology (IJEAT) 2019
8. Anuradha G, Revolutionary Yogic Agriculture, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3, September 2019

9. Deo, S., Deo, S.: "Cybersquatting: Threat to domain name", International Journal of Innovative Technology and Exploring Engineering, 2019.
10. Deo, S., Deo, S.: "Domain name and its protection in India", International Journal of Recent Technology and Engineering, 2019.
11. Dubey, R., Sakhalkar, U.: "A critical analysis of rising intolerance and growing polarisation: Lynching", Journal of International Pharmaceutical Research, 2019.
12. UjjwalaSakhalkar, Community Participation for access to Justice to children: A road map for future, International Journal of Recent Technology and Engineering,2019.
13. SalilShringarpure, Internet Trolling: Analyzing the legal myths and facts, International Journal of Engineering and Advanced Technology, 2019.
14. Shaikh, A., Khandare, J.: "International parental child abduction in United States of America and India", International Journal of Engineering and Advanced Technology, 2019.
15. Khandare, J., Shaikh, A.: "When life becomes death: A stifling story of air pollution", Journal of International Pharmaceutical Research, 2019
16. Pathak, A., Mishra, A.: "Human trafficking in India", Journal of International Pharmaceutical Research, 2019
17. Bendale, U., Dhere, V.: "Right of aged persons to live with dignity: A socio-legal perspective", International Journal of Innovative Technology and Exploring Engineering, 2019
18. Dhere, V., Bendale, U.: "Impact of smart city on social relations", International Journal of Innovative Technology and Exploring Engineering, 2019.
19. SukrutDeo and Dr. SapnaDeo, "Cybersquatting: Threat to Domain Name", International Journal of Innovative Technology and Exploring Engineering, 2019