CYBERCRIME AGAINST WOMEN IN INDIA

Kamireddy Chathurya Reddy
Department of ECE, Velammal Institute of Technology, Chennai, Tamilnadu, India
Divya.B
Department of ECE, Velammal Institute of Technology, Chennai, Tamilnadu, India
Vijay M
Department of ECE, Velammal Institute of Technology, Chennai, Tamilnadu, India

Article history:	Abstract:
Published: 10th March 2022	Indian civilization is one of the world's oldest civilizations. Women in India are been given as specific status in our country. They are treated as if they were goddesses. However, as society has modernized, these fundamental rights have been violated. In the realm of information technology, India is rapidly developing. People's day-to-day activities are increasingly reliant on computers. The year 2000 was a watershed moment in technological history. With the widespread use of computers, cybercrime is on the rise. Individuals' lifestyles have changed dramatically in this current era of globalization, and technological advancements have rendered man reliant on the internet for all of his requirements, either directly or indirectly. Individuals' lifestyles and working situations have been influenced by the advancement of the internet in both positive and harmful ways. Cyber-crime has become an issue as a result of this increase in technology and internet-based lifestyle. Cyber-crime is described as an illegal conduct that involves the use of the internet and computer systems as a tool, a target, or both. It can take many forms, including hacking, phishing, cyber terrorism, spoofing, stalking, data diddling, and so on. However, in terms of women's safety, when cyber-crime rises, "WOMEN" are disproportionately affected and become victims of cyber-crime such as pornography and cyber-stalking.

Keywords: Cyber security, Information Technology, Cyber-Crime, Women Safety.

1. INTRODUCTION

Women have been victims of various types of harassment for many centuries till now. Domestic violence, Sathi Pratha, acid-attack, rape, eve-teasing, sexual harassment, dowry death, molestation, kidnapping, honor-killing, female infanticide etc. are some forms which come into the category of violence against women. Recently, a death due to brutal gang rape of 23 year old paramedical student in New Delhi on December has put a spotlight on violence against women and caused to first time widespread protests by Indian people across the country that raised the hand against violence of women in India. The United Nations defines violence against women as "any act of gender-based violence that results in, or is likely to result in, physical, sexual or mental harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life [3]." Acc. to Swapna Majumdar, "Violence against women is neither culture nor region-specific; it cuts across community and class. Shocking though it is, the fact is that violence against women has become an acceptable norm of life because women accept violence as a part of their married life until it becomes intolerable [4]."

We all celebrate the international women day on 8 March every year for showing our respect, love, affections and appreciations towards women for their economic, political and social achievements in various fields. Even in India women are worshiped as goddess (Devi, Kanya, Mata etc.) but reality shows a bleak and worsening picture of this. In fact, women are worshiped only at religious places or on religious programs or festivals, but in the common life they are exploited in various ways and have always been victims of physical, psychological, sexual exploitations etc. India has become a worst place in the world for women exploitation. It feels proud itself because it is considered the largest democracy in world, but recent Delhi gang rape of a woman in running bus, wife battering, dowry harassment, dowry death, molestation, kidnapping, domestic violence, female infanticide , honor-killing, cyber violence etc. reveal the actual picture of India that how difficult life of women in the Indian Democracy. Indian Constitution mentioned equality for all in its Preamble e.g. "to secure to all its citizens, social, economic and political justice, liberty of thoughts, expressions, belief, faith and worship; equality of status and opportunity; Fraternity assuring the dignity of individual and the unity of the nation". But in spite of this, women are unable to get their rights as that of men (Pachauri 2010:1). The condition of violence against women is becoming grimmer day by day with its changing forms.

Now violence has taken new form against women, as it is changing because of technology which is called cyber violence that is the main focus of this paper. Incidences of online violation against women in India are quite high and these are believed to be on the increase. Cyber violence is a new form of violence against women which is facilitated by internet and information technology. Women are more prone to victimization than men in cyber space and most of them receive mails from unknown men with disturbing contents or texts, friend requests etc. which may be the result of data mining. Many women who do not mind to share their accounts and passwords with their spouses, boyfriends, are victims of harassment meted out by their ex-partners who exploit them by blackmailing, posting their pictures on internet sites which go viral, and by taking revenge through cyber space for breach of romantic commitments etc. Impersonation, emotional cheating, victimizing by making cloned profiles in the cyber space are growing in India and less awareness too causes the cyber victimization [6].

75% victims are believed to be female but these figures are more on assumed basis. The actual figures can really never be known because most crimes of such types go unreported having no a direct physical threat and are not much clear or implemented properly .This is why cyber-crimes against women are on the rise. Social branding expert Sanatan Baweja said that, "when you know there is no clear law about what is offensive the fear goes away [7].This paper has used various primary and secondary resources like book, reports, articles, news, web and electronic sources etc in order to carry out the study which supports the research paper to justify problems and arguments.

2. CERTAIN FORMS OF CYBER OFFENCES AGAINST WOMEN
In common parlance, Cyber-crime can be defined as any illegal activity for which a computer is used as its primary means of commission. Cyber Crimes are crimes which may be committed against persons, property as well as government.

Cyber space's have become havens for cyber criminals. Women are the most soft and vulnerable targets over the internet and it became a cakewalk to target the less aware individuals. Social networking platforms are the most prone areas to victimize people and especially women. The most common cyber-crimes inflicted to women are harassment via emails, cyber stalking, cyber pornography, obscenity, defamation, morphing and email spoofing [9]. The cyber world in itself has a virtual reality where anyone can hide or even fake his identity, this gift of internet is used by the criminally minded to commit wrongful acts and then hide under the blanket provided by the internet.

Women especially young girls inexperienced in the cyber world, who have been newly introduced to the internet and fail to understand the vices of internet are hence, the most susceptible to falling into the bait of cyber criminals & bullies.

Some of the prominent cyber-crimes against women are:
1) Violation of body privacy.
2) Online harassment.
3) Cyber stalking.
4) Exposure to online fraudsters.
5) Portraying women in a most indecent manner.
6) Workplace harassment with digital aid.

3. REASONS FOR THE GROWTH OF CYBER CRIMES AGAINST WOMEN
According to the official statistics provided by the National Crime Records Bureau, Government of India, 9622 cases of cyber-crimes were registered in 2014 and 5752 persons arrested. In 2015, 11,592 cases were registered an increase of 20% in registration of cases from the previous year – and 8121 persons arrested [12].

Thus, it is crystal clear that the cyber-crimes against women in our society have taken a toll since the introduction of information and technology and access of internet in almost every hand. And it is high time that there should be a strict involvement of legislature as well as the executive to curb the same.

Some of the prominent reasons for the growth of cyber-crimes against women can be regarded as:
1) The transcendental nature of the internet-no boundaries, ever changing.
2) Low equipment cost.
3) Numerous vulnerable targets- Loneliness is a prime cause as many female students and staff live away from their family and work for long hours over the computers. Thereby, the computers become their trusted pal.
4) Easy concealment due to anonymity.
5) Cyber-crimes in most of the cases are not even reported due to the fear of society, hesitation, shyness and fear of defamation.
6) In most cases, such cyber-crimes are not even addressed due to the hesitation and shyness of the victim and her fear of defamation of the family's name in the society.

However, even today the Indian police tends to not tends to take cybercrimes seriously. In such scenarios, the woman or the young girl who falls prey to cyber victimization should first contact a women assistance cell or NGO

(such as All India Women's Conference7, Sakshi8, Navjyoti9, Centre for cyber victims counselling10) which will assist and guide them through the process, also this will make sure that police does not take any case lightly.

The main reason for the increased number of cyber-crimes against women in India can also be regarded to as due to lack of legal security. The need of the hour is to make stringent laws and the proper implementation of such laws should also be ensured. The Government and the legislature should be made accountable to take effective steps in furtherance to protect women from cyber-crimes.

On the other hand, humiliation, mental torture, stress, depression aggravates the situation. On account of delayed justice, people have lost faith in the law enforcement authorities. Lack of legal awareness makes it more complex. Further, most women overlook the privacy rules and regulations listed on the social networking websites.

It is pertinent to note that the women themselves can help in regulating cyber obscenity by becoming aware of their rights and ensuring to abide by the safety measures provided and prescribed over the places. Some of the famous social media platforms provide wide options in their respective privacy policies to guard and protect women from such perpetrators.

At the same time, one should also bear in mind that, most of the popular websites declare their privacy policies that they will not take any responsibility for any sort of harassment caused to the users by other users. Therefore, before registering on every other social media platform, women should go through the privacy policies or safety measures related to such offences.

Negligence and non-vigilance in most of the cases is also a root cause in regards to women being the targets of cyber obscenity.

4. SOME SUGGESTIONS AND STEPS TO TACKLE CYBER CRIMES

Besides, depending on legal system against cybercrimes, women have to be aware of cyber victimization by self, because time has come to reject the acceptance of silent. Moreover cyber laws are not universal, as they vary country to country. Today, every netizen wants to browse web privately and safely especially women. We should take some steps to tackle this problem. Here are some steps and suggestions that how women can save themselves of being victimized in cyber space and how they can make their online perceptions and experiences a safer one, are as follows;

i. **Change passwords time to time:** In fact, we all love to have easy-to-remember passwords because, it is simpler. If one wants to lower internet crime risk, changing password is a great way to make personal data and social networks safe and difficult to access for cybercriminal (Pennelli 2012). Baffling or tricky password protect all accounts including cell phones, emails, landlines, banking, credit card etc. and are difficult for anyone to guess. Even, secret questions should not be easily answered [1,2]. Safest passwords contain letters, numbers and symbols. Avoid words that are in dictionary and any important dates and must use different passwords for different web sites [16].However, changing password can be very helpful to keep privacy safe. Regarding authentication, various biometric techniques are employed now with multimodal approach [18,19] which improves the efficiency.

ii. **Avoid revealing home address:** This is the rule for women in particular who business professionals are and very visible. They can use work address or a rent private mailbox. Thus, it can help them out in avoiding cyber stalkers [12].Moreover, women should avoid uploading more material on internet regarding their own information so that no one can easily access them.

iii. **Maintain stable social relationships:** It is also the fact that we all like to believe that we should have 2000 friends. Dunban's number[7] suggests a limit to the number of

iv. people, a human being can have a proper social relationship with, and that number is 150. Probably, we don't need those 2000 facebook friends, because we are likely physical unable to really know more than 150 of them. Maintaining a limit on the number of the people will ensure our information is distributed to people who you really know and away from friends-of-friends-of-friends who you actually do not know all too well [15].Women should make distance from impermissible friendships.

v. **Awareness campaign against cybercrimes:** Awareness campaign must be set up from the grass root level such as schools, collages etc about cybercrimes like stalking cheatings, economic cheatings, defamatory activities, misusing emails and social networking websites, virtual rapes, cyber pornography, email spoofing etc [17].These campaigns can be fruitful in paralyzing cybercrimes.

vi. **Seminars and workshops for better understanding of cyber victimization:** Police, Lawyers, social workers, and NGOs must be invited to education institutes, clubs, corporate offices, awareness-campaigns, seminars and workshops to discuss about legalities and illegalities of cyber conduct among adults inclusive of both genders. Reporting of cyber victimization at all levels directly to the police and NGOs working

cybercrimes must be encouraged. Secondly, workshops and seminars must be conducted for the police personnel for better understanding of such kinds of victimization and quick responses towards the complaints. Academic and legal experts, NGOs etc. must be invited for such workshops and seminars

vii. **Rigid and stringent laws:** India must bring in more rigid and stringent laws for cyber-crimes against women in the cyber space. It is evident that present India's Information Technology Act includes only few sections for cybercrime, especially against women, hence to curb cybercrimes, either IT Act must be re-modified or a separate law on cybercrimes should be created [13]. Proper law and order against crimes may lead to create good society.

viii. **Beware of unsolicited calls and messages:** Woman should avoid unwanted or unsolicited phone calls and massages because cell phone may be monitored. If it happens again and again, you should try to record phone calls of harasser and report to the police. Even, they should download applications from trusted websites. Besides, they should discuss and share the problem regarding cyber harassing with their trusted ones like parents, mates or spouses etc.

ix. **Understand privacy settings of social network:** Social networks and other online content and service providers all have privacy policies and private settings. One must try to understand privacy policies and adopt privacy settings that help in protecting oneself from any potential risk or online harm. So, we must have the knowledge about privacy settings of social networking.

x. **Anti-Virus must always be up to date:** One must keep Anti-virus up to date. According to FightCyberstalking, Trojans, worms, and email viruses are common ways for would-be cyber stalker to access one's information. One must make sure that Anti-Virus is up to date to lessen probability that one's PC cannot be attached with a Trojan virus, email virus or worms. Thus, it may help us to keep away from the access of cyber harasser.

xi. **Check account regularly:** It is clear that every net user has its own account on network sites. We should regularly check our email, blog or website accounts etc. By doing so, we will be in-touch with our belonging accounts on internet and we can lessen the possibilities of hacking, stalking etc by reviewing our account. It is found that some women don't check their account after they make their accounts on internet. Unfortunately, when it is checked, they found themselves trapped. So, net user especially women must not ignore this.

xii. **Protect data on the move:** In our daily life, we often use public computers in internet cafes etc. You should remember that when you are using internet on public computers, web browsers can keep a record of your passwords and every page you have visited. So, you should not forget to erase your tracks or history on web browsers [8]. Your little negligence can put you in threat. In other words, women should be distrustful in nature while using internet because stalker may try to rip you off.

xiii. **Keep firewall turned on:** Firewalls are first line of cyber defense and block connections to unknown or bogus sites and keep away from some kind of viruses

xiv. and hacker. These firewalls are recommended for single computers and are prepackaged on some operating systems or can be purchased for individual computers.

5. ROLE OF GOVERNMENT

In May 2016, the Union Minister for Women and Child Development, Ms. Maneka Gandhi, observed that the online abuse of women in India ought to be treated in the same manner as violence against women in the real world, and created a new forum for redressal, and further instructed the National Commission for Women to create a system for taking action against online abuse of women.24

After consultation on Cyber Crimes in India held on 23.07.2014, National Commission for Women has submitted a report on **"Ways and Means to Safeguard Women from Cyber Crimes in India",** which inter-alia recommended for stringent law, Policy to discourage hacking activities, dedicated helpline numbers, opening of more cyber cells, and imparting of proper legal, setting up forensic labs and technical training law enforcement agencies like police& judiciary etc. to combat cybercrime.

There are adequate provisions dealing with cyber-crimes in the Information Technology Act, 2000 as well as the Indian Penal Code, 1860. Government has, in fact, taken a number of legal, technical and administrative steps in furtherance to prevent and curb cybercrimes. These inter alia, include:

i. Cyber Police Stations and Cyber Crime Cells have been set up in each State for reporting and investigation of Cyber Crime cases.

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

iii. Various steps have been taken by Ministry of Home Affairs, Meity and State Government to modernize the setup and equip police personnel with knowledge and skills for prevention and control of cybercrime through various national and State Police academies/judicial academies and other institutes.

iv. An advisory on functioning of Matrimonial website on 6thJune, 2016 under Information Technology Act, 2000 has been issued by the Ministry of Electronics & Information Technology. Rules are also laid down thereunder 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.

v. Computer Security Policy and Guidelines to all the Ministries/Departments has been issued and circulated by the Government on taking steps to prevent, detect and mitigate cyber-attacks.

vi. A portal namely www.cybercrime.gov.in has been developed by Ministry of Home Affairs to allow public to report cybercrime complaints.

6. CONCLUSION

It finds that gaining exposure to combat cybercrime against women in general is difficult, and the only way to do it is to understand cybercrime. Criminals perceive cybercrime to be easier than traditional crimes because there is less likelihood of getting discovered and fewer consequences. The government must enhance the legal system to reduce cybercrime. Second, society's perception or attitude toward women must be altered, since women must no longer be viewed as a commodity. People must realize that violence against women is merely a consequence of gender discrimination and power imbalances between men and women. Thirdly, women must recognize that the moment has come to break their silence or hesitancy and speak up against cybercrime and for their rights. Fourth, it necessitates ongoing research and attention to cybercrime. It should be thoroughly researched and sponsored by the government. Fifth, police officers must be trained in order to combat and respond to cybercrime. Workshops and seminars on cyber space education must be held for this aim. Women should take part in such activities as well. However, in the end, individuals must adjust their attitudes toward women and cultivate a feeling of community, because cleanliness begins at home. Swami Vivekananda had said "The nation which doesn't respect women will never become great now and nor will ever in future" and in order to make India a great nation, let us work towards giving women their much deserved status and place.

REFERENCES

1. Agarwal, Rohit. CYBER CRIME AGAINST WOMEN AND REGULATIONS IN INDIA. 2013. Accessed on: 24 July 2014. Available at: <http://www.tmu.ac.in/gallery/viewpointsdcip2013/pdf/track4/t-403.pdf>.
2. Cyber Stalking. 23 July 2014. Accessed on: 25 july 2014. Available at: <http://en.wikipedia.org/wiki/Cyberstalking>.
3. Doyle, Carmel. Top tips to avoid being a cyber crime victim. 7 Fabruary 2012. Accessed on: 18 July 2014. Available at: <http://www.siliconrepublic.com/digital-life/item/25681-top-tips-to-avoid-being-a-c>.
4. Empowering women against cyber-violence. 16 January 2011. Accessed on: 20 July 2014. Available at: <http://www.theborneopost.com/2011/01/16/empowering-women-against-cyber-violence/>.
5. Geetha, B. "Cyber crimes have grown in numbers and character. Women, the chosen victims of cyber crimes choose to remain silent about them due to outdated stereotypes — which complicates implementation of the IT Act Vulnerable in virtual space." The Tribune, Chandigarh (2011). Accessed on: 18 July 2014. Available at: <http://www.tribuneindia.com/2011/20111107/edit.htm#6>.
6. Halder, Debarati and K. Jaishankar. CYBER VICTIMIZATION IN INDIA. A Baseline Survey Report. Tamil Nadu: Centre for Cyber Victim Counselling, 2010: 1-22. Accessed on: 17 July 2014. Available at: http://www.cybervictims.org/CCVCresearchreport2010.pdf
7. HalDer, Debarati and Karuppannan JaishanKar. "Cyber Socializing and Victimization of Women." September 2009: 5-26. accessed on 17 july 2014. Available at: <http://www.doiserbia.nb.rs/img/doi/1450-6637/2009/1450-66370903005H.pdf>.
8. Kaur, Ek Ong Kaar. First Master of Sikh Dharma. n.d. Aceessed on 21 July 2014. Available at: <http://www.harisingh.com/FirstSikhOfSikhDharma.htm>.
9. Lagal Article. Cyber Defamation In India. n.d. Accessed on: 29 July 2014. Available at: <http://www.helplinelaw.com/employment-criminal-and-labour/CDII/cyber-defamation-in-india.html>.
10. Majumdar, Swapna. "Sexual control and Violance." The Tribune (2003).
11. Mali, Adv. Prashant. IT Act 2000: Types of Cyber Crimes & Cyber Law in India-Part 1. December 2011. Accessed on: 29 July 2014. Available at: <http://www.csi-

india.org/c/document_library/get_file?uuid=047c826d-171c-49dc-b71b-4b434c5919b6&groupId=10157>.

12. IT Act 2000: Types of Cyber Crimes & Cyber Law in India-Part 2. December 2011. Accessed on: 29 July 2014. Available at: <http://www.csi-india.org/c/document_library/get_file?uuid=2ce4b842-aca6-4f54-87b6-d778093925d9&groupId=10157>.

13. Manila, News Agency. "Cyber violence against women." 10 January 2011. The Brunei Times. Accessed on: 20 July 2014. Available at: <http://www.bt.com.bn/features/2011/01/10/cyber-violence-against-women>.

14. Moore, Alexis A. 12 Tips To Protect Yourself From Cyberstalking. 8 January 2009. Accessed on: 13 July 2014. Available at: <http://womensissues.about.com/od/violenceagainstwomen/a/CyberPrevention.htm>.

15. Online Privacy & Safety Tips. 2010. Accessed on: 14 July 2014. Available at: <http://nnedv.org/downloads/SafetyNet/OVW/NNEDV_OnlinePrivacyandSafetyTips.pdf>.

16. Pachauri, S. K. Women and Human Rights. New Delhi: S.B. Nangia, A P H Publishing Corpration, 2010.

17. Pennelli, Paul. Cyberstalking Awareness: Protect Yourself On-Campus and Beyond With These 7 Steps. 31 January 2012. Accessed on: 13 July 2014. Available at: <http://blog.gradguard.com/2012/01/cyberstalking-awareness-protect-yourself-on-campus-and-beyond-with-these-7-steps/>.

18. VijayM, Indumathi G. "GwPeSOA-basedMSVNN: the multimodal biometric system for futuristic security applications." Sadhana. 2018;43(12). http://dx.doi.org/10.1007/s12046-018-0967-y.

19. Mohan V, Ganesan I. "A nature-inspired meta-heuristic paradigm for person identification using multimodal biometrics". Concurrency Computat Pract Exper. 2021;e6420. https://doi.org/10.1002/cpe.6420