Journal of Advances and Scholarly Researches in Allied Education
Vol. XV, Issue No. 5, July-2018, ISSN 2230-7540

Cyber Crime, Victimization against Women in India and It's Preventive Measures

Shyamapada Ghorai[1]* Prof. (Dr.) N. K. Thapak[2]

[1] Research Scholar, Swami Vivekananda University, Sagar, M.P.

[2] Associate Professor, Department of Law, Swami Vivekananda University, Sagar (M.P.)

Abstract – Utilization of the Internet keeps on impacting both decidedly and negatively, the social, financial, social, and political parts of each society. Most women who approach Internet don't know about the threats ailing in the Internet. Violence against women is an infringement of human rights and not another marvel. It is continually requiring it shapes investment to time in Indian history. With the progression of time, numerous feminists battled against women violence and for their strengthening in the society, yet there is no closure of her powerless life and her misuse. Because of the data innovation which acquired an extraordinary upheaval the correspondence space for making world a 'Global Village' and giving equivalent acknowledgment of rights to women. Innovation of World Wide Web, cell phones and tabs and so on changed women's standard of living, in spite of the fact that, these developments accompanied immense advantages for us, however it too has some negative consequences for our life and made incredible danger which is commonly known as Cyber Crime. For the most part, cyber crimes happen against women who can be effectively misused. Because of absence of confirmations and dread of defamation, recognizing criminal is exceptionally hard. Cyber violence has presented women to cyber defamation, sexual harassment and abuse, pornography, email-misrepresentation and so forth, in this research study we studied about the cyber crimes against women in India, its Victimization and preventive measures to uphold for stopping them.

----------X----------

I. INTRODUCTION

Cyber crime is much similar to environmental change; it's global marvel. The security and protection of a person is in question because of advancement and spread of technology. This technology has exploited the fundamental bestial characteristics of man and now represents a noteworthy risk to women on cyber space. India is one of the first and couple of nations to enact enactments to battle cyber crimes. In any case, the issues of women still significantly stay immaculate. The act identifies various cyber based crimes, yet much is left to be wanted of arrangements for victimization of women. Joined States give an account of Internet and Computing Trends says Indians are the second biggest sharers of personal information over the internet after Saudi-Arabians. With the goal of security and advancement of internet business, Government of India enacted the Information Technology Act 2000, yet as far as computer mingling correspondence and cyber crimes, this act is insignificant gap filler. First showing up in William Gibson's sci-fi "Warlock", 'Cyber Space' is an amalgamated term for the inter-web of buyers, computers and networks that guide in the inter-availability of the world. This cyber space is "the all out inter-connectedness" of human creatures through computers and media communications, without respect to the physical geography. Then again internet was cloned from "interconnection" and "network" (Aggarwal and Kaushik Dr., 2014).

Women have been victims of different kinds of harassment for a long time till now. Abusive behavior at home, Sathi Pratha, acid-attack, rape, eve-prodding, sexual harassment, share death, attack, seizing, honor-killing, female child murder and so on are a few structures which come into the class of violence against women. As of late, a death because of fierce assault of multi year old paramedical understudy in New Delhi on December has set a focus on violence against women and caused to first time broad challenges by Indian individuals the nation over that raised the hand against violence of women in India (Aggarwal, 2013).

Table 1: Classification of Cyber Crimes

Crimes against person or Individuals	Crimes against Property	Crimes against State/ Society

Cyber Stalking	Hacking	Sale of illegal articles
Dissemination of obscene Material	Unauthorized access over computer system	Cyber terrorism
Harassment via email	Virus transmission	Intention to extract secret information from computer system
Unauthorized control/access over computer system	Computer vandalism	Illegal human trafficking online.
Defamation	Financial scams and Frauds	Online gambling
Pornography including (Child pornography)	Intellectual property Crime	
Indecent exposure 6 Internet time theft	Denial of service attacks	Polluting youth through indecent exposure
e-mail spoofing	Virus transmission	Distribution of private

II. CYBER CRIME AGAINST WOMEN

Criminal activities that is customary in nature, for example, robbery, extortion, phony, defamation and underhandedness, which are all subject to the Indian Penal Code. The abuse of computers has likewise brought forth a range of new age crimes that are tended to by the Information Technology Act, 2000. Which has been corrected a few times and most recent in 2008 to bring quickly developing cyber crimes under its ambit, we can for the most part arrange Cyber crimes in two different ways:

1. The Computer as a Target: - utilizing a computer to attack different computers. For example Hacking, Virus/Worm attacks, DOS attack and so on.

2. The computer as a weapon: - utilizing a computer to carry out true crimes. For example Cyber Terrorism, IPR infringement, Credit card cheats, EFT fakes, Pornography and so on.

The state of violence against women is getting to be grimmer step by step with its evolving shapes. Presently violence has taken new structure against women, as it is changing a direct result of technology which is called cyber violence that is the fundamental focal point of this paper. Rates of online violation against women in India are very high and these are accepted to be on the expansion (Geetha, 2011). Cyber violence is another type of violence against women which is encouraged by internet and information technology. Women are more inclined to victimization than men in cyber space and a large portion of them get sends from obscure men with exasperating substance or writings, companion demands and so on which might be the aftereffect of information mining. Numerous women who wouldn't fret to impart their records and passwords to their spouses, boyfriends, are victims of harassment allotted by their ex-accomplices who abuse them by coercing, posting their photos on internet locales which circulate around the web, and by rendering retribution through cyber space for break of sentimental duties and so forth. Impersonation, passionate tricking, defrauding by making cloned profiles in the cyber space are developing in India and less mindfulness also causes the cyber victimization.

75% victims are accepted to be female however these figures are more on expected premise. The actual figures can extremely never be known in light of the fact that most crimes of such sorts go unreported having no a direct physical threat and are very little clear or actualized appropriately. This is the reason cyber crimes against women are on the ascent. Social branding master Sanatan Baweja said that, "when you know there is no unmistakable law about what is hostile the dread leaves. Be that as it may, cyber crime against women in India should be contemplated in detail and it is the demand of great importance fixing the reins of cyber harassers. This paper principally centers around violence against women through cyber space and internet by representing a few instances of cyber victims. It traces the state of Indian women in Cyber space Side by side; it will find out the factors prompting cyber victimization against women. Despite the fact that, it is hard to stop cyber crime in general, the paper recommends a few answers for control the cyber-crime against women (Debarati and Jaishankar (2014).

2.1 Cyber Crimes Stance in India's

The Ministry of Information Technology was shaped in 1999, loaded with the gigantic obligation of making India and IT superpower by 2008. In under a year, India saw the enactment of its first rule identifying with Information technology dependent on the example of Model Law on Electronic Commerce, 1996, embraced by the United Nation commission on International Trade law (UNCITRAL). Another act utilized altogether for direction was Electronic Transaction Act of 1998 Of Singapore. The Information Technology Act, 2000 was passed by the parliament on May 15, 2000 and told to come into power on October 17, 2000.The Act, looks to secure this headway in technology by characterizing crimes, recommending disciplines, setting down methodology for examination and

framing administrative experts. Two sorts of meaning of cyber crimes can be given. In thin terms cyber crime comprises of just offenses referenced under the IT Act, 2000, though extensively talking cyber crime can be said to be an act of oversight, commission or perpetrated on or through or with the assistance of internet, regardless of whether carried out specifically or in a roundabout way and which is denied by any law for which discipline corporal or money related is given. The creator limits the extent of his research just to cyber crimes caused to women and referenced in the IT Act, 2000 (Manila, 2014).

2.2 Causes of Cyber-crimes against Women in India

Indian women residents are as yet not open to promptly report the cyber abuse or cyber crime. The most serious issue of cyber crime lies in the usual way of doing things and the intention of the cyber criminal. Cyber space is a travel space for some, individuals, including guilty parties. While individuals don't live in cyber space, they go back and forth like some other spot. This nature gives the guilty parties the opportunity to escape after the commission of cyber crime. Numerous websites and blogs give security tips to the wellbeing of women and youngsters in the net. Yet at the same time then cyber crimes against women are on rise. As a general rule it is seen many talk companions appreciate prodding their women companions by words, for example, —sexy, —attractive‖ which are the virtual start of cyber profanity (Pachauri, 2010). They gradually bring their female companions into certainty and begin talking about their own issues like a genuine companion. Thus in numerous events they are effective in transforming the net kinship into a solid bond and bit by bit continue to send vulgar or unfavorable comments. In the event that the beneficiary shies away, the sender of such messages would turn out to be progressively urged to proceed. The issue would be unraveled just when the victimized lady without even a moment's pause report back or even caution the abuser about taking solid actions.

III. LOOPHOLES IN INDIAN LAWS

Most likely Information technology act, 2000 has been passed by the Indian Parliament with the target to encourage to anticipate Cyber Crimes. Be that as it may:

1. Information Technology Act, 2000 nor characterizes "cyber crimes" neither utilizations this articulation, yet just gives the meaning of and discipline for specific offenses. In this manner two sorts of meaning of cyber crimes can be given. In thin terms cyber crime comprises of just those offenses which are referenced under the Information Technology Act, 2000, though extensively talking cyber crime can be said to be an act of oversight, commission or carried out on or through or with the assistance of internet, regardless of whether perpetrated specifically or in a roundabout way and which is restricted by any law for which discipline corporal or money related is given. In this setting it very well may be reasoned that Information Technology Act, 2000 gives discipline to just certain offenses and isn't thorough of all cyber-crimes (Ahmad, 2005).

2. S.79 of IT Act, 2000 sets down conditions under which ISPs or intermediaries are excluded from culpability for hostile substance transferred by an outsider. It commits the intermediaries to work out "due perseverance", and to act on the requests of the court or the legislature and its offices to meet all requirements for resistance.

3. Cyber defamation has been characterized under the Indian Penal code however not in the IT Act, 2000. S.67, 67A, 67B, and 67C can't be said to cover book, flyer, paper composing, drawing, painting, portrayal or figure in electronic structure if there is any open great resistance like item being of general concern or kept for trust religious objects is advanced.

4. Once more, under no section in IT ACT 2000, Obscenity – personal review – Is an offense, in fact like in IPC 292 again on the off chance that it is demonstrated that you have distributed or transmitted or caused to be distributed in the electronic structure at exactly that point under Section 67 it very well may be an offense. Last yet not the least, the IT Act 2000 does not specify the ordinary cyber crimes like cyber stalking, transforming and email mocking as offenses (Kashmiria, 2014)

5. A contrast among pornography and kid pornography has been perceived in United States of America's Communications Decency Act, 1996 and United Kingdom Obscene Publications Act, 1959. Comparative separations is given under the. No such separation exists under Section 292 of Indian Penal Code, 1860 identified with criminal terrorizing yet the IT (Amendment) Act, 2008 has made kid pornography as explicit offense under Section 67B.

6. Tricking by impersonation has not been characterized and it isn't evident whether it alludes to bamboozling as alluded under the Indian Penal Code, 1860 as led by

specialized gadget or whether it is making another class of offense. Besides the term extortion is neither characterized under the IT Act, 2000 nor under the Indian Penal Code, 1860.It additionally being perceived as a psychological condition under Indian Penal Code, 1860 (Paranjape, 2010).

7. IT offenses are very specialized in nature which just a specialist or well-perused person can manage. Cyber Regulation Appellate Tribunal (CRAT) is one man commission requiring just a person with level of law, determining no IT foundation.

IV. CYBER VIOLENCE AND VICTIMIZATION AGAINST WOMEN IN INDIA

The information technology part in India has seen a quantum jump since 1990s which is as yet proceeding. Pretty much every family unit with moderate monetary condition have internet get to. At the end of the day, internet has gotten the world our lounge rooms. Individuals from the age gathering of 13 to 70 years who approach the internet are consistently utilizing this either at home, or at work environments, or at cyber bistros, or at training foundations and so on. Along these lines, it has presented the society to another world in which we can share our thoughts and culture esteems and can appreciate all chances.

Be that as it may, it's anything but a peril free zone. Cyber space has turned into an instrument for wrongdoers to defraud or encroach women, the most defenseless focuses on internet after kids. Internet has opened conduits for different crimes against women in the cyber space. Despite the fact that, artists and other world pioneers who partake in EU traditions for building up strict guidelines to control cyber crime against youngsters, never considered victimization of women in the cyber space as a major issue like kid pornography or hacking and so forth which require a consideration. Present day advancements have made life less demanding for women over the world, however next to each other, these have additionally prompted ascend in the crimes of electronic violence against women, alleged eVAM. Cheekay Cinco of the Association for dynamic interchanges says that, "Violence against women is changing a direct result of technology. This is the reason cyber crime against women is expanding step by step. Internet and electronic network has presented women to cyber-stalking, cyber defamation, harassments, email parodying, pornography, psychological torture and sexual abuse and so forth. By and large, women stay unmindful of these crimes and their innate peril. Celina Jaitley, a Bollywood actress, had recorded a grumbling with Mumbai Police against two websites including an outside one which have supposedly transformed her photos and transfer them to advance unmentionables items. However, most women are as yet unconscious of these crimes, until they come to think about reality, it gets past the point of no return by at that point. In this way, cyber space has moved toward becoming extremely a play ground for some false individuals who endeavor to defraud women through online harassment [10].

The investigation directed by Ms Jyoti Rattan uncovers that around 60 percent of all websites are sexual in substance. 20% of them requested their guests, 13 percent went intentionally and the rest were pictorially tricked. The expanding prominence of talk rooms and the defenselessness of personal information to criminal access make women and kids the simplest focuses in the ambit of liable crimes." There is no uncertainty that cyber crimes are anything but difficult to carry out with almost no assets, yet the harm can be colossal to the security of women. The internet technology appeared just in 1986; however it has appeared forceful development. For instance, power was first outfit in 1831, however it was not until 1882 that the principal control station was constructed, and it was an additional 50 years before power controlled 80 percent of the factories and family units over the United States. Radio was in presence 38 years before 50 million individuals utilized it; TV took 13 years to achieve a similar benchmark. It was 16 years before 50 million individuals utilized a personal computer. When the internet was made accessible to the overall population, it took just four years for 50 million individuals to go on-line." Thus, internet has seen a forceful development. Alongside advantages, it represents an extraordinary threat to women security (Halder and Karuppannan, 2014).

V. MEASURES FOR TROUBLESHOOTING CYBER CRIME

Also, contingent upon legal system against cyber crimes, women must know about cyber victimization without anyone else's input, since time has come to dismiss the acknowledgment of quiet. Besides cyber laws are not widespread, as they shift nation to nation. Today, every netizen needs to peruse web secretly and securely particularly women. We should find a way to handle this issue. Here are a few stages and proposals that how women can spare themselves of being victimized in cyber space and how they can make their online discernments and encounters a more secure one, are as per the following;

Abstain from uncovering home address: This is the standard for women specifically who business experts are and entirely obvious. They can utilize place of business or a lease private post box. In this way, it can enable them to out in staying away from cyber stalkers. Besides, women ought to abstain from transferring progressively material on internet with respect to their very own information so nobody

can without much of a stretch access them (Moore, 2014).

Awareness campaign against cyber crimes: Awareness campaign must be set up from the grass root level, for example, schools, arrangements and so on about cyber crimes like stalking cheatings, financial cheatings, disparaging activities, abusing emails and social networking websites, virtual rapes, cyber pornography, email caricaturing and so forth. These campaigns can be productive in incapacitating cyber crimes.

Keep up stable social relationships: It is likewise the fact that we as a whole prefer to trust that we ought to have 2000 companions. Dunban's number7 proposes a point of confinement to the quantity of individuals, a human being can have a legitimate social association with, and that number is 150. Presumably, we needn't bother with those 2000 Facebook companions, since we are likely physical helpless to truly know more than 150 of them. Keeping up a point of confinement on the quantity of the general population will guarantee our information is appropriated to individuals who you truly know and far from companions of-companions of-companions who you actually don't have a clue about great. Women should make separate from impermissible companionships.

Change passwords time to time: In fact, we as a whole love to have simple to-recall passwords since, it is less difficult. On the off chance that one needs to bring down internet crime hazard, changing secret key is an incredible method to make personal data and social networks protected and hard to access for cyber criminal. Astounding or dubious secret key protect all accounts including phones, emails, landlines, managing an account, Visa and so forth and are troublesome for anybody to figure. Indeed, mystery questions ought not be effectively replied. Most secure passwords contain letters, numbers and images. Maintain a strategic distance from words that are in lexicon and any vital dates and should utilize diverse passwords for various sites. Be that as it may, changing secret phrase can be exceptionally useful to guard privacy [13].

Be careful with spontaneous calls and messages: Woman ought to keep away from undesirable or spontaneous telephone calls and back rubs since mobile phone might be checked. On the off chance that it happens over and over, you should endeavor to record telephone calls of harasser and answer to the police. Indeed, they ought to download applications from confided in websites. Plus, they ought to examine and share the issue in regards to cyber irritating with their confided in ones like guardians, mates or spouses and so on.

Seminars and workshops for better understanding of cyber victimization: Police, Lawyers, social specialists, and NGOs must be welcome to instruction foundations, clubs, corporate workplaces, awareness-campaigns, seminars and workshops to talk about legalities and illegalities of cyber lead among grown-ups comprehensive of the two sexual orientations. Revealing of cyber victimization at all dimensions straightforwardly to the police and NGOs working cyber crimes must be supported. Furthermore, workshops and seminars must be directed for the police personnel for better understanding of such sorts of victimization and fast reactions towards the protests. Scholarly and legal specialists, NGOs and so on must be welcomed for such workshops and seminars.

Anti-Virus should dependably be exceptional: One must stay up with the latest. As indicated by Fight Cyber stalking, Trojans, worms, and email viruses are basic routes for would-be cyber stalker to get to one's information. One must ensure that Anti-Virus is cutting-edge to reduce likelihood that one's PC can't be connected with a Trojan virus, email virus or worms. In this way, it might assist us with keeping far from the entrance of cyber harasser (Pennelli, 2014)

Understand privacy settings of social network: Social networks and other online substance and specialist organizations all have privacy arrangements and private settings. One must endeavor to understand privacy arrangements and embrace privacy settings that assistance in protecting oneself from any potential hazard or online damage. Along these lines, we should have the learning about privacy settings of social networking.

Protect data moving: In our day by day life, we regularly utilize open computers in internet bistros and so on. You ought to recollect that when you are utilizing internet on open computers, internet browsers can track your passwords and each page you have visited. In this way, you ought not neglect to delete your tracks or history on internet browsers. Your little carelessness can place you in threat. As it were, women ought to be doubtful in nature while utilizing internet since stalker may endeavor to scam you.

Check account regularly: It is certain that each net client has its very own account on network destinations. We ought to regularly browse our email, blog or site accounts and so on. Thusly, we will be in-contact with our having a place accounts on internet and we can diminish the potential outcomes of hacking, stalking and so forth by inspecting our account. It is discovered that a few women don't check their account after they make their accounts on internet. Shockingly, when it is checked, they ended up caught. In this way, net

client particularly women must not overlook this (Pachauri, 2010).

Aside from above given recommendations, women ought to dependably be in-contact with profitable information about cyber crimes and ought to be cautious before they click any connection on internet. On the off chance that Internet, versatile and cyber space are threat to their security, it has a positive side as well and can likewise end up being helpful for them. There is part of information accessible on internet to go up against cyber crimes that how they can escape themselves of being victimized. Cyber crimes require an incredible consideration of Indian government to produce finance for research establishments engaged with averting cyber crimes. Additionally, instructing women can likewise assume an impressive job in averting crimes.

VI. CONCLUSION

Indian cyber laws itself need behind contemporary occasions, When Indian laws neglect to counter the changing situations of the cyber space, the approaching emergency to be looked by different nations must be envisioned. Political impediments, privacy issues, moral argument of limiting discourse and articulation on the internet, practical execution of genuine laws in the virtual world all are extreme snags standing between an iron clad act and cyber crimes. Cyber victimization of women is a piece of the image, yet managing firsthand and on need premise with this image can complete a lot of aiding in checking the hole and lessening cyber crimes. The perceivability to defeat the cyber crimes against women all in all is testing and the main route is to understand cyber crimes. Government needs to fortify the legal system to bring down cyber crimes, since lawbreakers think of it as a lot less demanding than traditional crimes because of less shot of being gotten and less penalties. Also, what should be changed is the sense or frame of mind of the society towards women, not to think about lady as a ware. Individuals need to understand that violence against women is only a sign of sexual orientation segregation and disparity in sex control relations. Thirdly, women ought to understand that the time has come to dismiss the quietness or hesitance and approach for battling against cyber crimes and for their rights. Fourthly, it requires a standard research and consideration on cyber crimes. Women ought to likewise take an interest in such kind of activities. Again be that as it may, at last, individuals needs to change their mentalities towards women and ought to build up the feeling of shared characteristic since neatness begins from home.

REFERENCES

1. Aggarwal, Nidhi, and Neerja Kaushik Dr. (2014). "Cyber Crimes Against Women." Global Journal of Research in Management 4.1: pp. 37-49.
2. Aggarwal, Rohit (2013). "Cyber Crime Against Women And Regulations In India." Http://www.tmu.ac.in/gallery/viewpointsdcip2013/pdf/track4/t-403.pdf. Web.
3. Geetha, B. (2011). "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: .
4. Halder, Debarati and K. Jaishankar (2014). 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
5. Manila, News Agency (2014). "Cyber violence against women." 10 January 2011. The Brunei Times. Accessed on: 20 July 2014. Available at: .
6. Pachauri, S. K. (2010). Women and Human Rights. New Delhi: S.B. Nangia, A P H Publishing Corpration.
7. Ahmad, F. (2005). Cyber law in India: Law on Internet. Delhi: New Era Law publications.
8. Kashmiria, S., Dr. (2014). Mapping Cyber Crimes Against Women In India. International Research Journal Of Commerce And Law, 1(5), 22-38. Retrieved December 7, 2015, from http://ijmr.net.in/download.php?filename=766t9kt3Iqv1Osa.pdf&new=IRJCLPAPER2DECE MBER2014.pdf
9. Paranjape, V. (2010). Legal Dimensions of Cyber Crimes and Preventive Laws. Allahabad: Central Law Agency.
10. Empowering women against cyber-violence. 16 January 2011. Accessed on: 20 July 2014. Available at: .
11. HalDer, Debarati and Karuppannan Jaishan Kar (2014). "Cyber Socializing and Victimization of Women." September 2009: 5-26. accessed on 17 July 2014.
12. Moore, Alexis A. (2014). 12 Tips To Protect Yourself From Cyberstalking. 8 January

2009. Accessed on: 13 July 2014. Available at: .

13. Online Privacy & Safety Tips. 2010. Accessed on: 14 July 2014.

14. Pennelli, Paul (2014). Cyberstalking Awareness: Protect Yourself On-Campus and Beyond With These 7 Steps. 31 January 2012. Accessed on: 13 July 2014. Available at: .

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

Corresponding Author

Shyamapada Ghorai*

Research Scholar, Swami Vivekananda University, Sagar, M.P.