International Journal of Pure and Applied Mathematics
Volume 118 No. 20 2018, 595-607
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

WOMAN HARASSMENT IN DIGITAL SPACE IN INDIA

Shweta Sankhwar
Research Scholar
B.B.A University (A Central University)
Lucknow, India

Arvind Chaturvedi
Add. SP
Special Task Force
Lucknow, India

ABSTRACT

India stepped toward digitalization which brought technological power. People explore using internet and made life easy and comfortable. They explore the unknowns and communicate with virtually anyone, anytime, anywhere across the world. Digital space has opened doors to cyber criminals and mostly woman is their target. Cyber-crime has emerged as a major challenge facing law enforcement agencies in the country, women and children remain at risk. Offenders are gradually misusing Cyber platforms to harass and abuse women and children for voyeuristic pleasures in India. A call for modernization of the preventive, conventional set up and equipped police personnel with knowledge and skills is for prevention and control of cyber-crime. This paper throws light on Cybercrime and legislative intervention measures. A model is proposed and gives preventative initiatives specifically to curtail cyber-crime against woman and children.

Keyword-*Cyber-crime, Cyber Harassment, Cyber stalking, Woman Empowerment, Cyber law*

INTRODUCTION

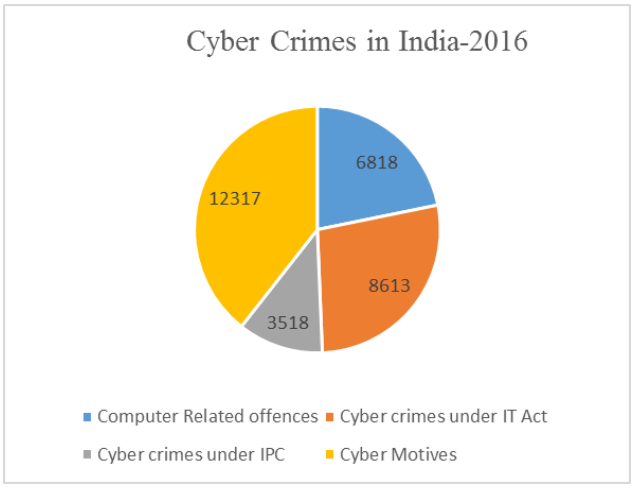
Digital India is the upshot of many innovations and technological advancements. More than half population are in not in habit of using Computer, internet and other devices which are most commonly used are social media sites (Facebook), chat rooms, skype, WhatsApp, Dating sites etc.At one side of the coin the digitalization has enhanced the system of India in all terms such as economy, education, governance etc., but at second it brought cyber-crimes also in India at large number. The definition of cybercrime continues to evolve as avenues open up that allow cybercriminals to target consumers in new ways. [1].

Cyber-criminals use computer technology to access personal information and use internet for harassment and exploitation purposes which includes stalking, blackmailing, threatening via emails, photo morphing, cyber pornography etc. Now-a-days, perpetrators are gradually misusing Cyber platforms to harass and abuse women and children for voyeuristic pleasures in India. Women and children are mostly targeted for cyber stalking, harassment, extortion, blackmail, etc. The Women often trust perpetrators or abuser and share their personal information which results numerous cybercrimes. Many times, perpetrators get a chance to harass, abuse, blackmail etc. the woman and children more because they are unaware about the procedure of filing a complaint. Massive awareness needs to be created among women and children regarding the safe use of Mobile Phones, Computers and the Internet [2].

Thus, there is an urgent need of bringing awareness and consciousness among women to be careful while using internet facilities and also a proper guidance if somehow, they face cyber-crime then they can raise their voice against it. There is also an alarming requirement for knowledge and technical enhancement for prevention of woman harassment in India. The remaining of this paper is organized as follows: In Section II, throw light on cyber-crimes and cyber law, Section III. Identifies the problem. Section IV is suggestive measures and proposed model. At last, the paper is concluded.

II. CYBER-CRIMES IN INDIA

Cybercrime went up by 6.3 per cent in 2016 (12,317) over 2015 (11,592). Uttar Pradesh (2,639 cases, 21.4 per cent) reported the most cases, followed by Maharashtra with 19.3 per cent (2,380 cases) and Karnataka with 8.9 per cent (1,101 cases). Some cybercrimes of 2016 are given in Figure.1



Cyber-crime Figure.1

National Crime Records Bureau (NCRB) of India does not maintain any separate record of cyber-crimes against children and woman [3]

CYBER CRIME AGAINST WOMAN

"Cyber-crimes against women and children are on the raise and they have been drastically victimized in the cyberspace" [4]. Some perpetrators try to defame women and children by sending obscene e-mails, stalking women and children by using chat rooms, websites etc., developing pornographic videos mostly created without their consent, spoofing e-mails, morphing of images for pornographic content etc. Indian women are not able to report cybercrimes immediately. Most of the problems can be solved if women report the crime immediately and warns the abuser about taking stronger action. Cybercrimes are proliferating at a higher rate in India. Generally, Virtual friends gain the confidence of their female friends and misuse the information of their female friends to mentally harass them. Such crimes are profoundly happening in India and also across the globe. For instance, blackmailing, threatening, bullying, or cheating via email is done by preparators. It often creates a problem when emails or social media messages are posted using fake accounts and thus, they are difficult to trace [2]. Perpetrator frame these cyber-crimes with a particular intention such as illegal gain, revenge, insult, to modesty of woman, extortion, blackmailing, sexual exploitation, defamation, incite hate

against community, prank satisfaction of gaining control, to steal information and also serious psychiatric illness.

1. **Cybercrimes**

The Major Cybercrimes which may put woman get into depression, hypertension and suffer from anxiety, heart disease, diabetic, thyroid and many more due to e-harassment. Most common types of cybercrimes are as follows:

- **Cyber stalking:** Cyber stalking is on the rise and women and children are the most likely targets. Cyber stalking a way to use the Internet to stalk someone for online harassment and online abuse. A cyber stalker does not engage in direct physical threat to a victim, but follows the victim's online activity to gather information, make threats in different forms of verbal intimidation. The anonymity of online interaction reduces the chance of identification and makes cyber stalking more common than physical stalking [3]
- **Defamation:** Cyber defamation includes both libel and defamation. It involves publishing defamatory information about the person on a website or circulating it among the victim's friends circle or organization [2].
- **Morphing:** Morphing is an activity to edit original picture to misuse it. Preparators download women pictures from social media, WhatsApp or some other resources and upload morphed photos on other websites such as social media site, porn sites or for registering themselves anonymously [7].
- **Cyber-pornography:** This is another threat to women and children because this includes publishing pornographic materials in pornography websites by using computers and internet [8].
- **E-mail spoofing:** It refers to an email that emerges from one source but has been sent from another source. It can cause monetary damage [5]
- **Phishing:** Phishing is the attempt to gain sensitive information such as username and password[5]
- **Trolling:** Trollspreadsconflict on the Internet, criminal starts quarreling or upsetting victim by posting inflammatory or off-topicmessages in an online community (such

as a newsgroup, forum, chat room, or blog) with the intention to provoke victims into an emotional, upsetting response [9-10].

2. Cyber Law

Under Information and Technology Act, 2000, stalkers and cyber criminals can be booked under several sections for breaching of privacy.

- **Section 67** deals with publishing or transmitting obscene material in electronic form. The earlier. [6]. Section in ITA was later widened as per ITAA 2008 in which child pornography and retention of records by intermediaries were all included.
- **Section 66A:**Sending offensive messages through communication service, causing annoyance etc. through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing) are all covered here. Punishment for these acts is imprisonment up to three years or fine [6]
- **Section 66B:** Dishonestly receiving stolen computer resource or communication device with punishment up tothree years or one lakh rupees as fine or both [6]
- **Section 66C:** Electronic signature or other identity theft like using others' password or electronic signature etc. [6]
- **Section66D** Cheating by personation using computer resource or a communication device shall be punished with imprisonment of either description for a term which extend to three years and shall also be liable to fine which may extend to one lakh rupee [6].
- **Section66E** Privacy violation – Publishing or transmitting private area of any person without his or her consent etc. Punishment is three years imprisonment or two lakh rupees fine or both [6].
- **Section66F** Cyber terrorism – Intent to threaten the unity, integrity, security or sovereignty of the nation and denying access to any person authorized to access the computer resource or attempting to penetrate or access a computer resource without authorization[6].
- **Section 72:** Punishment for breaching privacy and confidentiality [6].
- **Section 72A:** Punishment for disclosing information during lawful contract[6].

- **Section 441 IPC:** This section deals with criminal trespassing[6].
- **Section 354D:** This section deals with stalking. It defines stalker as a man who follows a woman and tries to contact such woman, monitors every activity undertaken by women while using digital media[6].

III. PROBLEM IDENTIFIED

Major types of cybercrimes prevailing in Indian context: cyber stalking, bullying, trolling, morphing and phishing. But many of them have no safeguard in our prevailing legal system. Thus, a clause must be included in Information Technology Act, 2000 which will contain all rules concerned with protection of electronic devices and another clause must be included which will focus on legal backing so that the evidences could be used in courts.

It was identified that there is no Standard Operating Procedures (SOPs) formulated for dealing with issues of cybercrimes. Proper training must be given to officers regarding SOP formulation and operationalization of devised protocols. Also, lack of officers in cyber cells is another major problem. Therefore, there is a requirement for posting capable officers who have adequate knowledge about various cybercrimes and technical knowledge of using computer resources, ethical hacking, etc.

It has been identified that international cooperation has not be standardized. If a case of cyber-crime involves another country then, procedure gets lengthy and several regulations must be followed. Foreign Service providers are not enough cooperative during investigations due to cross border legal issues. It is suggested that changes should be made in regulations regarding decoding of IP Address to service providers and all service providers must put their servers in India to track IP Address for fast and better investigation.There must be inter country investigation. Transnational treaty must be signed to effectively control cybercrimes.

Many women do not register complaint because the lengthy procedure and further due to fear of disclosing her identity.Mostly, when a woman gets trolled in social media sites, people blame her for being online or active on social media. Therefore, it is our social responsibility not to victimize women, instead help them to raise their voice against such criminal offences. It has been noticed that some women boldly reply to trolls but even then, they are stigmatized. Women do not have sufficient knowledge regarding privacy settings and using technology, thus training

must be imparted to women during awareness campaigns and they should be given knowledge about enhancing their privacy. Therefore, community-based awareness campaigns must be organized by professional people who have advanced knowledge about technology and have experience in handling cybercrimes. Even if victims complain, police investigate, there are not enough number of e-courts where the cases can be resolved.

Major Problems are briefed below:

1) Woman and child cyber harassment and related cyber-crimes remain overwhelmingly under-reported due to associated stigma and propensity of parents/guardians to not involve police in such matters.
2) Perpetrators know their victims well or they are related to them. Women are mostly unaware about privacy policies and safety tips for using social media sites. Women are less proficient in using technology.
3) Process of reporting such cybercrime against woman needs to be simplified and identity of woman and children involved protected to ensure such crimes do not go unreported. It is necessary simplify and strengthen cybercrime investigation involving woman and children.
4) Cyber laws have not been formulated properly and the procedure for registering a complaint is not known by woman. [2]
5) It is a staple of anguish that there has been unembellished under-reporting of cyber-crimes i.e. online harassment of women and child sex abuse in the India. National Crime Records Bureau (NCRB) of India does not maintain any separate record of cyber-crimes against children and woman.
6) The data is composed by NCRB currently is simple and provides an insight into the state of law enforcement in the country as it is unbelievable that in most of the states there is no incidence of online woman harassment or child sex abuse. The data indicates extremely deprived law enforcement regarding these crimes as it only gathers information of reported cases and it fails to throw light on true occurrence rate of such crimes. It does not depict actual number of incidents.
7) No Digital Police Portal is existing currently. Women and children who are facing increasing instances of abuse on online platforms.

8) Woman harassment and exploitation in cyber space is increasing with updated technology and anonymity. It takes huge time for investigation and many times cases are unsolved due to lack of Cyber Forensics laboratories.
9) Cyber criminals use digital media to harass women and even legal system is not defining the cyber laws in a holistic way. There is a need to use law as an instrument of change and thus, law makers should focus upon substantive equality. As like trolling should be defined well and scope of the cyber laws must get widened. Major legal lacuna i.e. having no clause for many common cybercrimes in legal system.
10) Foreign Service providers are not enough cooperative during investigations due to cross border issues.

VI. SUGGESTIVE MEASURES AND PROPOSED SOLUTION FRAMEWORK

It is high time to call for modernization of the preventive set up for cybercrimes and to equipped police personnel with suitable knowledge and skills. Some of the solution are given below:

1) NCRB should assemble all the cases of woman and child harassment and other cyber-crimes against woman and children under a separate category so that performance of law enforcement agencies in this regard could be discerned and observed properly.
2) Law enforcement agencies and police force need to be sensitized of the challenging facets of cyber-crimes against woman and children and their dimensions to record and initiate action against such crimes needs to be strengthened urgently.
3) There should be a Digital Police Portal or E-Portal where woman can report their problems online. This could reduce the number of cases under-reported due to associated stigma and propensity of parents/guardians to not involve police in such matters the portal also maintains the database of criminals which could really help law enforcement.
4) It is needed to collaborate both police force and cyber forensic laboratories together for better investigation.

5) Girls should be made aware about all types of cybercrimes and how to handle them. Spreading awareness regarding safe internet uses and complying procedure should have done among the woman.
6) School curriculum must cover all aspects of cybercrimes. Therefore, education system must initiate contemporary issues pertaining to cybercrimes.
7) It is suggested that all international service providers must put their servers in India to track IP Address for fast and better investigation.
8) We can notice that theimplementation of cyber laws is inadequate and people are unaware of the laws and still, there is less emphasis on cyber security.

PROPOSED SOLUTION MODEL

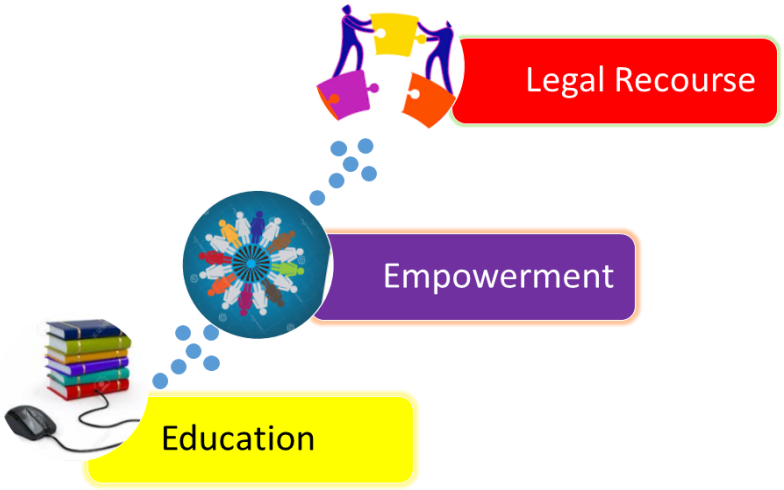


Figure.2 Cyber Crime Model Prevention Model for Woman

In this research paper, Cyber Crime Model Prevention Model proposed for woman. This modelstands on three pillars i.e., Education. Empowerment and legal recourse as shown in Figure.1.

1. **Education**pillar strengthens the education systemin terms of digital India. A Girls should get capacity building classes or workshops from school level. These capacity building workshops explore knowledge of tackling cybercrimes by using latest technologies and

girls should be made aware about handling technologies and knowledge regarding privacy settings. It encourages the woman to do more participation in digital media and be equipped to handle matters regarding cybercrimes. School curriculum must cover all aspects of cybercrimes and cyber security. Therefore, education system must initiate contemporary issues pertaining to cybercrimes. School curriculum should includefollowing points as given below:

- Digital world
- Do's and Don't
- Digital Etiquettes
- E-Safety and security
- Cyber Law in Brief
- Legal recourse
- Prosecution

2. **Empowerment**pillar encourages the woman to raise their voice against cybercrime. This could create an environment where women have equality on each level i.e. socially, economically, politically, mentally and so on. Some are defined below and also as shown in Figure.3.

- Legal Empowerment could be done by legislating required rules and guidelines with their implementation.
- Social Empowerment: This could encourage the victims to raise voice against their sufferings. NGOs can play vital role to provide a rightful platform where victims can get legal and procedural guidance.
- Mental Empowerment: The most important step in the success of woman who combat against their harassment in digital space. The most effective change can be brought by glorifying the victim's zeal to fight out harassment.

3. **Legal Recourse-** This pillar will work like a bridge and put a connection between woman and law enforcement. So, there should be a Digital police portal i.e. e-portal or e-courts where woman can report their problems online and step towards remedy at easy and

securely with less time and effort consumption. This could reduce the number of cases under-reported due to lengthy complying procedure and associated stigma & propensity of parents/guardians to not involve police. These e-portal also maintains the database of cases and criminals which could really help law enforcement. Advanced Technology and anonymity creates hurdles in investigation of cybercrime cases. It takes huge time for investigation and many times cases are unsolved. Therefore, law enforcement should be incorporated with Cyber Forensics laboratories for fast investigation.

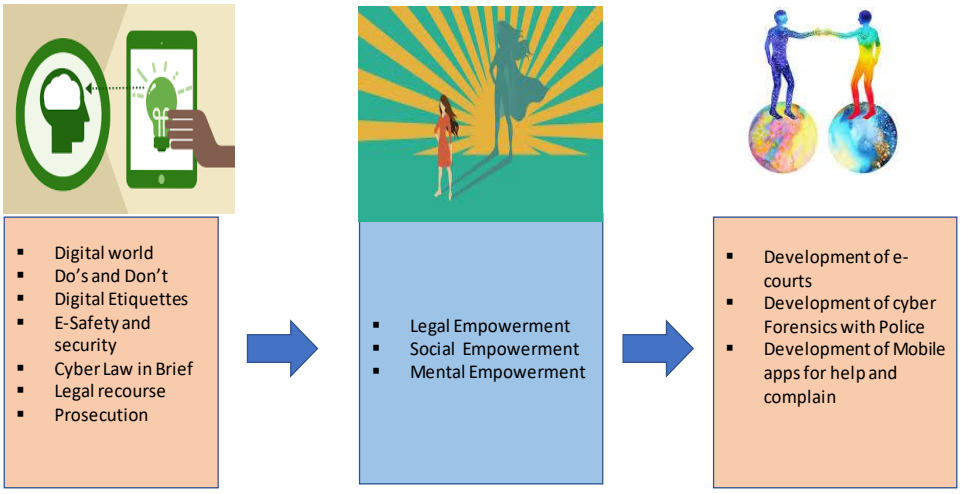


Figure.3 Cyber Crime Model Prevention Model for Woman

When women are able to eloquently participate in digital world their needs and rights will be heard and enforced. This will result women'ssafety &well-being and further, this will have a flow on effect to the society and next generation.

V.

CONCLUSION

There is a need for constant evaluation of cyber laws and procedure because women face difficulties while seeking redressal due to lack of awareness. In this paper, several problems is being identified and respective to these problems a preventionmodel is proposed. This model

could strengthen the woman and society.The police and the government, both have their parts to play, but these cyber-crimes will downcast only when legal steps are accompanied with woman awareness to bring a shift in the mentality of the society at large.

VI
REFERENCES

[1] Norton. (2015). Norton Cybersecurity Insights Report. Accessed on March 20, 2018 from online Available [https://us.norton.com/norton-cybersecurity-insights-report-india]

[2] Sharma, S.K. (2013). TumhariSakhi. New Delhi: Bukaholic Publications.

[3] National Crime Records Bureau (NCRB) of India-2016 online available [https//:www.ncrb.gov.in]

[4] Saha, Tanaya, and Akancha Srivastava. "Indian women at risk in the cyber space: a conceptual model of reasons of victimization." International Journal of Cyber Criminology 8.1 (2014): 57.

[5] Sankhwar, Shweta, et al. "A Novel Anti-phishing Effectiveness Evaluator Model." International Conference on Information and Communication Technology for Intelligent Systems. Springer, Cham, 2017.Melander, Lisa A. "College students' perceptions of intimate partner cyber harassment." Cyberpsychology, behavior, and social networking 13.3 (2010): 263-268.

[6] Cyber law of India. Online available [www.cyberlawsindia.net/]

[7] Thapa, Anju, and Raj Kumar. "Cyber stalking: crime and challenge at the cyber space." An International Journal of Engineering Sciences 4 (2011): 340-354.

[8] Marcum, Catherine D., et al. "Battle of the sexes: An examination of male and female cyber bullying." International Journal of Cyber Criminology 6.1 (2012): 904.

[9] Halder, Debarati, and JaishankarKaruppannan. "Cyber socializing and victimization of women." (2009).

[10] Henry, Nicola, and Anastasia Powell. "Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women." Australian & New Zealand Journal of Criminology 48.1 (2015): 104-118.