CYBER CRIMES AGAINST WOMAN IN INDIA AND THE LAW

Dr. Rupesh Kumar

INTRODUCTION

India is the upshot of numeroustechnological advancements and innovations. More than 50% population of India are in habit of using Computer, mobile and other devices which are commonly used for social media sites such as Facebook, WhatsApp, skype, Gmail etc.At one side of the coin the technological advancement has enhanced the system of India in all terms such as education, economy, governance etc., but at second side it brought various cyber-crimes also in our Nation at very large number. The definition of "cybercrime"is any typeof crime committed through internet by using various types of websites. Moreover it opens wide avenues that allow cybercriminals to target consumers in new and various ways.Cyber-criminals use different methods to access personal information of individual and use internet for exploitation and harassment purposes which includes blackmailing, stalking, photo morphing, threatening via emails, cyber pornography etc. [1]

The misusing Cyber platforms to abuse and harass children and women for voyeuristic pleasures is common in India. Children and women are mostly targeted for harassment, cyber stalking, blackmail, extortion,etc. The children and women often trust abuser and perpetrators and often share their personal and private information which results numerous cybercrimes. Many times, perpetrators get a oppurtunity to abuse, harass and blackmail. The children and woman are more targeted because of their unawareness about the procedure of filing a complaint. And various legislations. Massive awareness must be created among children and women regarding the safe use of Internet, computer and mobiles. Therefore, there is an urgent need of bringing consciousness and awareness among children and women to be careful while using and handling internet facilities and also a proper guidance must be provided how to face cybercrimes. Moreover, how they can raise their

[1] *Available at*: http://cybersecurityinsightsreport.org/_ (Visited on March 4, 2019).

concerned voice against it. There is also an alarming requirement for technical enhancement and knowledge for abolition of woman harassment in India. The paper is organized to throw light on cyber-crimes and cyber laws, Identifies the problem and suggestive measures and proposed model are specified. At last, the paper is concluded.

CYBER-CRIMES IN INDIA

Cybercrimes went up by 8.8 per cent in 2018 (22,117) over 2017 (17,392). In Punjab (3,659 cases, 31.4 per cent) cases in 2018 were reported, followed by Haryana with 29.3 per cent (3,180 cases) and Rajasthan with 18.9 per cent (2,131 cases).

1. CYBER CRIME AGAINST WOMAN

“Cyber-crimes” against children and women are on the raise and they have been continiously and drastically victimized in the cyberspace.” Some perpetrators try to defame children and women by using chat rooms, websites etc. And sending obscene e-mails, stalking women, spoofing e - mails, developing pornographic videos mostly created without their consent, morphing of images for pornographic content etc. Most of the Indian women in India are not able to report cybercrimes immediately. The problem can be solved easily if women report the crime immediately and complain it to the police and warns the abuser about taking strict and stronger action. Cybercrimes are proliferating at a very higher rate in India. Generally, male friends gain the confidence of their female friends andmisuse the information of their female friends to mentally torture them. Such crimes are profoundly happening in India and also across the world. For example, threatening, blackmailing, bullying, or cheating via email is done by preparators. It often creates a huge problem when social media messages and emails are posted using fake accounts and thus, they are difficult to trace the accused. [2]Perpetrators commit these type of cyber-crimes with a particular intention and motive such as revenge, illegal gain, insult, to modesty of woman,

[2] Sharma, S.K., *Cyber Crimes in India* 12(Bukaholic Publications, New Delhi, 3rd edn., 2018).

blackmailing, extortion, defamation, sexual exploitation,incite hate against community, prank satisfaction of gaining control, to steal information and also serious psychiatric illness.

2. NUMEROUS CYBER CRIMES

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

1. **Cyber stalking**: Cyber stalking is on the high rise in India.Children and women are the mostly targets. 'Cyber stalking' a way to use the Internet to stalk someone for online abuse and online harassment. A cyber stalker does not involve in direct physical threat, but follows the victim's online activity to gather information and make threats in the form of verbal intimidation. The anonymity of online interaction reduces the chance of identification of offender and makes cyber stalking more occurence and common crime than physical stalking.

2. Defamation: Cyber defamation includes both defamation and libel. It involves publishing defamatory about the person on a internet website and circulating it among the victim's social circle or town.

3. Morphing: Morphing is a type of activity to edit the original picture and use in different forms to degrade the image of person. Preparator download woman pictures from social media, facebook or some other resources and upload photos on other websites for instance social media sites, porn sites or for registering themselves anonymously.

4. Cyber-pornography: This is another serious threat to children and women. The publishing pornographic and objectionable materials in pornography websites by using internet.

5. E-mail spoofing: It refers to any type of e-mail that emerges from one source but has been sent from some another source. It can cause huge monetary loss.

6.Phishing: It is an attempt to gain very sensitive information about a person such as username and password.

7. Trolling:Trollspreadsconflict on the Internet, criminal starts fighting or upsetting victim by posting inflammatory kind of messages in an online community with the motive to provoke victims into an upsetting and emotionalresponse.[3]

3. CYBER LAWS

The Information and Technology Act, 2000 :

The complaint can be lodged against cyber criminals and Stalkers and they be can booked under numerousSections of the Act for breaching of privacy. The various Sections are as follows :

Section 67: deals with,"publishing or transmitting different types of obscene material in electronic form." The earlierSection in "Information Technology Act, 2008 was later widened in which child pornography were all included.

Section 66A: deals with, "sending vulgar and offensive messages through communication service, causing annoyance to person. through an electronic communication or sending an email to deceive or mislead the recipient about the origin of such messages are all covered here. Punishment for these acts is imprisonment up to two years or fine.

Section 66B: Dishonestly receiving stolen computer resource or communication device from person is an offence which leads to punishment up to 4 years or 25, 000 rupees as fine or both.

Section 66C: deals with electronic signature or other theft such as using others electronic signature or password etc.

[3] *Available at:*https//:www.ncrb.gov.in (Visited on June 12, 2019).

Section66D :deals with cheating by personation using internet resource or a any kind of communication device shall be punished with imprisonment for a term which extend to 4 years and shall also be liable to fine which may extend to 50, 000.

Section66E Privacy violation – deals with transmitting or publishing private area of any person without his approval etc. The punishment is of four years imprisonment or1 lakh rupees fine or both.

Section66F Cyber terrorism – Intent to threaten the integrity, unity, security or sovereignty of the Country and denying access to any individual authorized to access the computer or access a computer resource without authorization or attempting to penetrate.

Section 72: deals with breaching privacy and confidentiality.

Section 72A: deals with for disclosing integral information during lawful contract.

Section 354D: This section deals with stalking itself. It defines stalker as a psycho man who follows a woman and tries to contact with such woman, monitors various activities done by woman while using internet resources.[4]

4PROBLEM IDENTIFIED

The major kinds of cybercrimes prevailing in India are bullying, cyber stalking, trolling, phishing and morphing. But mostly many of them have no proper safeguard in our prevailing legal system. Therefore, a clause must be included and mentioned in Information Technology Act, 2000 which must contain all pertaining rules concerned for protection of electronic devices crimes and another clause must be mentioned and included which will focus on legal backing Thus, the evidences could be used in courts.

[4] Saha, Tanaya, *Indian Women at Risk in the Cyber Space*54 (Mohanta Publications,New Delhi, 4th edn., 2017).

It is identified in our Country that there is no Standard Operating Procedures (SOPs) formulated for dealing with issues and crimes of cyber. Proper training must be given to officers concerned and various necessary information regarding SOP formulation and operationalization of devised protocols must be provided to them. Also, lack of vacancies of officers in cyber cells is another integral major problem. So, there is a requirement for posting capable and intelligent officers who have adequate knowledge and skills about various cybercrimes occurring in this digital era and major technical knowledge of using computer resources, ethical hacking, etc.

It has been also identified that cooperation of international Nations has not be properly standardized. If a case of cybercrime involves another Foreign Nation then, procedure gets more lengthy as compared to us and several rules and regulations must be followed. Foreign Service providers agencies are not enough cooperative during enquiry due to cross border legal issues. It is suggested that changes must be made in regulations of decoding of IP Address to the service providers and all service providers should put their servers to track IP Address for fast and better enquiry.There should be inter Nation investigation. Transnational treaty should be signed to effectively eradicate cybercrimes.Many women do not lodge complaint because of the long procedure and further becauseof fear of disclosing her identity to the society. Mostly, when a woman gets trolled in social networking sites, people accuse her for being active on social media. Therefore, it is our social duty not tovictimize women, but to help them to raise their voice against such offences which are danger for whole society. It has been noticed that some women only boldly reply to trolls but even then, they are stigmatized. Most of the women do not have sufficient knowledge regarding various privacy settings and using technology, thus the training should be imparted to women during campaigns and they should be given knowledge of enhancing their privacy. So, community-based awareness campaigns should be organized by the people who have advanced and deep knowledge about technology and have proper experience in handling cybercrimes. Even if victims complain, police investigate, there are not enough e-courts where the matter can be resolved.[5]

[5] Halder, Debarati, *Cyber Socializing and Victimization of Women*134 (Ansal Publications, New delhi, 2014).

5. Major Problems are briefed below:

1) Children and women cyber crimes and related cyber-harassment remain overwhelmingly unreported due to associated stigma and of parents/guardians thinking to not involve police in such matters.

2) Perpetrators know their victims well or they are somehow related to them. Women are mostly unaware of privacy policies and various safety tips for using numerous social media sites. Women are less proficient in using technology than men.

3) Process and procedure of reporting such cybercrimes against woman needs to be simplified and matter should be solved in less time and identity of woman and children involved must be protected to ensure that such type of crimes do not go unreported. It is necessary to make simplify and strengthen cybercrime investigation involving children and woman.

4) Cyber enactments have not been enacted properly and the procedure for lodging a complaint is unaware by woman.

5) It is a staple of anguish that there has been not proper record 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 maintained proper record of cyber crimes against children and woman.

6) The data which is composed by NCRB Agency currently is simple and provides an insight into the state of law enforcement in the Nation and it is unbelievable that in whole of the Country there are very minor incidents of online woman harassment or child sex abuse. [6]The data clearly indicates extremely deprived law enforcement regarding these cyber crimes as it only gathers information of reported cases and it fails to throw light on true occurrence rate of such crimes.

[6] Sakshi Sinha, "Woman Exploitation and International Concern" 8 *The Indian Journal of Public Administration*101-108 (2012).

7) No Digital Police Portal is on exist currently forchildren and women who are facing increasing instances of abuse on online platforms.

8) Woman exploitation and harassment in cyber space is increasing with updated technology. It takes large time for investigation and most of the times cases are unsolved due to lack of Cyber Forensics laboratories.

9) Legal system is not defining the cyber legislations in a holistic way. There is a need to enforce law to eradicatecyber crimes. Therefore, law makers must focus upon substantive equality. As like trolling should be mentioned well and scope of the cyber legislations must get widened.

10) Foreign Service providers of different Nations are not enough cooperative during investigations due to cross border disputes

6. SUGGESTIVE MEASURES AND PROPOSED SOLUTION FRAMEWORK

It is now time to call for taking preventive steps for cybercrimes and to equipped police personnel with suitable knowledge and required skills. Some of the proper solutions are given below:

1) NCRB Agencymust assemble all the matter of cases of children and woman harassment and other major cybercrimes against children and woman under a separate category so that performance of law enforcement agencies in this regard could be observed properly.

2) Law enforcement agencies need to be sensitized of the numerous challenging facets of cyber-crimes against children and women and their dimensions to record and initiate action against such crimes needs to be strengthened properly.

3) There should be a Digital Police Portal or E-Portal where woman can report and lodge their problems and complaints online. This could reduce the number of matters under-reported due to associated stigma and propensity of society/parents/guardians

to not involve police in such kind of matters the portal also maintains the database of criminals which could really help law enforcement.[7]

4) Nowadays, it is needed to collaborate both cyber forensic labortaries and police force together for better and proper investigation.

5) Womenmust be made aware about all kinds of cybercrimes and how to handle them. Spreading awareness and organizing campaigns regarding safe internet uses must be in priority list.

6) Our school curriculum must cover all and different aspects of cybercrimes. so, education system must initiate contemporary issues pertaining to cybercrimes.

7) It is overwhelmly suggested that all international service providers and users should put their servers in India to track IP Address for better and fast investigation.

8) We can notice that theimplementation of cyber laws is inadequate and society is unaware of the legislations and still, there is very less emphasis on cyber security.

7. PROPOSED SOLUTION MODEL

1. **Education** :

Education pillar strengthens the education systemin terms of digital era. Girls must get classes or workshops on cyber crimes from school level. These capacity building workshops explore knowledge of tackling cybercrimes by using latest technologies and awareness should be created among girls about handling technologies and knowledge of privacy settings and it encourages the woman to do more participation in digital media and be well equipped to handle matters of cybercrimes. [8]

2. **Empowermentpillar**

[7] Rajeshwar Singhal, *Safety of Woman*176 (Appurva Publishers, New Delhi, 3rd edn., 2003).

[8] M. Koteswara Rao, *Human Rights* 167 (Allahabad Law Agency, Allahabad, 3rd edn., 2006).

Itmotivates the woman to raise their voice and take action against cybercrimes.This could create an atmosphere where woman have equality on each level i.e. socially, , politically, politically, mentally and so on. Legal Empowerment could be done by legislating required guidelines and regulations with their implementation.

3 Social Empowerment:

This could encourage the victims to take against their sufferings. NGOs can play integral role to provide a rightful platform where victims can get legal guidance. This is the most vital step in the success of woman who combat against their harassment in digital India.

4 Legal Recourse-

This pillar will work like a bridge and put a connection between woman and law enforcement. Therefore , there must be a Digital police portal i.e. e-portal or e-courts where woman can report their problems easily and file their complaints online and take proper steps towards remedy securely with less time and effort consumption. This could reduce the number of cases under-reported due to lengthy complying procedure and fear of parents/guardians to not involve police.[9]

CONCLUSION

There is a need for constant evaluation of cyber legislations and procedure because women face major difficulties while seeking redressal due to unawareness. In this paper, numerous problems is being identified which are faced by women in digital era due to cyber crimes and respective to these various problems a preventionmodel is proposed. [10]This model could strengthen the woman and society.The Government and the police, both have their roles to play, but these cyber-crimes will downcast only when the steps are takenfor woman awareness and to change the mentality of the society at large.

[9] Alex Georgie, *The Woman and the State in India* 33 (Oxford University Press, Oxford, 4th edn., 1998

[10] Preetha Joshi, *United Nations Impacton Countries* 99 (B.R. Publications, New Delhi, 4th edn., 2007).