ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

CYBER VULNERABILITY OF WOMEN AND CHILDREN

Dr. K. I. Pavan Kumar,

Associate Professor KLEF College of Law, Vaddeswaram, Guntur.

(indupavan73@kluniversity.in)

INTRODUCTION

Society is engulfed by the technology. Usage of internet is considered as human right by United Nations Human Rights Council in June 2016[1]. To carry out every day activities, most of the businesses and individuals are dependent on computer networks. Cybercrime is a menace growing proportionately with the usage of technology in the modern life. As the cyber society is advancing cyber vulnerabilities have also increased substantially.

It is not an exaggeration to say that Information Technology encapsulated every aspect of human life. It engulfed into it, every individual irrespective of his/her religion, race, caste, creed, sex, place of birth, social status and physical location. Computer Networked environment has changed the way the people live, their thinking, their intentions and the very purposes of their life. It did bring-in lot of opportunities to individuals at micro level and facilitated the Governments in terms of saving time and cost of public administration, at macro level. It did provide many business and employment opportunities globally.

However, the negative side of the technological is that, it also has opened the doors to the antisocial and criminal elements. The varieties of crime, committed online, had never been previously possible. The online miscreants are breaking law by committing traditional crimes in non-traditional manner, with technical sophistication and highhandedness causing lot of hardship for law enforcement.

Cybercrime operates on the premise that is entirely a new phenomenon. Cyber vulnerabilities encompass many aspects like, e-commerce, freedom of speech, Data Protection, Privacy; IPR issues etc., out of them, genderbased crimes drew lot of attention by the researchers and policy makers. The uniqueness of cyberspace makes it difficult to conceptualize and combat the crimes committed online. Before getting into the offences against women in cyberspace, it is necessary to appreciate the reasons how cybercrimes are different from conventional crimes:

[1] 'The Promotion, Protection and Enjoyment of Human Rights in the Internet', A/HRC/32/L.20, 27 June 2016

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

Physical contact is done away with: In cyber space, the physical contact between the victim and the criminal is not need to accomplish a crime. If not for all, for most of the offences committed offline, physical contact is a pre-requisite to accomplish a crime. Online crimes can be committed sitting in any corner of the globe.

Long term victimization: The Internet provides an opportunity to commit the offence, repeatedly, continuously, sometimes even without knowledge of the victim ex: child abuse.

Transcend Jurisdictional boundaries: These crimes transcend the boundaries, victimizing different people from different locations.

The Scale: the ubiquitous impact of cybercrimes, in terms of volume of loss and its far reaching nature is unique feature of cybercrimes. It is not possible to conduct a crime at such a scale in the physical world.

The Speed: the speed at which the cybercrime committed is at a machine speed.

Perception: When pubic financial institutions like banks are subjected to cyber-attacks, public get to know about it very rarely, because of negative perception and media impact. The conservative approach, in sharing information to the public has increased the cybercrime vulnerability. Similarly, in case of women and children also there is lot of social resistance. Many victims do not disclose their victimization sometimes; they don't even realize that they are victimized by a cybercrime.

Lack of Common consensus on cybercrimes: Common consensus has not been reached yet as to the nature of cybercrimes.

However, the Author restricts the scope of this Article to the offences committed against women online. Women especially young girls who are inexperienced in the cyber world, and newly introduced to the internet fail to understand the immoralities of the internet, and hence are most susceptible to cybercrimes. Some of the cybercrimes against Women are as under:

CYBER STALKING:

The most notorious and frequently committed internet crime in the information age is Cyber Stalking. In general sense, whether sexual in nature or not, every action which tortures, harasses, terrorizes and intimidates the victim is Stalking. At the same time any apparent intrusion into the privacy of an individual against the consent of such individual is also called stalking. It occurs mostly with women and children. Therefore it can be stated that following or spying a woman on the Internet using any form of electronic communication, to cause a fear of violence or distress in the mind of such women or constant interference with the

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

mental peace of such person is forbidden under law and is termed as stalking. Stalking can take place either physically or by the through electronic means of communication, which is called as cyber stalking. In Cyber stalking, a personal is victimized by constant and repetitive harassment, disturbing a person using computer networks.

Stalking is defined under Section 354 D (2)[2] of IPC. Cyber stalking is not specifically defined in IPC. According to the above mentioned section in the Criminal major Law of the land, for the purpose of cyber stalking it can be understood that any man who follows women by email or in social media, chat groups, Facebook, twitter or by any other mode of communication through internet, is said to have committed stalking. For the first conviction, punishable up to 3 years imprisonment +fine and for second and subsequent convictions imprisonment up to 5 years with fine is provided.

In India the first 'cyberstalking' case, reported in the year 2001. One Manish Kathuria was stalking by using the name of Ms. Ritu Kohli. Ms. Manisha also shared Ritu Kohli's landline number online. As a result, she was getting many phone calls with indecent proposals. She lodged complaint before Delhi Police for legal action. Police has booked case under Section 509 of IPC for outraging the modesty of women. But the section does not have mention about online related issues. However, section 66A of IT Act, 2008 has forbidden the act of sending offensive messages as punishable on the grounds of 'intrusion into the privacy of others'. The sexual harassment online is rampant. Because internet as medium has lot of sexually explicit content available and is easily accessible to all ages. Sending images of sex to others or passing sexually colored remarks online or demanding sexual favour or doing unwelcome verbal or non-verbal conduct of sexual nature is very easy, hence commission of sexual harassment is also become easy.

Behavior and motive of a stalker:

1. Intentionally harasses a woman
2. Causing fear and mental agony
3. By following her on the internet
4. By sending/posting messages on the chat rooms that are visited by her frequently.
5. Posting messages indicating/relating to her, in bulletin boards.
6. Sending the number of messages to her email

[2] After the December 2012 gang rape incident, with the recommendations of Justice Varma Committee, Anti-Stalking Law introduced. Section 354D Added to IPC by the Criminal Law (Amendment) Act, 2013.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

7. Stalking is continuous, repetitive in character
8. The motivation is to:

a. Harass her sexually, or
b. Gain love, or
c. Take revenge or
d. Hurt ego or
e. Gain power

Here in the author likes to throw light on Cyber sexual harassment, which indeed is the ulterior end and ultimate result of cyber stalking. Any intended and repetitive behavior , put forth by a person/persons through the medium called internet is called harassment. Any acts or behavior which includes persistent and unwanted sexual advancements through internet is called as Cyber sexual harassment. In India , Sec 354 –A IPC, inserted through the criminal Law Amendment Act, 2013 defines the acts and prescribes punishment for the offence of sexual harassment through the Criminal Law Amendment Act, 2013 , whereas Sec 67 A and Sec 67 B of IT Act provides definitions and various forms of cyber sexual harassment.

Stages of Stalking

1. Stalkers at first try getting access to email IDs, Facebook accounts, mobile numbers, twitter accounts, Gmail and other social media accounts of a targeted victim. However, it is not always necessary that stalker first identify a person for his harassment, it could be other way around like stalker harasses those whose data is easily accessible to him. Because for harassment, there needs to be no specific motive. Getting data of someone itself motivates and encourages the stalker to intrude into the victim's domain.
2. Then Cyber stalker monitors the person's movements online.
3. Then Cyber stalker's target and harass their victims via various online communication methods.

Difficulties in handling cyber stalking:

1. The anonymity in cyberspace makes it complicated to identify the culprit.
2. The victims generally are not willing to lodge complaints against stalkers for various reasons including lack of awareness and prevailing social taboos.
3. If the victim of this offence is a child, he/she cannot even share about what is going wrong with them.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

4. A criminal case starts with a police station where no one knows the provisions of cyber law this is also posing an additional difficulty in mitigating cyber stalking[3].
5. In addition to the above barriers the technical legal issues like Jurisdiction, contributing to the lawlessness in the cyber world.

Dissemination of obscene Material & Pornography

The most unethical practice in vogue on internet is dissemination of obscene material. The rate and the nature of offences committed online are raising the basic question on our civility. In India Sec 67 of IT Act, 2000, provides more rigorous punishment than Sec 292 of IPC . Except for the exceptions provided in the Section, Sec 292 of IPC holds the acts such as writing, drawing, painting, representing, selling, hiring distributing, publicly circulating, exhibiting, possessing , importing, any object, figure, paper, book or pamphlet holding obscene material punishable for a term which may extend to imprisonment for a term which may extend to 2 years and fine up to two thousand Rupees for the first time and for subsequent conviction the punishment may extend to imprisonment for a term which may extend to 5 years and fine up to five thousand Rupees. In short publishing or transmitting obscene material in documentary form electronic form is held an offence and is punishable.

Among all the internet-related crimes obscenity and pornography are two such crimes that directly affect the cultural values of the society. Cyber obscenity involves websites, online magazines holding pornographic contents and gives access to internet to download and transmit pornographic pictures, photos and writing. The Bekkoame case[4] is the first case where the accused was convicted for distributing obscene images to the public through internet. Since then many administrative and legislative steps were taken by various countries to mitigate the office. But it could be analyzed by observing a plethora of cases that the severity of punishment is not sufficient in deterring the offenders from committing the offence, which is a detriment to any civilized society, especially in this internet era . In 2008 an attempt was made via The Indecent Representation of Women (Prohibition) Act to combat the acts of obscenity against women. But the Act considers obscene acts covered only by print media and the matters pertaining to electronic media or the activities that take place on mobile phones are not covered under thy said Act. BY this it could be understood

[3] https://internetdemocracy.in/media/keeping-women-safe-gender-online-harassment-and-indian-law-2
[4] (18February1998, decision, case number; Heisei 10 MU Criminal 141, Tokyo District Cour Hanrei-Jiho no.1637p.152

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

that abuse or harassment which is sexual in nature carried out through is not considered as grave as other forms of abuses. If practicalities are observed the existing legal and judicial trends have proved to be obsolete and inadequate in combating cyber obscenity. The Indecent Representation of Women (Prohibition) Amendment Bill, suggests to widen the scope of the Act, by which acts against women and transmission of obscene stuff through internet, electronic media and web are also covered.

In the United States of America, "the Communications Decency Act of 1996" and subsequent amendments to it, attempts to curb the child pornography. However, the expected results could not be achieved by the Act. As an administrative measure, the Internet Corporation for Assigned Names and Numbers (ICANN) is also discouraging registration of the sites with ".XXX" Domain names. If anybody looking to register '.XXX' domain must get permission from International Foundation for Online Responsibility (IFFOR). In India, the Department of Electronics and Information Technology has asked the Department of Telecommunications to notify internet service providers to block access to 857 URLs[5]. While so, the other school of thought believes that interfering with the personal choices of individuals is against the spirit of the Constitution of India, Article 21, Right to Life and Personal Liberty.

Test of obscenity :

In Britain: Globally various tests have been adopted by the courts to determine whether a content is obscene or not. Like Hicklin test[6], in this test, first the alleged content will be separated from the other work to test whether the said content has any impact on the susceptible readers, like children or weak minded adults. If that content has ability to corrupt the minds of those readers the content is said to be obscene. In case of testing the literary work, the test of *literary morality* was adopted by the British courts, wherein the test is like what a father could read aloud, in his house could be considered valid.

In US: Similarly in the United States he Courts have adopted a test called *Roth Test*[7] it was held that the content that has a tendency of enticing a person for sexual desires are only obscene. This test is applied from the point of a person having contemporary community

[5] By order no. 813-7/25/2011-DS (Vol.-V)
[6] Regina v. Hicklin (1868) British Case law.
[7] Roth v. United States (1957)

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

standards of behavior. The content as a whole was taken into account, unlike Hicklin test, to see whether the content, as a whole, redeems the social values or not.

In India: In the case of Ranjit D Udeshi vs. The State of Maharastra[8] for the first time the India court defined obscenity. The alleged content:

1. Should deprave and corrupt the minds that are prone to such immoral influences.
2. The content should suggest the thought of most impure
3. That which has tendency if creating impure and lustful thoughts

However, in the case of Aveek Sarkar v. State of West Bengal, Supreme Court has adopted the 'community standard test' (Roth test). The community standard test is not defined so it can be applied to any community including internet community as well. The Supreme Court of India drew a line of difference between *sex* and *obscenity*[9]. Depending on the context of the content, in reference, sex always need not be an obscene. The content availability and accessibility varies from time to time. Hence the obscenity of the content must be viewed from point of the society we are referring to. Therefore online obscenity cannot be tested on the footing of offline content. The rules of the game would vary substantially.

The content vulgarity or sexual explicitness may not be unethical in cyberspace, if it becomes the standard of the cyber society or order of netizens. Perhaps, the only thing that could be done is restricting, technologically, the access to the content and providing enough disclaimers on the content vulnerability.

I. Morphing:

Morphing is editing the original picture to make it look completely or largely different. Often it is misused in the cyber world with malicious motives. The criminal minded elements would download pictures of girls from various online sources like Facebook, Twitter etc., and then morph them such that they represent those girls indulging in such activities. Sometimes, those morphed photographs are used to blackmail those girls for money or for other ulterior motives. Even spreading, putting those morphed photographs would damage the social image of those girls.

In the case of Bal Bharati Air Force School's case, a 16-year-old schoolboy created a website by name www.amazing-gents.8m.net wherein, the details about the physical attributes and

[8] LAWS(SC)-1964-8-27

[9] K. A. Abbas vs The Union of India & Anr.(1971) AIR 481.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

sexual preferences of his schoolgirls and teachers are given. He was then arrested and prosecuted and convicted[10].

II. E-mail Spoofing (deceiving):

It occurs when a person sends an E-mail to deceive others by luring him with easy gains. A website, pretending to be a genuine bank portal, deceives the innocent customer of the bank by taking user ID and Password of the customer, to believe it to be the original one. The innocent customer types his user ID and Password only to receive a false error message that the website not available. In the meantime, the dishonest spoofer obtains confidential information of the victim and withdraws money from his/her bank. This is the financial implication of E-mail Spoofing as an offence.

Similarly, an email appears to have been sent by a known person, but was actually sent from a different source. Cyber miscreants play this kind of 'hide and seek' to get personal information and images (mostly of women) and then use them to blackmail or harass them.

Some of the sociological reason for not being able to control the cybercrimes against women includes :

1. Lack of awareness as to cybercrimes
2. Social taboos on the victims
3. Family concerns
4. Most of the times the victims take blame on them, believing to be equally responsible for the incident.
5. Fear of media, as it can expose the identity of the victim's family and friends

As the victims are sharing information with friends, who are of the same age group who are equally untrained. By the time the family members or investigation officer gets to know about the offence, the damage would have already been caused. Therefore, it could be said that every effort must be taken by the family members, cyber experts and government to win the confidence of the victims so that the investigation could be expedited.

Several legal, technical and administrative measures were initiated by the Government to combat incidents of cyber crimes. Few significant them are as follows:

1. Structuring police stations and cells specifically to deal, investigate entertain, and aid cases and victims related to cyber crimes in each state.

[10] http://www.dqweek.com/net-pornography-incident-at-bal-bharti-school-raises-several-issues/

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

2. Training labs are set by Ministry of Electronic and Information Technology (MEITY) in north – eastern states and few cities like Kolkata, Bangalore, Pune and Mumbai to train police staff and judicial officers in investigation processes and evidence preservation in cyber crime cases. At the same time State governments with the help of MEITY and Ministry of Home Affairs took initiatives to set up modernized equipment to police to prevent , prohibit and control Cyber crimes.
3. Rules were formulated in 2016 by Ministry of Electronic and Information Technology (MEITY) for functioning of matrimonial websites to ensure safety and to secure people who use these websites and get deceived by the wrong and misleading information available on these sites. .
4. Computer Security Policy and Guidelines were circulated by the government to all the Ministries/Departments on taking steps to prevent, detect and mitigate cyber wrongs.
5. The Ministry of Home Affairs has developed a portal namely www.cybercrime.gov. for allowing the public to report cybercrime complaints.

CONCLUSION:

Indian Penal Code, 1860 is the Conventional and major Penal law of the land. In order to constitute an offence an act has to be performed , clubbed with guilty intention of the accused. Cybercrime which is a new age offence differs from conventional crime because of the way it is committed. Due to the technological advancements , IPC had to undergo amendments many a times, especially in the light of First Schedule of Information Technology Act,2000.The amended provisions of IPC have widened the offences involving electronic media and records. Words such as ‘computer resources’ and ‘electronic record’ were inserted in sections such as 119,167,173,175 of IPC. More particularly, Criminal Law Amendment Act,2013 covers the acts which involve the use of computers or any other forms of electronic devices to outrage the modesty of women. Unlike IPC , IT Act,2000 is a specific Law which deals exclusively with the aspects of use of use of information technology, including commission of cyber crimes.The provision under Sec 77 of IT Act,2000 provides that the offender shall not be released from liability under any other law , although he is held liable under any of the provisions of IT Act,2000.

Women in India like men are guaranteed with the basic rights like Right to equality, Right to freedom, right to life and liberty, Right to health, education, food,

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

employment, entertainment etc., by the Constitution of India. Modesty and Privacy which are deemed to be the integral parts of Right to life are not protected appropriately and adequately by the legislative and judicial trends , which adversely effects the social and economic development of the country at large. This latch is more dominantly observed in the cases, involving cybercrimes against women.

More particularly, women in India do not report the matters which are sexual in nature due to various reasons like social taboos, concerns relating to personal and family reputation , fear of negative publicity of media etc. Present era dominated by machines and technology knocks the door of the women to be cautious about the pitfalls of the usage of internet.

That apart more significantly, the 3 organs of the State ie., Executive, Legislature and Judiciary need to advance effective measure by enacting and enforcing stringent laws and rules substantively and procedurally to curb up the menace of cybercrimes. Establishing an adequate number of female cyber cells, ensuring safe and secured trial procedure by involving presence of female judge and conducting in camera proceedings, ensuring presence of female police personnel during investigation may resort to hike ion the cases of reporting against cyber crimes. At the same time, there is a requirement for the Indian legislature to acknowledge certain activities like cyber-bullying, cyber eve-teasing etc in IT Act,2000 through necessary amendments. The author here more significantly wants to stress on the identification, recognition of certain unlawful activities conducted via internet by the Criminal Major Law of the land ie., IPC and there by incorporating the same by considerable amendments to parent Criminal Act.

Cyber crime, being transnational in nature requires formulation of laws at international level as well. A common and harmonious recognition of laws at international level by unification of laws of all the nation states, by extending the scope of jurisdiction of the municipal laws for adjudicating and executing the matters pertaining to cyber crimes supports speedy trial and avoids delay in adjudication of cases . Therefore it is suggested that uniform provisions at international level as mentioned under Budapest Convention are required to harmonize the national laws involving cyber crimes.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

Some of the general precautions, non-exhaustive, are given under to help children/women to protect themselves from these cybercrimes:

1. Avoid friend requests from unknown person on social media platforms.
2. Avoid sharing personal information date of birth, address, phone number and school name etc., on social media.
3. Avoid talking about the physical or sexual experiences.
4. Avoid sharing sexually explicit photographs or videos.
5. Never turn on the webcam while chatting with a partner while he is not on cam.
6. When a chat partner suggests keeping the chat confidential or secret, keep the parents posted about the same.
7. Never install or subscribe to dating websites or apps.
8. Remember that the posts online remain there for many years and can be retrieved any time by anyone.
9. Safeguard the social networking account by using a complex password and change it periodically.
10. Use the option to restrict the visibility of the posts, in social media, to the selected persons or groups.