Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 6, 3920-3927

An Outline On Increasing Online Gender Violence Against Women In India And The Role Of Cyber Security

Adv. Ranjita Madiwale[1] , Dr.Sona Kumar[2]

[1]*Research scholar School of Law, G H Raisoni University, Amravati*, ranjita.madiwale06@gmail.com
[2]*Supervisor and Assistant Professor, G H Raisoni Law college ,Nagpur*, sona.kumar@ghru.edu.in

Abstract - The aim of this research paper is to study and analysis about the online gender violence in the form of various online crimes happening against Indian women in the cyber space after digital revolution in the form of access of internet and to find out the effective precautionary preventive measures to fight against this criminality.

According to the recent report presented by the National Crime Records Bureau (NCRB), and the data of NCW online crimes against women in India is increasing day by day. Multiplicity of crimes has brought in its wake by the advancement in computer technology and internet and delivered ever-increasing opportunities and prospects for the criminals to harassed women in cyber space.

As per recent data India has more than 560 million internet users and ranks second in the world in terms of the number of people with internet access. It was also estimated that by 2023, there would be over 650 million or more than that internet users in the country. As per the data available 40 present internet users are women in India. Who are mostly using social media without any knowledge of safety and security rules and become easy prey to the hands of online criminals.

Growing Online-crime has thus become a reality in India which is difficult to detect, not often reported and even challenging to prove in spite of several provisions in legislations, efforts of government and judiciary. Thus it is the urgent need of the century to find the effective measure to cope up with this menace in the form of powerful and controlling cyber security.

Technology is considered as a two-edged sword that can be working for either for good or evil purposes. This paper proposes the good positive use of technology in the form of cyber security for elimination of evil purpose of technology which is online crimes against women in India.

Keywords: women, online-crime, internet, cyber, security.

Introduction

New advanced technology introduced in life of human being and the entire world is now in the garb of its ever increasing scope. Specifically, new advanced communication technology which is possible only with the aid of Internet, has been integrated as a vital part of living at this time. Newly advanced computer technology provides an improvement to the human life and makes it easier and more comfortable. It enhances accuracy, swiftness and effectiveness of the life of all human beings.

Woman in the present era also whether she is a house wife or a working woman uses these advanced digital technology very easily. It is the reality that women in today's age have more facilities which probably women of prior years' didn't have.

It is true that development in the form of world wide web, mobile phones ,smart phones has absolutely changed ,raise the standard of living of women ,all these inventions came with massive benefits but it too has negative impact on women's life and created has great threat and violence in their life.

Violence against women and girls which is the part and parcel of their life since time immemorial is taking on fresh new forms with the constantly growing rates of easily accessible internet globally and the wider use of digital technologies. Physical, sexual and psychological ferocity taking place offline, including on the street, at home or in the workplace, have boomed, improved, spread and deteriorated by new advanced information and communication technologies. New forms of violence have also emerged.

Internet has positively provided the space for women to be linked worldwide and in ways not previously imagined. Women use internet to express themselves on various social sites as likewise as men in the society, but here also gender based violence appeared in their side.

Women in India are also becoming easy victim of advanced technology generated or facilitated crime. This creates a peril in their smooth life. Indian women who are already under the burden of various types of gender violence; advanced technology has increased their burden. Online gender violence in India is another type of violence against women which is encouraged by internet and information technology which has given birth to new kind of crime against women called as cyber or online crime against women.

In the cyber space, women are victims not only in the hands of individuals or group but also in the hands of technology where they have been drastically victimized by using various modes and methods.

Different types of online crime against women

One of the newly emerging crime techniques to manipulate innocent women by developing online trustful relation with women known as online grooming.

In the modus oprendi of Online grooming criminal deliberately cultivate an emotional connection with a woman in order to get something in return it happened. When a person uses social media, online grooming is a common technique used to manipulate women to obtain the trust of the target and finally utilize that trust and faith to use the victim.[1] It happens when the women use social media, where online groomers or predators deliberately cultivate an emotional connection with women in order to get something in return.[2]

Online and technology-facilitated violence against women exists in a continuum with the different forms of violence against women happening offline. Most of the forms of online and technology-facilitated violence against women are existing crimes and offences, but are expanded, amplified or widespread by the internet and digital technologies, for example in the case of domestic violence.

Scholar has stated here that online grooming is the opening doors to variety of other crimes against women such as morphing, cyber defamation, and blackmailing, forced porn and so on and named it all as technology generated crimes.

Crimes such as-:

1] **Cyber Pornography-** which means the publishing, distributing or designing pornography by using cyberspace. Revenge porn that is when any person willingly with intension circulates, distributes, or prints any absence or sexually explicit material without the consent of the person. With the easily availability of Internet and world web in India has significantly influenced pornography.

2] **Morphing** -Crimes against women involving morphed photographs are repeatedly on the rise in India. Usually celebrities are the main target of cyber criminals for doing morphed images, but nowadays, a simple ordinary woman is targeted by a criminal who may seek to revenge on any women for not an accepting proposal for an intimate connection, or to blackmail her or to otherwise harass her. Sometimes criminal minded people just do crimes like morphing only for business purposes for selling naked pictures of women or for blackmailing[3]

3] Online defamation -which is increasing with leaps and bounds refers to defamatory information being spread over the internet to harm a person’s reputation and image. The wide accessibility, mass reach, and increasing popularity of the internet make this offence more harmful than ever, and statutory provisions have been enacted as a safeguard against this issue.

Defamation that takes place in cyberspace is online or cyber defamation. It occurs when the internet is used as a medium to defame an entity. For example, posting defamatory statements about someone on social networking sites such as Facebook, WhatsApp, etc. falls under cyber defamation. Spreading emails with malicious content that can harm the reputation of a person also falls under the offence.

4] **Online sexual harassment** – It includes online flashing or sending unsolicited sexual images and comments, sexualized defamation as slander, sendup for sexual purposes; Sexualized and gender-based trolling; Image-based sexual harassment such as creep shots; which include sexually suggestive or private pictures taken and share on online without consent of women ,Image-based sexual abuse (non-consensual image or video sharing, or non-consensual intimate

[4]

image or "revenge porn") recorded sexual assault and rape, either live-streamed or distributed on pornographic sites.

5] Women trafficking -which is not a new concept, trafficking of women is an ancient enterprise that dates back nearly back to the beginning of civilizations. Female slaves were often highly valued in the ancient nations for the use of prostitution, but today it has become an international industry. The problem of women trafficking is growing rapidly and has received serious dimensions in the recent context of globalization. Trafficking especially of women is now a global problem that transcends borders and is often a crime just out of reach of national law enforcement agencies, especially when it moves to the online space Victims of women trafficking in India are predominantly illiterate and poor women who have limited opportunities to make money.

Perpetrators use social media to connect with the victim by hiding identities and increasing online anonymity. An analysis of cases in the 2018 UNDOC

Global report on trafficking in persons shows how perpetrates sequences their actions by identifying potential victims on social media, establishing a relationship of trust, and subsequently entrapping them in exploitative situations. Indian women are very easily tapped in their plans as due to their specific vulnerabilities, as they face various emotional and psychological distresses in their lives[4].

Aforesaid online violence against women occurs with the aid of different platforms and with a variety of tools, both publicly accessible and private, such as social networks, private messaging apps, e-mails, dating apps, forums, media comment sections, video games or videoconferencing platforms. The social media has most vital role in incasing online violence against women in India.

Social media and online crime against women

"Social media has become a good attractive and easily accessible ground for online criminals to harassed women by personal data leakage, stalking, cyber impersonation[5].

The new development in technology in the cyber space in the forms of wireless computing ,Wi-Fi ,broad brand ,social networking sites like Facebook ,Whatsapp, Instagram ,Snapchat ,Twitter which provide gateway ways to expanded social interaction enables the criminals to victimized women . The emergence of social networking technology has given birth to new forms of violence towards women .With the help of these technology criminals target vulnerable women easily and emerged a new form of online interpersonal violence. Women, especially Indian women belong to vulnerable group who are easily targeted by online criminals and are very easily caught in the web of criminals in cyber space.

This fact proves by the statistics of growing cases of online crime at the time of nationwide lockdown of covid-19 pandemic. When whole country was in lockdown at their homes and social media was the only one option to get connected with other people.

Significant' increase in online crime against women during lockdown.

As per the various surveys realized during the pandemic Violence against Women shows that "84% of respondents experienced online abuse from strangers.

The nationwide lockdown imposed from March 25 to April 14, and then extended to May 3, aims at preventing the spread of the novel coronavirus that has claimed 1,147 lives and infected 35,043 people in the country.

According to National Commission for Women (NCW) data, 54 cybercrime complaints were received online in April in comparison to 37 complaints – received online and by post -- in March, and 21 complaints in February. The panel is taking complaints online due to the lockdown.

Cyber experts, however, said the numbers are just the "tip of the iceberg"[6]

"We received a total of 412 genuine complaints of cyber abuse from March 25 till April 25. Out of these, as many as 396 complaints were serious ones from women, (and these) ranged from abuse, indecent exposure, unsolicited obscene pictures, threats, malicious emails claiming their account was hacked, ransom demands, blackmail and more," said the founder of the Akancha Foundation, Akancha Srivastava.[7]

Thus it is the reality that advancement of technology is the main cause behind online gender violence in India.

This makes life of Indian women more and more miserable.

Violence against women affects women because of their gender and their intersecting identities and exists on a scale that spreads online and technology-facilitated

Scope of increasing online crime against women in India

As per the National Crime Records Bureau
(NCRB) data from years 2017 to 2021 shown excessive hike in the cases of cyber pornography, Hosting, Publishing sexual material in India, which are easily taken and shared online by the online groomers as stated by the victim at the time of reporting of the cases.

India saw a great growth in online crimes against women between 2018 and 2020, according to the (NCRB), with cases lodged for publishing sexually explicit content online increasing to 6,308 from 3,076[8]

Recently , the Mumbai police arrested a third suspect involved in the Bulli Bai app case, the NCRB said in a report that Uttar Pradesh (2,120) saw the highest number of cases of sexually explicit content online, followed by Assam (1,132). Cases of cyber stalking and bullying of women rose from to 872 in 2020 from 739 in 2018, it said.[9]

The conviction rate for publication or transmission of sexually explicit content was 47.1% while in cases of cyber stalking and bullying are much more than that.

Among the metro cities, Bengaluru (248) reported the highest number of cases for publishing and transmitting obscene or sexually explicit act in electronic form, followed by Lucknow.

The increase in crimes against women in cyberspace encouraged several states to set up devoted units, said the report. Kerala Police is setting up a new cyber police battalion. Telangana has a dedicated cybercrime investigation department. Delhi Police has set up a special wing for cybercrimes and has a cyber-fraud detection unit in every district[10].

Legislative strategies to deal with online crime against women.

To deal with increasing cases of online violence against women Information Technology Act 2000 is available in India. Which was further amended in 2008.

The objectives of the IT Act are crystal clear from its preamble which confirms that it was formed largely for improving e-commerce hence it covers commercial or economic crimes i.e. hacking, fraud, and breach of confidentiality etc. but the drafters were unacquainted with the protection of net users.

Information technology act, 2000 has been passed by the Indian Parliament with the objective to facilitate the prevent Cyber Crimes. But the reality is that it is not a separate code for electronic transactions. It has only a gap filling role and it does not provide a separate legal regime and does not cover up the issues that have cropped up by the use of Internet especially cyber stalking, morphing and e-mail spoofing. In a sense this Act and its latest amendment of 2008 have the following drawbacks namely there exists no statutory definition explaining the term cyber-crime in any law in the respective countries.

The study revealed that there is no uniform law for online crimes, the police, prosecutors and the courts have to look into existing laws which are scattered in traditional criminal laws such as Indian Penal Code (IPC), the Evidence Act or the recently developed laws such as information technology (IT) Act and so on for providing justice to the victims. Furthermore, it has been noted that many websites have their servers outside India and harassers take huge advantage of this[11].

The study revealed that there is no uniform law for online crimes, the police, prosecutors and the courts have to look into existing laws which are scattered in traditional criminal laws such as Indian Penal Code (IPC), the Evidence Act or the recently developed laws such as information technology (IT) Act and so on for providing justice to the victims. Furthermore, it has been noted that many websites have their servers outside India and harassers take huge advantage of this geographic technical difficulty.

Even after the enactment of IT act various online harassment and crimes against women were introduced and growing but the present act (even after the amendment) has no special provisions regarding women issues only.

In spite of several provisions in legislations, efforts of government and judiciary the percentage of online gender crime is increasing day by day. So there is an urgent need to find the measure to cope up with the menace of online crime, which has changed the background or scenery of crime and criminal justice system

Challenges facing in the detection and elimination of online crime.

After analyzing the scope and the legislative strategies on online crime in the present time ,it would be apt to say that ;it would be very difficult to detect and eliminate online crime from society as

Identifying the form of violence is often difficult, as most forms of online violence do not have a clear legal definition and many forms overlap.

Filing of complaints is very difficult for victims of physical gender-based violence against women in general and it would be more problematic in cases of online and technology-facilitated violence against women, because of the technicality and evidential proves so most of the time women unable to file complaints ., it can remain challenging in more remote areas.

Most of the time the law –enforcement official are not trained to handle the technicalities of investigation of online crime so they also not willing and efficient to handle the complaint.

IT Act unable to give appropriate methods and directions for the investigation of online crime.

Most of the time victim is unaware about the procedure of filing of online crime complaints. The investigation work related to this kind of case is phenomenal. “There are so many reports, so many messages; the identification of people is time-consuming, requesting information from the service providers costs a lot of resources. There for there is much gap between the actual number of online violence against women and reported cases, actual number of cases being much greater then number of reported cases.

Most of the online crimes persist to be unreported due to the hesitancy and shyness of the Indian women and their fear of defamation of family’s name. Several times, women believe that she herself is responsible for the crime done to her. The women are more vulnerable to the danger of online crime as the wrongdoer’s identity remains unidentified and he may constantly threaten and blackmail the victim with different names and identities.

So the filing of complaints are very less and therefor the rate of punishment in online crime is negligible .there is no deterrence of punishment and law to criminals and so there were no check on online criminals.

Apart from that hacking tools and programs are readily available on the internet with the help of video’s it’s very easy to adopt the technique of hacking .In such a way digital technology misused for harassing human on cyber space and specially women who were mostly used social media to connect with friends ,relatives or to post photos and videos.

Cybercriminal very easily have access to this data, they could stale and share or they can sell your sensitive personal information or even change data, morphed the photos so that it benefits them in some way. Cybercrime against women occurs when a criminal gains access to a user’s personal information to steal funds, access confidential information, which could cause a range of problems in the life of women.

Cyber-crime in present era would become an unavoidable offense. Social media is one of the places where we leave most data and information behind.

Social engineering remains the easiest form of cyber-attack with ransom ware, phishing, and spyware being the easiest form of entry. Third-party and fourth-party vendors who process your data and have poor cyber security practices are another common attack vector, making vendor risk management and third-party risk management all the more important.

Day by day the world of the modern women has become increasingly dependent on digital technologies. This dependence means that there are more chances of victimization on cyber space. Personal Information theft is the furthermost costly and fastest-increasing section of online crime. Generally this happens only by the increasing disclosure of personal information to the web via cloud services.

Present Indian women are more technologically reliant than ever before and there were no sign that this trend will slow. Personal data disclosures that could result in identity theft and then it publicly posted on social media accounts.

Currently, treat of hacking or other online crime are no longer stopped by antivirus software or firewalls. The peril of online crime is continuously growing and can happen with anybody at any time. In reality human error is a major cause behind 90% of online crime against women in India.

Indian women are not technologically sound and unaware about safety measures to be fallowed at the time of using Internet and social media.

There for to avoid online crime against women is a greatest challenge in India.

For that the only solution is to find drastic cyber security measures and to understand the importance of cyber security in a real sense.

Need of cyber security to fight against growing online crime against women

Cyber security is related to protecting your internet and network based digital equipment’s and information from unauthorized access and alteration.

Cyber security is important to keep our private information, data, and devices safe. With the aid of proper cyber security measures people can protect their vast store quantities of data on computers and other internet-connected devices.

After analysis of the data of increasing online crime against women in India it is observed that, threats of online crime is the part and parcel of our everyday life.

As a result, cyber security is becoming more important than ever before.

There for its urgently needed to understand what we're exposed to online and how can we will protect ourselves from possible technologies of hacking and malware used by the cyber criminals.

By the moving world, cyber security has revolved out to be the major concern of the 21st century.

Cyber security acts as a precaution to reduce the effect of prospective online crimes as it provide security to protect computers, computer hardware, software, networks and data from unauthorized access, exposures provided through Internet by online criminals.

As per the famous phrase attributed by Dutch philosopher Desiderius Erasmus in around 1500centry

"Prevention is better than cure"[12]

Cyber security is the only drastic Precautionary measure when laws and other measures taken by government are failed to stand up against growing online crimes.

This digital world has improved out the life of Indian women but on some place, it has underground unpleasant reality. To avoid the unpleasant situation,

it is very essential to have tightened internet security, which is actually a right of every net user and it is duty of the internet provider to provide secure network to user. For taking cognizance on this issue Indian government has established National Cyber Security Policy 2013 for preventing Cybercrimes in India.

India now has a strategy in the form of policy which provide for the legal basis for the cause of cyber security in India. The vital objectives behind this policy are to create cyber- ecosystem in India. With the prospective to facilitate and monitoring at national level the cyber-crime and cyber infrastructure growth for cyber security compliance, cyber-attacks in India.[13]

Later in year 2020 Indian government has also formulated a National Cyber Security Strategy with the aim to improve cyber awareness and cybesecurity through more stringent audits and focus on the need of cyber security and suggested a separate budget for cyber security [14]

Such types of initiatives taken by government show that government also aware of the fact that cyber security has important role in the elimination of online crime.

The use of encryption technology is also important to avoid the harassing of online criminality.

If the false e-mail identity registration should be treated as illegal and it should be treated as offence as per the legislation would definitely help to control and it.

Hence, the scholar stated that importance of cyber security is a significant topic of today's era because it is more inclined toward social media. So, it is very essential to give importance to cyber security as the chief strategy for the security of Indian women. Aftermath is not subjected to one but to the entire society.

Result and Discussion

Technology plays a vital role in present scenario in growing cases of crimes against women. Online criminals and groomers take the advantage of digital platforms and adopt new strategies for smooth working of their ill intentions.

Technology such as advanced digital communication highly used by criminals to commit crime against women and women are the most attractive medium of criminals in cyber space.spcifically Indian women are also not very well aware about the various security measure which would be taken at the time of using social media so the scholar pointed here that ,there is a gap between technology and knowledge .which is also one of the reason behind increasing online violence against women in India after technological advancement .

The development of technology has carried about major changes in the current society. But human experience has shown that every technological change brings with it some unexpected complications, taking advantage of which the law breakers explore new techniques to commit their criminal activities.

From foregoing study it indicates that online violence such harmful activities in the cyberspace which may cause damage to a person, property or even the State or society as a whole. It is also true that cybercrime is a boundary less crime having no territorial jurisdiction so it would be very difficult to detect.

Therefore the menace of online criminality is not confined to one or two countries but the whole world is facing this enormous problem as a "technological contempt". India is no exception to this technology generated menace.

Growing online gender violence shows that there was a change to the background or scenery of crime and criminal justice system.

The new development in technology in the cyber space has emerged a new form of online interpersonal violence.

The silence of women and not reporting of the crime to the government authorities is also one of the reasons why the perpetrators are roaming free. Criminals take the benefit of such pity condition of victim women and many times blackmail them, because of all these harassing situation women are under great mental pressure that affects their health. In some situations they end their life as they are unable to handle the pressure. Here the scholar mentions that technology which was made with great object of welfare of human being works as a destroyer in cases of crime against women which are now committed the help of technology.

No doubt Information technology act, 2000 has been passed by the Indian Parliament with the objective to facilitate the prevent Cyber Crimes. But the reality is that it is not a separate code for electronic transactions. It has only a gap filling role and it does not provide a separate legal regime and does not cover up the issues that have cropped up by the use of Internet especially cyber stalking, morphing and e-mail spoofing. In a sense this Act and its latest amendment of 2008 have the following drawbacks namely there exists no statutory definition explaining the term cyber-crime in any law in the respective countries.

At the same time Act is silent about the precautionary measures and methods adopted for online security of the netizens.

Unawareness about the safety measures regarding cyber security is one of the vital causes behind growing online criminality.

Therefore at the concluding lines scholar stated that to cope up with the growing menace of online crime a strong cyber security is the need of the hour.

As every day online criminals invent new technology of hacking and harassing and which is more advanced and more risky to human being.

It is not possible to control such growing technology generated criminality only by legislations ,as it beyond their limitations .so if there were effective security available in cyber space for the net users or all the apps ,website were secure to the user and they have knowledge and awareness regarding it will definitely help in elimination of online crime.

Suggestions

In view of the growing dimensions of online crimes, there is need for adopting suitable supervisory legal measures and effective law enforcement mechanism to tackle the problems.

The user should also follow the Self-regulation rules at the time of using internet.

User especially women must avoid providing personal details such as family background ,picture related to the people with whom you are socializing, your private moments etc. on social websites like Facebook, Google+, Twitter, LinkedIn as it can be easily misused.

There is a serious need for training of law to enforcing agencies and IT professionals to curb the menace.

While a lot can be said about the IT Act, 2000, there is room for some improvement. Maximum punishments under the Act are bailable thus there is a necessity to increase the punishment and make the serious online gender violence offences as non bailable offences.

It is essential to have effective security measures for the users when they use different apps and sites ,for that government should made the drastic laws and permission should be granted only to the secure service provide, for that it is essential to take measures at International level.

Online crime against women is form of gender violence and eradicating any gender violence from society only laws are not sufficient but it requires cooperation and positive support from society also for that society has to change its attitude towards women, So that they would able to raise their voice against online crime and also file the complaint against such crime fearlessly without any burden and social stigma.

The most important is to create the awareness regarding online crimes especially amongst women and girls for that more and more legal awareness camps, campaign in schools and colleges should be organized by the governments and NGO.

To fight with this new form of criminality there is need to take effective cooperative measures from all the corners of the society because it is a socio legal technical issue and to build cyber secure environment needs co-operation and dynamic support of people, organizations, legislature, enforcing agencies, Government, judiciary and the most important is the cyber security provider and cyber regulatory bodies for regulation of rules, rights and duties of netizens. It also needs the cooperation from International organization for preventive cyber security measures.

Technology is an ever-growing concept and one that advances more and more with the changing world. The criminals will misuse it with great measure in the future for doing more criminal activities. Thus, we also have to take drastic preventive measures in the form of cyber security to cope up with problem of increasing online crime against women .As stated by the scholar earlier technology is considered as a two-edged sword that can be working for either for good or evil purposes. This paper proposes the good positive use of technology in the form of cyber security for elimination of evil purpose of technology which is online crimes against women in India. Cyber security is the urgent need today's society otherwise we won't be able to match the speed of these criminals and then no woman in the society will be safe.

References:

1] Barnes and Teeters (1959). New Horizons in Criminology. (3rd Ed.) PrenticeHall Publication Pg. 15-16.

[2] Crime in India (2015). Cybercrime, Ministry of Home Affairs Government of
India, chapter 18, Pg. 164.

[3] Desai, N. (1977). Women in Modern India. Vora Publication (2nd Ed.) Pg. 7-10.

[4] Duggal, P. (2017). Cyber Crime, Universal Publication (2nd Ed.) Pg. 17.

[5] Gaur, K.D. (2016). Textbook on Indian Penal Code. (6th Ed.) Universal Law Publication Pg. 9-10.

[6] Khubalkar, D. Dr. (2019). Cyber crime Law in India. (1st Ed.) University
Book House Pg. 15.

[8] Mittal, M. (1995). Woman in India Today and Tomorrow. (1st Ed.) South
Asia Book Publication Pg. 10-15.

[9] Anand, A.S, Chief Justice. 2004. Justice for Women, Concern and Expression, 2nd ed: Universal Law Publishing Co. Pvt. Ltd.

[10] Cyber crime against women in India. https://sagepub.com

[11] Halder, D and Jaishnkar, K; Cyber victimization in India: A baseline survey report(2010) December 1 (2010)

[12]CYBER CRIME AGAINST WOMEN IN INDIA by Debarati Halder, K.Jaishankar (2017)

[13] Ghorai,S., (Dr.) Thapak, N. K., Cyber Crime, Victimization against Women in India and It's Preventive Measures ; Journal of Advances and Scholarly Researches in Allied Education | Multidisciplinary Academic Research

[14]www.ncrb.gov.in

[15]https://feminisminindia.com

[16] https://womenagainst.com

[17]www.newapps.nic.in

[18]www.unodc.org