Cyber Crimes against Women: A Gloomy Outlook of Technological Advancement

Abhinav Sharma & Ajay Singh
Faculty of Law, Aligarh Muslim University
Aligarh, India

ABSTRACT: The right to internet usage has now become a human right, as declared by the United Nations Human Rights Council in June 2016. The number of internet users are rapidly growing in India as well and the idea of a modern India has had a strong focus on science and technology for its all-inclusive development.

In this research paper, the authors shall analyze the role of the increase in technology, thereby, easier access to internet and social media platforms as a major cause of increasing cyber-crimes against women in the Indian society. The netizens, women in particle, are more susceptible to the criminal activities carried out by means of internet, which is also referred to as cyber-crimes.

The judiciary along with the police department and the investigative agencies should be boosted up with the modern web-based applications in order to be a step ahead from such perpetrators.

The legal remedies available under various piece of legislations dealing with the menace of cyber-crime have been focused upon. The role of government in the current legal scenario and the accountability of the government is also discussed in detail.

The focus will also be on the various factors resulting in the increase of cyber-crimes against women and the effects of such crimes on the victim.

The paper concludes by considering the loopholes in the system, that neither the provisions of the Indian Penal Code, 1860 nor the Information Technology Act, 2000 satisfactorily deal with such offences and fail to provide adequate safety measures to curb the same.

Lastly, the author(s) recommends certain necessary measures that need to be taken in order to address the issue of cyber-crimes against women in a holistic and effective manner.

PHRASES: Information Technology, Legislature, Cyber-crimes, Legal Remedies, Netizens..

I. INTRODUCTION

India is developing rapidly and one of the major factors contributing to its growth is the technological advancement. It is pertinent to note that every time there is a revolution, it has greatly benefitted the mankind. India surely marches ahead unprecedentedly with advancements in the technology department and more particularly, the information technology. The idea of a modern India has had a strong focus on science and technology for its all-inclusive development.

However, this rapid advancement has its downside too. The netizens, women in particle, more susceptible to the criminal activities carried out by means of internet, which is also referred to as cyber-crimes. Women due to various factors such as unawareness, lack of privacy regime etc. are prone to such cyber-attacks over the internet.

The right to internet usage has now become a human right as declared by the United Nations Human Rights

Council.[1] The number of social network users in India has increased drastically from 181.7 million in 2015 to 216.5 million in 2016 to a projected 250.8 million in 2017.[2] It is expected that the same would increase to at least 336.7 million by 2020.[3] A study of internet users in India, conducted by the Boston Consulting Group and Retailers Association of India, states that approximately 29% of the users in India are women.[4]

One cannot shy away from the fact that women in our society are prone to cyber offences every now and then, which is a major concern considering its impact.

Cyber-crime is a global phenomenon. With the advancement in technology, cyber offences and the victimization and objectification of women are increasing and it poses a great threat to the security and mental health of the individual. Though, India is one of the few nations to enact and enforce a piece of legislation[5] to combat cyber-crimes, any special provision regarding the cyber-crime against women still remains untouched. The grave threat to security of women in general has not been considered by the Act.

Cybercrimes against women are still taken lightly in India, mostly because in general the respect towards women in our modern society is on a decrease and also a lot of people are unable to come to terms with the fact that even posting images of someone online in a crime. Cybercrimes such as morphing, e-mail spoofing do-not have a moral backing in society and hence are taken lightly. This brings us to the most important part where social advancement is needed, people need to recognize the rights of others and realize what constitutes a crime.

The people must learn not to interfere with the private lives of others, to have respect towards women. All this can only be done if young kids are taught from a young age to respect women.

Hence, to counter cybercrime against women in India, not only stricter penal reforms are needed but also a change in education system is a huge requirement. Such change cannot come from within a single block of society but people, government and NGOs etc. need to work together to bring forth such changes.

II. UNDERSTANDING CYBER CRIMES

In common parlance, Cyber-crime can be defined as any illegal activity for which a computer is used as its primary means of commission. Cyber Crimes are crimes which may be committed against persons, property as well as government.

Cyber space's have become havens for cyber criminals. Women are the most soft and vulnerable targets over the internet and it become a cakewalk to target the less aware individuals. Social networking platforms are the

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

[2] Number of social network users in India from 2015 to 2021 https://www.statista.com/statistics/278407/number-of-social-network-users-in-india/ Last visited on: 16/08/2018.

[3] Ibid.

[4] Boston Consulting Group & Retailers Association of India (2016), Decoding Digital @ Retail: Winning the Omnichannel Consumer.

[5] Information Technology Act, 2000.

most prone areas to victimize people and especially women. The most common cyber-crimes inflicted to women are harassment via emails, cyber stalking, cyber pornography, obscenity, defamation, morphing and email spoofing.

The cyber world in itself has a virtual reality where anyone can hide or even fake his identity, this gift of internet is used by the criminally minded to commit wrongful acts and then hide under the blanket provided by the internet.

Women especially young girls inexperienced in the cyber world, who have been newly introduced to the internet and fail to understand the vices of internet are hence, the most susceptible to falling into the bait of cyber criminals & bullies.

Some of the prominent cyber-crimes against women are:

- Violation of body privacy.
- Online harassment.
- Cyber stalking.
- Exposure to online fraudsters.
- Portraying women in a most indecent manner.
- Workplace harassment with digital aid.

III. REASONS FOR THE GROWTH OF CYBER CRIMES AGAINST WOMEN

According to the official statistics provided by the National Crime Records Bureau, Government of India, 9622 cases of cyber-crimes were registered in 2014 and 5752 persons arrested. In 2015, 11,592 cases were registered an increase of 20% in registration of cases from the previous year – and 8121 persons arrested.[6]

Thus, it is crystal clear that the cyber-crimes against women in our society have taken a toll since the introduction of information and technology and access of internet in almost every hand. And it is high time that there should be a strict involvement of legislature as well as the executive to curb the same.

Some of the prominent reasons for the growth of cyber-crimes against women can be regarded as:

- The transcendental nature of the internet-no boundaries, ever changing.
- Low equipment cost.
- Numerous vulnerable targets- Loneliness is a prime cause as many female students and staff live away from their family and work for long hours over the computers. Thereby, the computers become their trusted pal.
- Easy concealment due to anonymity.
- Cyber-crimes in most of the cases are not even reported due to the fear of society, hesitation, shyness

[6] Crime in India 2015, Chapter 18- Cyber Crimes, Ministry of Home Affairs, Government of India, p. 164

and fear of defamation.

- In most cases, such cyber-crimes are not even addressed due to the hesitation and shyness of the victim and her fear of defamation of the family's name in the society.

However, even today the Indian police tends to not tends to take cybercrimes seriously. In such scenarios, the woman or the young girl who falls prey to cyber victimization should first contact a women assistance cell or NGO (such as All India Women's Conference[7], Sakshi[8], Navjyoti[9], Centre for cyber victims counselling[10]) which will assist and guide them through the process, also this will make sure that police does not take any case lightly.

The main reason for the increased number of cyber-crimes against women in India can also be regarded to as due to lack of legal security. The need of the hour is to make stringent laws and the proper implementation of such laws should also be ensured. The Government and the legislature should be made accountable to take effective steps in furtherance to protect women from cyber-crimes.

On the other hand, humiliation, mental torture, stress, depression aggravates the situation. On account of delayed justice, people have lost faith in the law enforcement authorities. Lack of legal awareness makes it more complex. Further, most women overlook the privacy rules and regulations listed on the social networking websites.

It is pertinent to note that the women themselves can help in regulating cyber obscenity by becoming aware of their rights and ensuring to abide by the safety measures provided and prescribed over the places. Some of the famous social media platforms provide wide options in their respective privacy policies to guard and protect women from such perpetrators.

At the same time, one should also bear in mind that, most of the popular websites declare their privacy policies that they will not take any responsibility for any sort of harassment caused to the users by other users. Therefore, before registering on every other social media platform, women should go through the privacy policies or safety measures related to such offences.

Negligence and non-vigilance in most of the cases is also a root cause in regards to women being the targets of cyber obscenity.

IV. EFFECTS OF CYBER CRIMES AGAINST WOMEN

Although any type of crime has a huge negative effect on the victim and the society as a whole. Some have less and some have a huge one, but effect is everywhere.

[7] http://www.aiwc.org.in/ (Private group of women assisting other less fortunate women to fight the crimes committed against them)

[8] http://www.sakshingo.org/ (NGO assists women in dealing with govt authorities)

[9] http://www.navjyoti.org.in/ (NGO by Kiran Bedi, assist women in several aspects)

[10] http://www.cybervictims.org/(Private group of legal minded individuals who help the victims of cybercrimes)

The first reaction of a woman who has seen herself as a victim is in a deep mental shock. It becomes hard for her to believe that it is the same old self she knows for so many years; since her birth to be precise, especially in the cases of cyber defamation or cyber pornography.

The next thing which comes in her mind when such a case happens is "Oh, I have been seen in such an embarrassing state by millions of net users by now. Where do I hide my face now?" The psychology of the poor victim can be easily understood, but no one except the victim herself can guess the after effects in future on her. Some gets panicked. She cannot confide it with his family or friends.

The thoughts of making her "secret self" public, bites her day and night. Some start losing their basic interests in life like eating, socializing or even working with the daily schedules. The most dangerous effect is the urge of revenge. When the ash of taking revenge burns inside her, there is every possibility of her turning herself into a cyber-criminal to take revenge of her insults and then slowly the passion of destroying other's peace at the cost of her happiness grips her mind.

Meaning thereby, a cyber-crime against women makes her helpless, hopeless and harms her emotional and mental well-being. It ultimately acts as a barrier to the empowerment of women having a lifelong devastating effect on the victim.

V. LEGAL PROTECTION (REMEDIES)

The first ever conviction in India for cyber pornography, was in the case of ***Suhas Katti* v. *State of Tamil Nadu***, decided by a Chennai Court in 2004.[11] The woman, a divorcee, complained to the police about a man who was sending her obscene, defamatory and annoying messages in a Yahoo message group, after she turned down his proposal for a marriage. The accused opened a fake email account in the name of the woman, and forwarded emails received in that account. The victim also received phone calls by people who believed that she was soliciting for sex work. The police complaint was lodged in February 2004 and within a short span of seven months from the filing of the First Information Report, the Chennai Cyber Crime Cell achieved a conviction. Katti was punished with two years' rigorous imprisonment and Rs. 500 fine under S. 469 IPC (forgery for the purpose of harming reputation), one year's simple imprisonment and Rs. 500 for offence under S. 509 IPC (words, gestures or acts intended to insult the modesty of a woman) and two years' rigorous imprisonment and with Rs. 4000 fine for offence under S. 67 of IT Act 2000 (punishment for publishing or transmitting obscene material in electronic form).

The very first instance of cyber defamation in India was recorded in the case of **SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra**[12] - cyber defamation was reported when a company's employee (defendant) started sending derogatory, defamatory and obscene e-mails about its Managing Director. The e-mails were

[11] Order passed on 5th Nov'2014 in CC No. 4680 of 2014

[12] http://cyberlaws.net/cyberindia/defamation.htm Last visited on: 16/08/2018.

anonymous and frequent, and were sent to many of their business associates to tarnish the image and goodwill of the plaintiff company. The plaintiff was able to identify the defendant with the help of a private computer expert and moved the Delhi High Court. The court granted an ad-interim injunction and restrained the employee from sending, publishing and transmitting e-mails, which are defamatory or derogatory to the plaintiffs.

Thus, the Courts have also played an active role to provide legal security over the internet. People need to have put faith and belief in the justice delivery system. Judiciary is for the society and it will always be the support system a society needs to grow and develop.

The following legal remedies available to a victim of cyber-crimes:

- **Online/Mobile Harassment/Cyber Bullying and Cyber Stalking**

Harassment through electronic means by sending grossly offensive or menacing information, and persistently causing annoyance, injury, insult etc. is punishable with imprisonment for a term which may extend to 3 years and with fine.[13]

- **Sending offensive messages through a computer resource or communication device: Section-66A, IT Act**

It includes:

i. Any information that is grossly offensive or has menacing character, or
ii. Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, enmity, hatred, ill will, persistently by making use of such computer resource or a communication device, or
iii. Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages.

Such an act is punishable with imprisonment for a term which may extend to three years and fine.[14]

- **Sexual Harassment: Section-354A IPC**

A man committing any of the following acts:

i. Physical contact and advances involving unwelcome and explicit sexual overtures; or
ii. A demand or request for sexual favors; or
iii. Showing pornography against the will of a woman; or
iv. Making sexually coloured remarks,

Shall be guilty of the offence of sexual harassment.

The first three offences of sexual harassment carry punishment of rigorous imprisonment for a term which may

[13] Section-66A. Information Technology Act, 2000.
[14] ibid.

extend to three years, or with fine, or with both.[15]

The last offence of sexual harassment carries punishment of imprisonment of either description for a term which may extend to one year, or with fine, or with both.[16]

- **Stalking: Section-354D IPC**

Any man who:

i. Follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or

ii. Monitors the use by a woman of the internet, e-mail or any other form of electronic communication,

commits the offence of stalking.

And whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and shall also be liable to fine.[17]

- **Violation of Body Privacy: Section-66E IT Act**

Capturing the image of a private body part of a person is punishable with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or both.[18]

- **Voyeurism: Section-354C IPC**

Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed wither by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years,[19] and shall also be liable to fine, and shall be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but may extend to seven years, and shall also be liable to fine.[20]

In a case where the victim consents to the capture of the images or any act but not to their dissemination to third persons and where such image or act is disseminated, such dissemination shall be considered as an offence under this section.[21]

- **Punishment for publishing or transmitting obscene material in electronic form: Section-67 IT Act**

Whoever publishes transmits or causes to be published in the electronic form, any material which is lascivious

[15] Section-354A Indian Penal Code, 1860.
[16] ibid.
[17] Section-354D Indian Penal Code, 1860.
[18] Section-66E. Information Technology Act, 2000.
[19] Section-354C Indian Penal Code, 1860.
[20] Ibid.
[21] ibid.

or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees.[22]

- **Material containing sexually explicit act, etc. in electronic form: Section-67A IT Act**

Whoever publishes or transmits or causes to be published or transmitted in the electronic from any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees.[23]

VI. ROLE OF GOVERNMENT

In May 2016, the Union Minister for Women and Child Development, Ms. Maneka Gandhi, observed that the online abuse of women in India ought to be treated in the same manner as violence against women in the real world, and created a new forum for redressal, and further instructed the National Commission for Women to create a system for taking action against online abuse of women.[24]

After consultation on Cyber Crimes in India held on 23.07.2014, National Commission for Women has submitted a report on **"Ways and Means to Safeguard Women from Cyber Crimes in India",** which inter-alia recommended for stringent law, Policy to discourage hacking activities, dedicated helpline numbers, opening of more cyber cells, and imparting of proper legal, setting up forensic labs and technical training law enforcement agencies like police& judiciary etc. to combat cybercrime.

There are adequate provisions dealing with cyber-crimes in the Information Technology Act, 2000 as well as the Indian Penal Code, 1860. Government has, in fact, taken a number of legal, technical and administrative steps in furtherance to prevent and curb cybercrimes. These inter alia, include:

i. Cyber Police Stations and Cyber Crime Cells have been set up in each State for reporting and investigation of Cyber Crime cases.
ii. Cyber Forensics Training Labs in north-eastern States and cities such as Mumbai, Pune, Kolkata and Bangalore has been set up by the Ministry of Electronics & Information Technology(MeitY) to train State police officials and judiciary in cybercrime detection and collection, preservation and seizing of electronic evidence and dealing with cybercrime.
iii. Various steps have been taken by Ministry of Home Affairs, Meity and State Government to modernize the setup and equip police personnel with knowledge and skills for prevention and control of cybercrime

[22] Section-67. Information Technology Act, 2000.
[23] Section-67A. Information Technology Act, 2000.
[24] Online trolling against Women to be considered violence: Maneka Gandhi, Deccan Chronicle, 18th May'2016.

through various national and State Police academies/judicial academies and other institutes.

iv. An advisory on functioning of Matrimonial website on 6thJune, 2016 under Information Technology Act, 2000 has been issued by the Ministry of Electronics & Information Technology. Rules are also laid down thereunder directing the matrimonial websites to adopt safeguards to ensure that people using these websites are not deceived through the means of fake profiles or misuse/wrong information posted on the website.

v. Computer Security Policy and Guidelines to all the Ministries/Departments has been issued and circulated by the Government on taking steps to prevent, detect and mitigate cyber-attacks.

vi. A portal namely www.cybercrime.gov.in has been developed by Ministry of Home Affairs to allow public to report cybercrime complaints.

VII. LOOPHOLES IN THE CURRENT LEGAL SCENARIO

The increasing number of crimes against women are a huge concern for any state however, cybercrimes make it even more challenging as criminals have the opportunity to create fake identities and then after indulge in illegal activities. To counter this government should make strict laws to apply on the Internet Service Providers(ISP), as they alone have the complete record of all the data being accessed by anyone surfing on net. ISPs should be made to report any suspicious activities that any individual is indulging into, this will help to curb crimes in nascent stage.

Legislature needs to make stricter regulation for cyber cafes, who should keep a proper detailed record of their customers who utilized their internet services, often people go to cyber cafes to indulge in criminal activities so as their own IP addresses are not revealed in any future investigation. This is another manner to mask identity.

People need to be cautious over which parts of their daily lives are being recorded by cameras & should act modest in such times. Awareness over cyber culture and its back draws also need to be improved amongst people. People need to be made aware of their rights. Studies show that a large population of internet users in India have no knowledge of their rights in such matters.

The prominent hindrances related to the issue of cyber-crimes against women are related to the procedural aspects of litigation such as the conflict of jurisdiction, loss and lack of evidence, lack of cyber army and cyber savvy judiciary. Judiciary plays a vital role in by shaping the enactment of the statutes framed to tackle the issues. Today with the growing arms of cyberspace, the territorial boundaries seem to have no value or restrictions thus the concept of territorial jurisdiction as envisaged under S.16 of C.P.C. and S.2. of the I.P.C. providing least value to the relevance of the issues relation to the cyber-crime and thus will have to give way and scope to alternative method of dispute resolution.

If we look into the law, we find that under no section in IT ACT 2000, Obscenity, i.e. personal viewing, which can be the violation to some other person's rights, to be an offence. If we look into IPC, only section 292 tells if it is proved that you have published or transmitted or caused to be published in the electronic form then only it can be an offence. Moreover, the Information Technology Act, 2000 addresses certain common cyber-crimes such as cyber stalking, morphing and email spoofing as offences. The women netizens in India are reluctant to report the cyber-crime immediately due to the fear of being recognized at the public sphere. Though such incidents are on the rise, only a few victims are willing to register a case and demand for justice.

Thereby, the main reasons for the failure to curb such crimes against women can be confined to:

- Preconceived notions about police and the criminal justice system.
- Attitude of the victim.
- Patriarchal society.
- Fear of revealing of past history.
- Privacy issues.

VIII. CONCLUSION: A WAY FORWARD

The chief problem of cybercrime lies in the modus operandi and the persistence of the cybercriminals. The judiciary along with the police department and the investigative agencies should be boosted up with the modern web-based applications in order to be a step ahead from such perpetrators.

It is the job of the legal system and regulatory agencies to keep pace with the technological developments and ensure that newer technologies do not become tools of exploitation and harassment.

Governments can take legislative measures that ensure human rights; especially women's rights are protected online just as they are physical spaces. Legislations should not just protect users; however, it should also educate and inform all groups on how to exercise their communication rights.

Moreover, individuals should be more aware online as well as offline with regards to the precautionary measures in the cyber space and the remedies available if their right is violated. Though there used to be several difficulties in dealing with cybercrimes such as loss of evidence and lack of cyber army but with the Criminal Law Amendment Bill (2013) most of these problems have been taken care. However, several changes are still needed such as cyber savvy judges.

It can be stated that proper implementation of laws along with public awareness and education of women concerning their rights and legal remedies can play a crucial role in eradicating cybercrimes from our society. Enacting of laws cannot be the only recourse available to curb such crimes. Also, only looking from the angle of protection of the social mores would also not suffice.

The digital technology has grown faster than the laws governing the technology. Hence the existing laws fall short to tackle the situation.

The menace of cyber-crime extends not only to India, but is widespread across the planet. Hence, there is a need for coordinated and integrated effort on part of the world community. Additionally, grievance redressal mechanisms and institutions should be vitalized and popularized, with the ease of lodging complaints and minimizing delay in investigation and prosecution as major objectives.

IX. SUGGESTIONS/TIPS TO FOLLOW TO STAY SAFE FROM CYBERBULLYING:

- The increasing number of crimes against women are a huge concern for any state, however, cybercrimes make it even more challenging as criminals have the opportunity to create fake identities and then after indulge in illegal activities. To counter this government should make stricter laws to apply on the Internet Service Providers(ISP), as they alone have the complete record of all the data being accessed by anyone surfing on net. ISPs should be made to report any suspicious activities that any individual is indulging into, this will help to curb crimes in nascent stage.
- Legislation needs to make stricter regulation for cyber cafes, who should keep a record of their customers who utilized their internet services, often people go to cyber cafes to indulge in criminal activities so as their own IP addresses are not revealed in any future investigation. This is another manner to mask identity.
- Peopleneedtobecautiousoverwhichpartsoftheirdailylivesarebeingrecordedby cameras & should act modest in such times. Awareness over cyber culture and its back draws also need to be improved amongst people. People need to be made aware of their rights, studies show that a large population of internet users in India have no knowledge of their rights in such matters.
- Approach the police when you are getting harassed online and not be scared of he perpetrator.
- Email spoofing is possible because of Simple Mail Transfer Protocol (SMTP), the main protocol used in sending email, does not allow an authentication mechanism. Although an SMTP service extension allows an SMTP client to negotiate a security level with a mail server, however this precaution is not always taken. So women should take precaution and always add the SMTP service extension with the SMTP client.

The women netizens in the Indian society still do not immediately report the cyber-crime or the cyber abuse. The major issue of cyber-crime lies in the modus operandi and the motive of the cyber-criminal. People misuse the anonymity which the cyber space provides. This particular nature of the cyber space provides the offender a

chance to escape and hide after the commission of cyber-crime. Thus, necessary steps should be taken to ensure the adequate reporting of crimes and protection of the identity of the individuals.